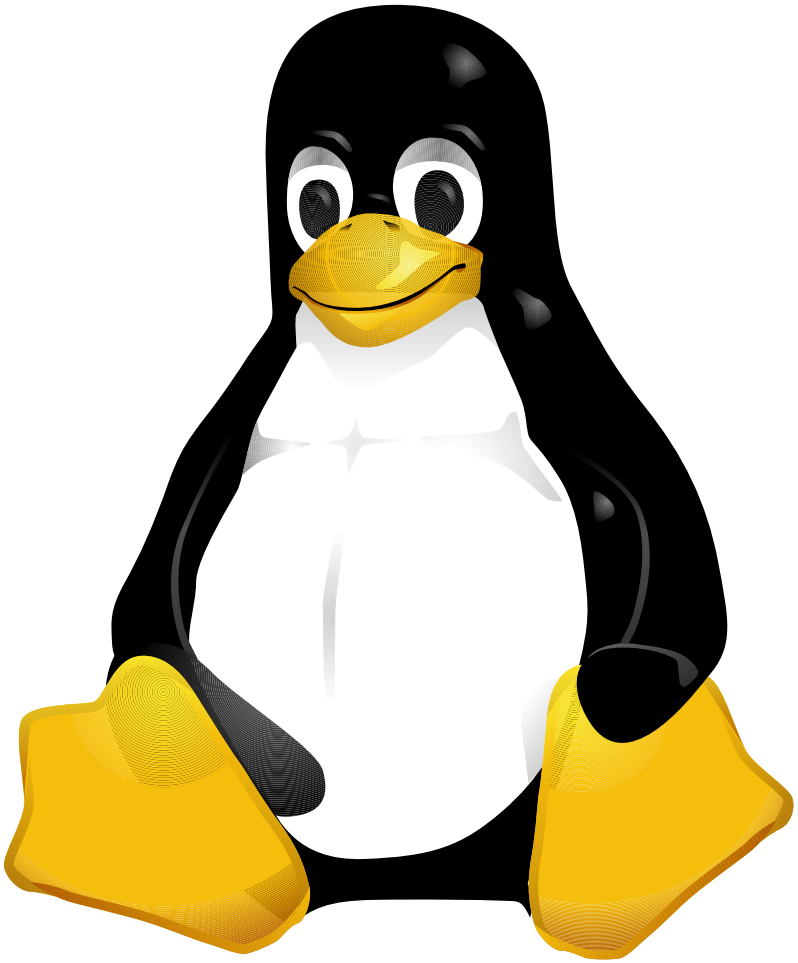
Technische Praxis der Computersysteme

Teil 2-1

Systemadministration unter Linux/Unix

Roland Steinbauer, Oliver Fasching, Andreas Nemeth,
Martin Piskernig, Florian Wisser

Version 1.00, April 2001



Inhaltsverzeichnis

Literatur

[1] Evi Nemeth, Garth Snyder, Scott Seebass, Trent R. Hein. *Unix System Administration Handbook.* 3rd Edition. Prentice Hall, New Jersey. 2000.

[2] Matt Welsh, Lar Kaufman. *Running Linux.* 3rd Edition. O'Reilly & Associates Inc. Sebastopol, CA. 1999.

[3] Aeleen Frisch. *Essential System Administration.* 3rd Edition. O'Reilly & Associates Inc. Sebastopol, CA. 2002.

[4] Cameron Newham, Bill Rosenblatt. *Learning the Bash Shell.* 2nd Edition. O'Reilly & Associates Inc. Sebastopol, CA. 1998.

[5] Lars Wirzenius, Joanna Oja, Stephen Stafford. *The Linux System Administrator's Guide.* Version 7.0. `http://www.linuxdoc.org/LDP/sag`. 2001.

[6] Steve Frampton. *Linux Administration Made Easy.* `http://linuxdoc.org/LDP/lame/LAME/linux-admin-made-easy`. 1999.

[7] Matt Welsh et al. *Linux Installation and Getting Started.* `http://linuxdoc.org/LDP/gs`. 1998.

[8] Larry Wall. *Programming Perl.* 3rd Edition. O'Reilly, UK. 2000.

Vorwort

Die vorliegende Version 1.0 ist eine wesentlich überarbeitete Neuauflage des Skriptums vom Sommersemester 2001. Teil 2-1 beinhaltet eine Einführung in die Grundlagen der Systemadministration unter Linux/Unix mit Ausnahme der Netzwerkfunktionen, die im Teil 2-2 behandelt werden.

Gegenüber dem Vorjahr wurde die Kapitlezusammenstellung teilweise neu arrangiert und vor allem die Kapitel 1, 3, 4, 8 und 10 neugestaltet und das Kapitel 12 sowie die Grundlagen der Sicherheit von Computersystemen vom Teil 2-2 in den Teil 2-1 vorverlagert. Desweiteren habe ich mich bemüht, die gesamte Präsentation homogener zu gestalten und die stilistischen Eigenheiten der verschiedenen Kapitel (deren ursprüngliche Entstehung verschiedenen Autoren zu verdanken ist) auszugleichen. Schließlich habe ich versucht, der schnellen Entwicklung des Gebiets Rechnung zu tragen und die nötigen Aktualisierungen vorgenommen.

Großartig unterstützt wurde ich in all diesen Belangen von Oliver Fasching, der auch die Verwaltung des LaTeX-Quellcodes übernommen hat. Weiters gilt mein besonderer Dank den zahlreichen StudentInnen und meinen Tutoren, die mich auf viele Unklarheiten und Fehler in der Version 0.95 aufmerksam gemacht und damit wesentlich zur Verbesserung des Textes beigetragen haben.
Wie immer gilt mein ganz besonderer Dank den Mitarbeiterinnen des Sekretariats für ihre freundliche Unterstützung.

Roland Steinbauer, April 2002

Vorwort zur Version 0.95 (Sommersemester 2001)

Das vorliegende Skriptum dient zur Begleitung des 1. Blocks der Vorlesung „(Technische) Praxis der Computersysteme, Teil 2“ im Sommersemester 2001 am Institut für Mathematik der Universität Wien, die als Fortsetzung der Vorlesung vom vergangenen Wintersemester konzipiert ist. Es deckt die (meisten) grundlegenden Themen der Unix/Linux Systemadministration – mit Ausnahme aller Netzwerkfunktionen – ab: Letztere bleiben dem 2. Block und einem weiteren Teil des Skriptums vorbehalten.

Als Vorkenntnisse für ein erfolgreiches Lesen sind die grundlegende Vertrautheit im Umgang mit einem Unix-System, der Unix-Shell und die Beherrschung eines Texteditors (bevorzugt `vi`) zu nennen; etwa in dem Umfang, wie sie im ersten Teil der Vorlesung bzw. des Skriptums vermittelt werden.

Grundlage des „Werks“ sind die Vortragsfolien und -vorbereitungen der letztjährigen Vorlesung mit gleichem Titel, die ich ebenso am Institut für Mathematik gehalten habe. Schon damals wurde ich tatkräftig von Florian Wisser als Tutor unterstützt; Reinhard Danzinger, Andreas Nemeth und Martin Piskernig haben als Hörer aktiv ins Geschehen eingegriffen und zu einigen Themenbereichen selbst Vorträge ausgearbeitet. Nun wurde das vorjährige „Skriptums-Gerippe“ unter geteilter Autorschaft zu einem fortlaufenden Text erweitert, der viele der ursprünglichen Folien als Zusammenfassung und Referenzpunkte enthält, aber auch zum eigenständigen Lesen und Lernen einlädt.

Als Quellen haben wir – neben unserer Erfahrung als Systemadministratoren und den im Text angeführten Seiten im Internet – vor allem die Bücher [1] und [2] herangezogen.

Der Umfang des Textes ist vor allem durch das Einbeziehen vieler praktischer Aspekte (etwa in Kapitel 6 und 11) überraschend angewachsen, sodass das ganze Projekt beinahe den vorgegebenen zeitlichen Rahmen gesprengt hätte. Die sehr zügige Endredaktion hat mich davon abgehalten, an Formulierungen zu feilen

und den einen oder anderen Aspekte noch stärker zu betonen, weshalb die Versionsnummer nochmals unter 1.0 geblieben ist.

Besonders zu Dank verpflichtet bin ich neben meinen Koautoren meinen (Ex)-TutorInnen Mark Heinzle, Barbara Pocza und Matthias Zeichmann sowie unserem Sekretariat, das mich mit besten Kräften bei der (rechtzeitigen) Fertigstellung des Skriptums unterstützt hat.

Wie immer liegt die Verantwortung für alle Ungereimtheiten und Fehler bei mir und ebenso natürlich wie im Wintersemester ergeht die Einladung an alle Interessierten, an einer verbesserten Neuauflage für das nächste Mal mitzuarbeiten. Weitere Informationen zur Vorlesung, den Übungen und zum Thema finden sich unter `http://www.mat.univie.ac.at/praxis`.

Roland Steinbauer, April 2001

1 Einleitung

In diesem ersten Kapitel geben wir einen Überblick über Grundlagen und Aufgaben der Systemadministration. Wir besprechen kurz allgemeine Strategien und Methoden, die „politischen“ Aspekte der Systemadministration und widmen uns dann ihren praktischen Auswirkungen. Wir besprechen kurz die häufigsten Aufgaben in der Systemadministration und diskutieren Aspekte des Rootzugangs zu Unix-Systemen.

1.1 Aufgaben in der Systemadministration

Wir geben hier einen kleinen Überblick über die in der Systemadministration anfallenden Aufgaben und Tätigkeiten. Diese müssen nicht unbedingt alle von einer Person erledigt werden und in der Praxis werden oft verschiedene Aufgabenbereiche von verschiedenen Personen wahrgenommen. Trotzdem muss es für jedes System mindestens eine Person geben, die alle diese Tätigkeiten versteht, den Überblick bewahrt und sicherstellt, dass alle Aufgaben richtig und zeitgerecht erledigt werden. Die Liste der Aufgaben ist weder erschöpfend noch strikt nach Prioritäten geordnet; letztere variieren von System zu System.

Benutzerverwaltung: In einem Multiuser System müssen die Accounts der einzelnen Benutzer gewartet werden. Die Hauptaufgaben bestehen im Hinzufügen neuer und im Löschen von nicht mehr benötigten Benutzeraccounts. Diese Prozeduren können automatisiert werden aber gewisse administrative Entscheidungen sind naturgemäß unabhängig davon zu treffen. Kapitel 3 gibt einen Überblick über die technischen Aspekte der Benutzerverwaltung.

Software: Sowohl das Betriebssystem selbst, wie auch Anwenderprogramme müssen upgedatet, neue Anwendungen installiert werden. Sehr wichtig ist das *Testen* all dieser Programme (auf verschiedener Hardware, in verschiedenen Systemumgebungen, etc.). Wir besprechen das Installieren von Software und das Package-Management unter Linux im Kapitel 4.

Aufgaben in der Systemadministration

- Benutzerverwaltung: Accounts anlegen und löschen
- Software: Installation und Upgrade
- Hardware: Wechsel der HW, Einbau, Kaufentscheidung
- Backup: wichtig!!!
- Systemmonitoring: Sicherheit und Performance
- Troubleshooting: Problem- und Fehlersuche und -behebung
- Benutzerbetreuung: Anfragen (Politik!)

Folie 1

Hardware muss erneuert und verändert werden. Die Aufgaben des Administrators reichen vom Einbau neuer Hardware in vorhandene Rechner über den Umbau von Hardware bis zur Integration neuer Rechner in ein Netzwerksystem. Außerdem sind Administratoren sinnvollerweise in die Kaufentscheidungen miteinbezogen.

Backup: Eine der langweiligsten aber wichtigsten Routineaufgaben in der Systemadministration ist das Erstellen, Überprüfen und Aufbewahren von Backups. Hier sind auch wichtige administrative Entscheidungen zu treffen. Wir befassen uns mit Backups in Kapitel 9.

Systemmonitoring: Der Administrator ist für das Funktionieren des Gesamtsystems verantwortlich. Um dies zu gewährleisten sind eine Reihe von Routineaufgaben notwendig, die das Überprüfen von Systemlogfiles, das Lesen der Rootmail, und das Überwachen von Systemdiensten im Hinblick auf Sicherheit und Performance inkludieren. Wir besprechen Aspekte und Tools des Systemmonitorings in Kapitel 5, Logging in Abschnitt 12.3, System- und Netzwerksicherheit in den Kapiteln 12 und 18.

Troubleshooting: Software und Hardware ist fehlerhaft. Die Aufgabe des Systemadministrators ist die Analyse und das Isolieren von auftretenden Problemen, um dann die richtigen Maßnahmen ergreifen zu können, zB das Einschalten der richtigen Experten (Hardwareservice, etc.). Oft ist das Aufspüren und Isolieren des Problems die eigentlich schwierige Aufgabe, die eine gute Kenntnis des Systems und seiner Funktionsweisen voraussetzt.

Benutzerbetreuung: Obwohl selten in der Arbeitsplatzbeschreibung eines Administrators zu finden, nimmt diese Tätigkeit oft den Löwenanteil der Arbeitszeit in Anspruch. Benutzerbetreuung hat viele „politische “ Aspekte und ist oft Hauptauslöser von Frustration und Überlastung von Systemadministratoren; siehe dazu Folie 2.

1.2 Allgemeine Strategien und Methoden

Im Rahmen einer Firma oder Organisation (zB Universitätsinstitut, Schule) die große EDV-Systeme für Verwaltungs- und/oder Lehrzwecke und/oder andere produktive Aufgaben betreiben, kommt Systemadministratoren eine ganz besondere Verantwortung im Bezug auf das Funktionieren der gesamten Infrastruktur zu. Computersysteme besitzen aufgrund ihrer rasanten Entwicklung und der immer schneller und weiter fortschreitenden Vernetzung über eine beträchtliche Eigendynamik. Die organisatorischen und rechtlichen Rahmenbedingungen innerhalb vieler Firmen und Organisationen können nicht Schritt halten und es entstehen Graubereiche und Unklarheiten.
Systemadministration findet in diesem Spannungsfeld statt. Erfahrungsgemäß wenden Systemadministratoren viel Zeit und Energie in diesem nicht technischen sondern „politischen“ oder sozialen Arbeitsfeld auf. Wir geben hier einen kleinen Überblick und verweisen auf die ausführlichen Überlegungen und Erfahrungsberichte zu diesem Themenkomplex im Kapitel 27 von [1].

Viele erfahrene Administratoren empfehlen eindringlich die schriftliche Niederlegung von Regeln und Verfahrensweisen. Diese *Regeln* (Policy) sollten vom Management der Organisation genehmigt und auch in ihren juristischen Dimensionen abgesichert sein. Bereiche in denen diese Regeln große Wichtigkeit haben sind auf Folie 3 aufgezählt.
Niedergeschriebene *Verfahrensweisen* oder Methoden (Procedure) für gewisse Eventualitäten und/oder Routineaufgaben der Systemadministration in Form von Rezepten dokumentieren einerseits die übliche Praxis und stellen andererseits deren Einhaltung sicher; sie Reduzieren die Wahrscheinlichkeit von Fehlern und setzten nachvollziehbare Standards. Eine Liste von Aufgaben, die so standardisiert werden sollten, finden sich auf Folie 4.

„Politik“

Sysadmin im Spannungsfeld

- Verantwortung für Infrastruktur
- Eigendynamik von Computersystemen
- Organisationsstrukturen
- Security

empfohlen

- niedergeschriebene Regel
- Übereinstimmung mit Management
- überprüfen rechtlicher Aspekte

Folie 2

Policy

feste Regelungen für

- verfügbare Services
- Rechte und Pflichten der User
- Rechte und Pflichten der Sysadmins
- Gastaccountvergabe
- ...

Folie 3

Darüber hinaus gibt es Fragen und Aufgaben, die genau zwischen Regeln und Methoden zu entscheiden/regeln sind; zB wer bekommt einen Account am System und was passiert, wenn diese Person die Organisation wieder verlässt? Das „Ob“ wird von den Regeln bestimmt, das „Wie“ von der Verfahrensweise. Die Tatsache, dass das gesamte Regelwerk schriftlich niedergelegt ist und Teile (etwa eine Benutzungsordnung) sogar mit Unterschrift bestätigt sind, garantiert die Konsistenz und Verbindlichkeit der Standards.
Besondere Relevanz und Brisanz erlangt diese klare Strukturierung im Bereich der *Sicherheit* (Security) von Computersystemen. Da sich die Sicherheit des Systems im Allgemeinen indirekt proportional zur Bequemlichkeit der Benutzung und zur Zahl und Qualität der angebotenen Services verhält, ist hier ein besonderes Spannungsfeld gegeben (vgl. Kapitel 12).

Auch im Bereich der *Benutzerbetreuung* – der in der Praxis sehr zeitaufwendig und nervenaufreibend ist – ist eine niedergeschriebene Policy Gold wert. Es sollte genau geklärt werden, welche Services und welcher Support den Usern zusteht und was von den Systemadministratoren *nicht* erledigt wird/werden muss. Weiters sollte klargestellt werden, in welcher Form Useranfragen an die Administratoren herangetragen werden müssen, bzw. welche Information eine Anfrage mindestens beinhalten muss, um bearbeitet zu werden. Anfragen der Art: „Was habt ihr denn wieder gemacht; mein Computer geht schon wieder nicht!“ sind nicht nur ärgerlich, sondern tragen auch nicht zur effizienten Problembearbeitung bei. Anfragen sollten immer mindestens die folgende Informationen beinhalten müssen: Auf welchem Host tritt bei welchem Benutzer welches Problem auf? Wie heißt die genaue Fehlermeldung, falls eine auftritt? Ist das Problem reproduzierbar? Wie wichtig ist die sofortige Problembehebung? Es bietet sich zB an, nur Anfragen über ein standardisiertes Webformular entgegenzunehmen.

Zum Abschluss verweisen wir noch Explizit auf die Abschnitte 27.3 und 27.8 in [1] für eine statistische Untersuchung über die realen Arbeitsbedingungen von Systemadministratoren sowie für „War Stories and Ethics“.

Procedure

Verfahrensweisen in Rezeptform

- Dokumentation und Standards
- weniger Fehler, mehr Konsistenz

für folgende Situationen

- Anlegen neuer Benutzer
- Einbinden neuer Hosts
- Sicherheitskonfiguration
- Backup und Restore
- Upgrade und Installation von Software
- Security Alarm, Notfälle
- Recovery from Desaster
- ...

Folie 4

1.3 Rootzugang

Jedes Unix-System verfügt über einen Administratoraccount, den sogenannten *Rootaccount* (Login: root), der durch die UID 0 (User Identity; siehe Kapitel 3) definiert ist. Dieser ist mit besonderen Privilegien und Rechten am System ausgestattet (siehe Folie 6), die das Erledigen aller administrativen Tätigkeiten, die Konfiguration des Systems, das (De)Installieren von Systemsoftware und vieles andere mehr ermöglicht. Für root gelten keine Dateiberechtigungen, root kann Dateibesitzer und Prozessbesitzer ändern und (ohne Passwort) auf jedem Account einloggen. Root „kann im Wesentlichen alles“, außer dem offensichtlich Unmöglichen, d.h. jede gültige Operation an einer Datei oder einem Prozess vornehmen.

Aus dieser (notwendigen) „Allmacht“ des Rootaccounts ergibt sich sowohl eine große *Verantwortung*, wie auch ein hohes *Gefahrenpotential*. Root kann alle Dateien auf dem System lesen zB auch die Email aller Benutzer. Dies ist sinnvoll, um etwa nach Viren in Mailattachments zu scannen. Andererseits verbietet (nur) die Etikette und sein Verantwortungsbewusstsein root die Mail anderer zu lesen.
Natürlich birgt die Verwendung der Rootaccounts vor allem durch ungeübte oder gar böswillige Hände vielfältige Gefahren in sich. Root kann zB alle Dateien auf den Festplatten löschen oder gar die Platten formatieren. Daher gilt vor allem für Anfänger in der Systemadministration: „Sit on your hands before you press ENTER!“ Da aber natürlich auch erfahrenen Administratoren Fehler unterlaufen (können), sollte der Rootaccount sehr sparsam und wirklich *nur (!)* zur Systemadministration verwendet werden, also *nur dann, wenn es unbedingt erforderlich ist*. Es ist nicht nur schlechter Stil, sonder äußerst gefährlich, wenn der Administrator gewohnheitsmäßig statt (s)eines eigenen (normalen) Benutzeraccounts den Rootaccount verwendet.

Der Rootaccount

- Account des Systemadministrators
- definiert durch User Identity (UID) = 0
- „allmächtig“
- große Verantwortung
- gefährlich in ungeübten oder böswilligen Händen
- sparsame Verwendung; **nur** wenn wirklich nötig!!!

Folie 5

Rootrechte

jede gültige Operation an einer Datei oder einem Prozess vornehmen

- Dateiberechtigungen gelten für root nicht
- kann Dateibesitzer ändern
- Prozessbesitzer ändern
- Runlevel ändern
- Hostnamen setzen
- Netzwerkgeräte konfigurieren
- Systemzeit setzten
- Devicefiles erzeugen
- negative Nicewerte setzen
- ...

"Sit on your hands before you press ENTER!"

Folie 6

Neben der äußerst sparsamen Verwendung des Rootaccounts sollte ein Rootlogin weder auf der grafischen Oberfläche (manche Systeme (zB SuSE 7.2) warnen explizit beim Login davor) noch direkt auf einer Textkonsole erfolgen. Der Grund dafür ist, dass dann im Logfile `/var/log/messages` nur die Tatsache vermerkt wird, dass root eingeloggt hat; es ist aber nicht ersichtlich, *wer* als root eingeloggt hat. Stattdessen sollte (jeder) der Administrator(en) zunächst unter seinem eigenen (normalen) Benutzeraccount einloggen und dann mittels des Kommandos `su` (Switch User) auf dem Rootaccount einloggen. Dabei wird natürlich das Rootpasswort abgefragt. Im Logfile wird dann eingetragen, welcher Benutzer das `su`-Kommando ausgeführt hat (vgl. Folien 8, 9).
Bei Verwendung der Syntax `su -` gelangt man in ein Root-Loginshell, also mit dem in `/root/.bahsh_profile` festgelegten Environment (inklusive richtigem Suchpfad; vgl. Teil 1, Abschnitt 6.2). Dem `su`-Kommando kann als optionales Argument ein Username übergeben werden (der Default ist also root) um in den Account des entsprechenden Users einzuloggen. `su` fragt nach dem Passwort des Accounts außer, wenn root das Kommando ausführt; so kann root in jeden beliebigen Account einloggen. Auf vielen Systemen ist als Schutzmaßnahme die Verwendung des `su`-Kommandos auf die Benutzergruppe `wheel` beschränkt (mittels PAM-Konfiguration; siehe Abschnitt 12.2), sodass die Accounts aller Administratoren zu dieser Gruppe gehören müssen.
Logins als root über ein Netzwerk sollten (wenn überhaupt) nur mittels Secure Shell (`ssh`) erfolgen. Wird ein webbasiertes Konfigurationstool (Webmin, Linuxconf; siehe Kapitel 2) benutzt, sollte unbedingt eine SSL-Unterstützung (Secure Socket Layer) verwendet werden, die einen verschlüsselten Datentransfer erlaubt.

Oft wird der Rootaccount als Gruppenaccount verwendet, d.h. mehrere Personen (Administratoren) kennen das Rootpasswort. In diesem Fall ist es aus mehreren Gründen (Fehlersuche, etc.) wichtig zu wissen, wer als root eingeloggt war (für die praktischen Aspekte siehe voriger Absatz). Eine gute Methode, um in dieser Situation nicht den Überblick zu verlieren wer was getan hat, ist das Führen eines „Logbuchs". Jeder Administrator muss vor dem Ausloggen als root in der Logbuchdatei (zB

`/root/LogBook`) eintragen, warum er als root eingeloggt war und was er getan hat. Eventueller Nachlässigkeit kann mittels eines Eintrags `vi /root/LogBook` in `/root/.bash_logout` abgeholfen werden.

Unter Unix ist es generell nicht möglich Rootrechte abgestuft zu vergeben, d.h. es gibt keinen Account, der etwa „halbe“ Rootrechte besitzt; das Unix-Sicherheitskonzept ist „binär“; entweder man darf „alles“ (root) oder „nichts“ (normaler Benutzer). Abhilfe schafft hier ein Tool namens `sudo`, das es erlaubt gewissen Benutzer(gruppen) das Ausführen gewisser Befehle als root zu gestatten, ohne das Rootpasswort abzufragen; es wird lediglich das Passwort des Benutzers abgefragt, um Missbrauch zu verhindern. So kann etwa einem Mitarbeiter die Möglichkeit eingeräumt werden, Backups zu machen oder Benutzeraccounts anzulegen, ohne dass er im Besitz des Rootpassworts sein muss. Neben einer sehr detailliert abgestuften Konfiguration ermöglicht `sudo` das Mitloggen aller ausgeführten Befehle, sodass immer ersichtlich ist, wer wann was getan hat. Für weitere Informationen siehe `http://www.sudo.ws`; leider ist das `sudo`-Paket nicht Bestandteil aller Linux-Distributionen.

Klarerweise kommt beim Schutz des Rootaccounts dem Rootpasswort ganz besondere Bedeutung zu. Alle Regeln für eine gute Passwortwahl (vgl. Teil 1, Abschnitt 3.1) sollten hier genau befolgt werden. Das Rootpasswort sollte in unregelmäßigen, unangekündigten Abständen geändert werden. Auf verschiedenen Systemen sollten verschiedene Rootpasswörter verwendet werden. Weiters sollte das Rootpasswort geändert werden, wenn immer der Verdacht besteht, dass die Sicherheit des System kompromittiert wurde und wenn einer der Administratoren, der im Besitz des Passworts ist, die Organisation verlässt.

Root Login

- **nur** wenn wirklich nötig
- **nicht** unter X Window
- **nicht** direkt auf der Konsole
- **nicht** über unsichere Netzwerkverbindung
- **richtig:**
  - lokal: `su`-Kommando
  - remote: `ssh`,
    SSL bei webbasierten Tools

Folie 7

Switch User (su)

```
[roland@pablo roland]$ whoami
roland
[roland@pablo roland]$ su
Password:
[root@pablo roland]# whoami;pwd
root
/home/roland
[root@pablo roli]# echo $PATH| grep sbin
[root@pablo roli]# exit
[roli@pablo roli]$ su -
Password:
[root@pablo root]# whoami;pwd
root
/root
[root@pablo root]# echo $PATH
/bin:/sbin:/usr/bin:/usr/sbin:
/usr/local/bin:/usr/local/sbin:
/usr/bin/X11:/usr/X11R6/bin:/root/bin
[root@pablo root]#
```

Folie 8

Rootlogin – Logeintrag

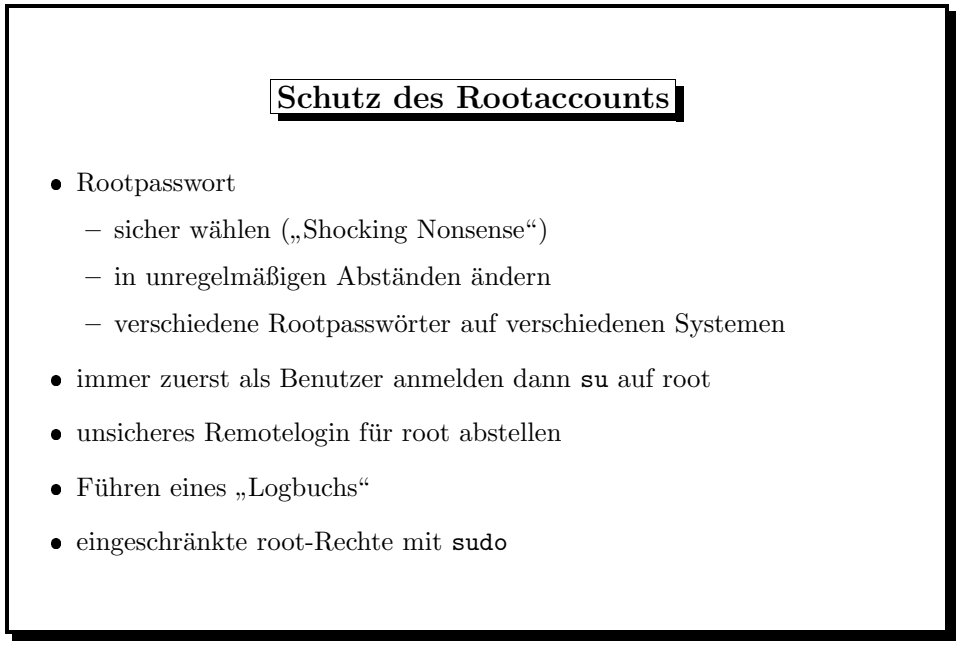
- falsch: auf Konsole oder unter X

```
$ tail /var/log/messages
Mar  9 11:06:20 pablo login(pam_unix)[1021]: session
                opened for user root by LOGIN(uid=0)
Mar  9 11:06:20 pablo  -- root[1021]: ROOT LOGIN
                ON tty4
```

- richtig: `su`

```
$ tail /var/log/messages
Mar  9 11:06:44 pablo su(pam_unix)[6341]: session
                opened for user root by roli(uid=500)
```

Folie 9



Folie 10

2 Administrationstools

In diesem Kapitel geben wir einen groben Überblick über die grundlegenden Methoden der Systemkonfiguration. Neben den wichtigsten Methoden – dem Editieren der entsprechenden Konfigurationsdateien und dem Erstellen und Modifizieren der Konfiguration mittels Shellscripts – stehen unter Linux verschiedene Administrationstools zur Verfügung. Wir behandeln kurz die distributionsunabhängigen Tools Linuxconf und Webmin, sowie einige distributionsspezifische Administrationsprogramme.

2.1 Systemkonfiguration

Generell ist unter Unix (beinahe) die gesamte Konfiguration des Systems in *Textdateien* gespeichert; der kleinste gemeinsame Nenner jeder Konfigurationsarbeit an Unix-Systemen das Editieren von ASCII-Dateien. Daher ist für Systemadministratoren die Beherrschung eines Editors ebenso unerlässlich, wie die gute Beherrschung (zumindest) einer Shell.
Eine besondere Rolle spielt hier der vi-Editor, der auf praktisch allen Unix Systemen zur Grundausstattung gehört und auch in jedem Notfall zur Verfügung steht. Wir empfehlen daher jedem angehenden Administrator unbedingt zumindest die Grundbedienung des vi zu erlernen. Ein guter Kompromiss ist hier der `gvim`-Editor, eine graphische vi-Version, die zwar das „vi-Feeling“ vermittelt aber auch über Menüs bedienbar ist (siehe auch Teil 1, Kapitel 5).

Weiters spielen *Shellscripts* eine entscheidende Rolle in der Systemkonfiguration; weitaus die meiste Konfigurationsarbeit an Unix-Systemen wird über Shellscripts erledigt. Das Lesen, Verstehen und Modifizieren vorhandener Scripts sowie das Schreiben eigener Shellscripts gehört daher zur alltäglichen Arbeit eines Systemadministrators. Am weitesten verbreitet ist die `sh`-Scriptsprache, die auch in der Linux-Standardshell `bash` implementiert ist. Wir erklären die Grundlagen der Bashprogrammierung in Kapitel 11.
Für größere Projekte empfiehlt sich auch die Scriptsprache *Perl*. Diese bietet mehr Flexibilität als die `sh`-Sprache und besitzt viele Charakteristika, die sich besonders für die Systemkonfiguration eignen. Eine Einführung in Perl findet sich zB in [8].

Der Großteil der Systemkonfigurationsdateien in vielen Unix-Systemen ist im Verzeichnis `/etc/` (manchmal auch `/adm/` oder `/var/adm/`) und seinen Unterverzeichnissen gespeichert. Beispiel dafür ist zB die Datei `/etc/inittab`, die das Verhalten des Initprozesses bestimmt und die Initscripts in AT&T-artigen Systemen (die dem System V Standard folgen; unter ihnen die meisten Linux-Distributionen) in `/etc/init.d/`, die die meisten Systemdienste starten (siehe Teil 1, Kapitel 9).

Der genaue Pfad verschiedener Konfigurationsdateien variiert allerdings stark zwischen den verschiedenen Unix- und auch Linux-Varianten. Unter RedHat zB wird das Verzeichnis `/etc/sysconfig/` verwendet, um dort in einzelnen Dateien wichtige Parameter für einzelne Komponenten der Konfiguration des Gesamtsystems (zB Netzwerk, Systemzeit, ...) zu speichern.
Unter SuSE wird ein anderes Schema verwendet. Es gibt eine (große) globale Konfigurationsdatei `/etc/rc.config`, in der faktisch alle Parameter gespeichert werden. Ein eigener Dienst (rc.SuSEconfig) wertet diese Datei aus und schreibt die Parameter in die (vielen) eigentlichen Konfigurationsdateien, die dann von den entsprechenden Prozessen gelesen werden.

Systemkonfiguration

- gesamte Unix-Konfiguration in Textdateien gespeichert
  - Beherrschung eines Editors (`vi` !)
  - Beherrschung der Kommandozeile
- meiste Konfigurationsarbeit durch Scripts erledigt
  - Beherrschung der `sh`-Scriptsprache
  - Für größere Projekte: Perl

Folie 11

Konfigurationsdateien

- meist in `/etc/` und Unterverzeichnissen
  manchmal `/adm/`, `/var/adm/`, ...
- viele Unterschiede zwischen Unix-Varianten
  und auch den einzelnen Linux-Distributionen
- RedHat: einzelne Dateien in `/etc/sysconfig/`
  zB `network, keyboard, mouse`, ...
- SuSE: globale Datei `/etc/rc.config`
  Dienst `rc.SuSEconfig` erstellt einzelne Dateien

Folie 12

2.2 Administrationswerkzeuge

Neben der für den Systemadministrator unerlässlichen Beherrschung der entsprechenden Unix/Linux-Befehle an der Kommandozeile bietet Linux die Möglichkeit verschiedene (großteils graphische) Konfigurationsprogramme zu Hilfe zu nehmen. Diese erlauben menügesteuert Änderungen an der Systemkonfiguration vorzunehmen; im wesentliche schreiben sie die entsprechenden Konfigurationsdateien und (re)starten die jeweiligen Services und Daemonen. Obwohl es für den Administrator wichtig ist die einzelnen Konfigurationsdateien und zumindest ihre grundsätzliche Syntax zu kennen und sie per Hand editieren zu können, erleichtern es die nun vorzustellenden Programme dem Einsteiger einen Überblick zu bekommen und gewisse Konfigurationsarbeiten zu erlernen.

Es gibt verschiedene Administrationsprogramme, die für beliebige Linux-Distributionen verwendet werden können; zB Linuxconf und Webmin. Darüber hinaus besitzen manche Distributionen eigene Administrationstools, die auf die Verwendung mit ebendieser Distribution zugeschnitten sind. Paradebeispiel ist YaST („Yet another Setup Tool“) von SuSE.

Linuxconf
ist ein mächtiges Tool, das für (fast) alle Konfigurationsarbeiten am System herangezogen werden kann. Es wurde ursprünglich von *Jacques Gélinas* entwickelt; die Projekthomepage findet sich unter `http://www.solucorp.qc.ca/linuxconf/`. Linuxconf besitzt eine modulare Struktur, d.h. für jede Konfigurationsaufabe (zB Konfiguration eines bestimmten Serverdienstes) ein eigenes Interface, das die entsprechenden Tasks übernimmt. Dadurch ist Linuxconf sehr flexibel und leicht erweiterbar. Linuxconf ist Bestandteil vieler Distributionen; RedHat beabsichtigt aber, Linuxconf in Zukunft nicht mehr in die Distribution aufzunehmen.

Administrationstools

- distributionsunabhängig
  - Kommandozeile (natürlich...)
  - Linuxconf (Konsole, graphisch, Netzwerkinterface)
  - Webmin (Netzwerkbasiert)
- distributionsspezifisch
  - YaST, YaST2 (SuSE)
  - Lisa (Caldera)
  - (c)kontrol-panel (RedHat)
  - ...

Folie 13

Linuxconf

- mächtiges Konfigurationstool
- praktisch für das ganze System
- geschrieben und gewartet von Jacques Gélinas
- Homepage `http://www.solucorp.qc.ca/linuxconf`
- verwendet übersichtliche Baumstruktur

Folie 14

Linuxconf darf nur von root benutzt werden und kennt vier Betriebsarten: Das *Kommandozeileninterface* ist vor allem für die Verwendung in Scripts konzipiert. Auf der Textkonsole kann ein *„Zelleninterface“*, im X Window ein entsprechendes *graphisches Interface* verwendet werden. Schließlich stellt Linuxconf auch einen *netzwerkbasierten Modus* zur Verfügung. Damit ist es möglich, sich mit dem Webbrowser ihrer Wahl mit Linuxconf zu verbinden und nach Abfrage des Rootpassworts die Konfigurationsarbeit durchzuführen.

Praktisch sieht die Verwendung von Linuxconf (mit Ausnahme des Kommandozeileinterfaces) vor, zuerst durch die in einer baumartige Struktur aufbereiteten Konfigurationspunkte zu browsen und in den entsprechenden Menüs die Änderungen einzutragen. Dann kann man mittels „Preview“ sehen, welche Änderungen (schreiben von Konfigurationsdateien, Neustarten von Services) ausgeführt werden müssen, um die angestrebte Konfiguration zu erreichen. Schließlich kann man diese Tasks ausführen lassen. Linuxconf schreibt alle von ihm ausgeführten Änderungen in der Datei `/var/log/netconf.log` mit.
Das Linuxconf-Webinterface ist standardmäßig aus Sicherheitsgründen deaktiviert, kann aber mittels Linuxconf selbst aktiviert werden. Es muss allerdings auch der Internetdaemon `(x)inetd` am System laufen um das Webinterface verwenden zu können. Man kann sich dann mit einem beliebigen Webbrowser auf Port 98 (`http://myhost.mydomain:98`) verbinden. Fraglich bzw. eine Geschmacksfrage ist, ob ein Webbrowser das geeignete Tool zur Systemadministration ist; vor allem sicherheitsrelevante Fragen sind hier zu beachten. Es lässt sich zwar festlegen, von welchen Hosts aus das Interface benützt werden darf, um aber das Rootpasswort verschlüsselt über das Netz zu versenden, muss erst ein Webserver mit Unterstützung für SSL (Secure Socket Layer) aufgesetzt werden (Details unter `http://www.terminator.net/linuxconf/linuxconf-ssl.html`). Außerdem muss man beachten, dass die meisten Webbrowser Passwörter speichern, also ein unberechtigter Benutzer eventuell durch Betätigen des „Zurück“-Buttons des Browsers auf die Linuxconf-Seite gelangen kann.

Linuxconf verwenden (1)

- nur root !
- 4 Betriebsarten
  - Kommandozeile (Scripts!)
  - Charakterzellen (interaktiv, textbasiert)
  - X-Window-basiert (interaktiv, GUI)
  - Netz-basiert (interaktiv, remote)
- Logfile `/var/log/netconf.log`

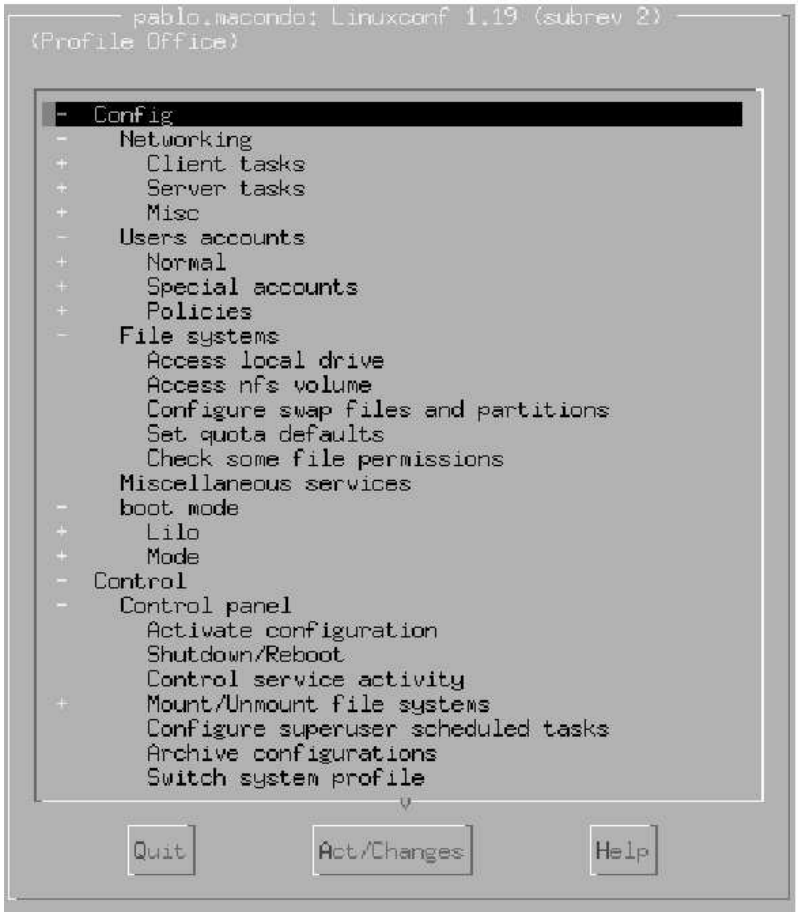
Folie 15

Linuxconf verwenden (2)

- browse Linuxconf-Baum
- mache Änderungen
- Vorschau auf Änderungen
- Aktiviere Änderungen
- verlassen

Folie 16

Linuxconf-Zelleninterface



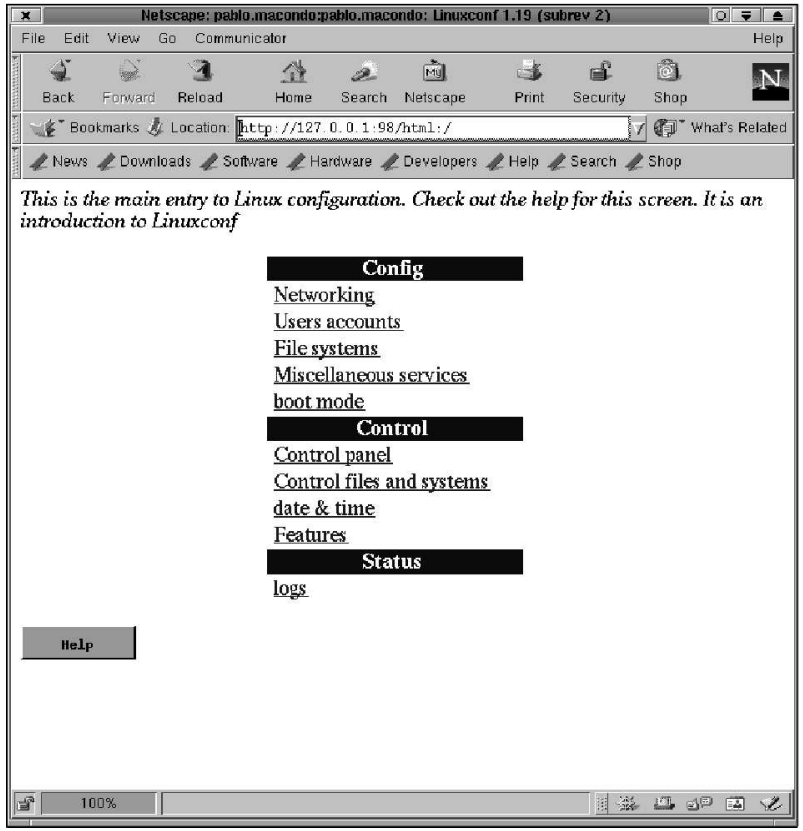
Linuxconf-GUI

Linuxconf-Netzwerkinterface

- standardmäßig deaktiviert
- einschalten:
  Config; Network; Misc; Linuxconf Net Access
  Internetdaemon (`(x)inetd`) muss laufen
- erreichbar am Port 98 (`http://myhost.mydomain:98`)
- Sicherheit!!!
  Hostaccess, verschlüsseltes Passwort, Browser speichert Passwort

Folie 17

Linuxconf-Webinterface



Webmin
ist ein relativ neues, netzwerkbasiertes Tool zur Systemadministration. Es verbindet einen modularen Aufbau mit dem Konzept einer plattformübergreifenden graphischen Administrationsoberfläche. Webmin unterstützt alle wichtigen Unix-Versionen, ist aber zB in der aktuellen RedHat-Distribution nicht enthalten. Rpm-Pakete kann man aber von der Webmin Homepage `http://www.webmin.com` herunterladen und sind problemlos installierbar. Für die Benutzung von Webmin gilt Ähnliches wie für das Netzwerkinterface von Linuxconf: der Server ist mit einem beliebigen Webbrowser auf dem Port 10000 (also unter `http://myhost.mydomain:10000`) erreichbar. Eine SSL-Unterstützung muss „per Hand“ eingebaut werden (siehe dazu `http://www.webmin.com/webmin/ssl.html`).

Neben diesen distributionsunabhängigen, bzw. distributionsübergreifenden Konfigurationstools stellen einige Distributoren eigene, auf genau diese Distribution zugeschnittene Werkzeuge zur Verfügung. Beispiele hierfür sind folgende

Distributionsspezifische Tools

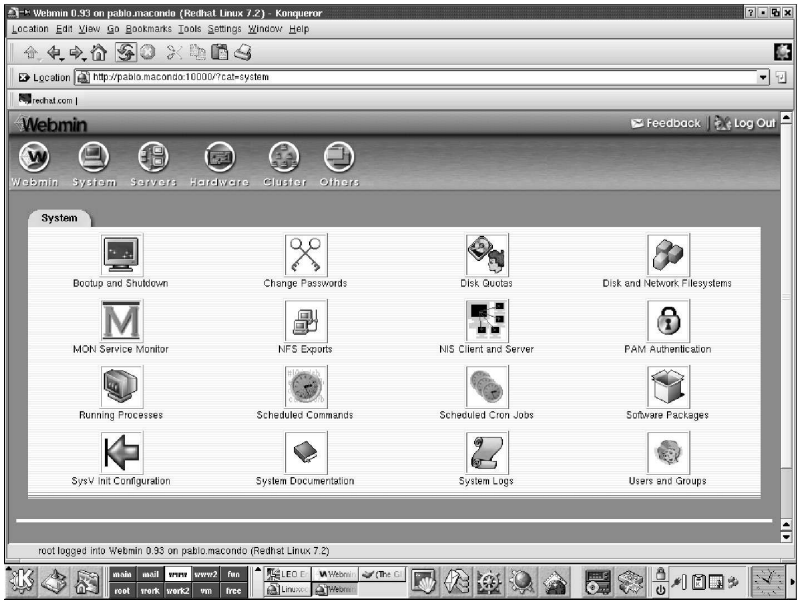
- *YaST* („Yet another Setup Tool“) bzw. YaST2 ist das Administrationswerkzeug von SuSE, das eine einfache Installation und Administration dieser Distributionen ermöglicht. YaST kann in anderen Distributionen nicht verwendet werden und ist nicht (einfach) erweiterbar. Andererseits ist es schwierig, SuSE-Distributionen ohne YaST zu konfigurieren; YaST schreibt das globale Konfigurationsfile `/etc/rc.config` und erzeugt mittels Aufrufs von `rc.SuSEconfig` daraus die entsprechenden Konfigurationsdateien für die Dienste. Händisch editierte Dateien werden dabei überschrieben, sodass jede Konfigurationsarbeit außerhalb von YaST sehr erschwert wird.

Webmin

- webbasiertes Konfigurationstool
- unterstützt neben Linux alle wichtigen Unix-Versionen
- Open Source (BSD Open Source License)
- modulare Struktur
- plattformunabhängige Konfigurationsumgebung

Folie 18

Webmin



- *Lisa* ist das Administrationstool von Caldera Open Linux und ebenfalls nur für diese Distribution verwendbar.
- Debian verwendet für mehrere Aufgaben kleine spezialisierte Tools, zB `modconf`, `tzconfig`, `rconf`.
- *Control-panel* ist ein graphisches Administrationstool für RedHat-Linux, kann aber auch unter Mandrake, Turbo Linux und einigen anderen Distributionen verwendet werden. Seit RedHat-7.2 wird es allerdings nicht mehr unterstützt und es gibt nur nur mehr seine KDE-Version `kontrol-panel`. Das k(c)ontrol-panel stellt einen graphischen Launcher für verschiedene Tools zur Verfügung. Vor dem Start des entsprechenden Tools wird das Rootpasswort abgefragt.

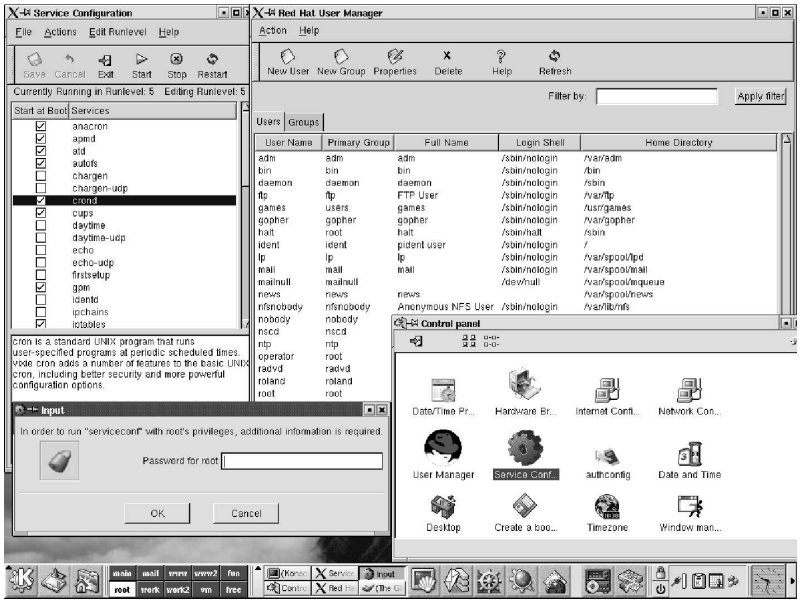
Darüber hinaus integrieren manche Distributionen verschiedene grafische Tools zur Systemadministration in die Desktopsysteme KDE und Gnome, die meist über das Startmenü und das Untermenü „System“ aufrufbar sind.
Ein Beispiel ist etwa unter RedHat das KDE Tool zu Benutzerverwaltung `kuser`. Unter SuSE ist Yast2 bzw. seine Module über KDE- oder Gnome Menüs erreichbar.

Distributionsspezifische Tools

- YaST, YaST2 (SuSE)
- Lisa (Caldera Open Linux)
- (c)kontrol-panel (RedHat, Mandrake, ...)
  - Systemdienste (Runlevel Editor)
  - Zeit
  - Netzwerk
  - Modem oder ISDN Anschluss
  - Usermanager
  - Authentifizierung

Folie 19

Kontrol-panel



3 Benutzerverwaltung

In einem Multiuser-Betriebssystem verfügt jeder Benutzer über einen von anderen Usern getrennten Bereich, wo er persönliche Daten und Einstellungen für die von ihm benutzten Programme ablegen kann. Dieser Bereich (das Heimat- oder Homeverzeichnis) zusammen mit Informationen über den Benutzer, wie etwa Benutzername, Passwort, Gruppenzugehörigkeit, Loginshell etc., die in globalen Konfigurationsdateien gespeichert sind, definiert einen „Benutzer-Account“. In diesem Kapitel beschreiben wir, wie Accounts angelegt, verwaltet und gelöscht werden.

3.1 Accountinformationen

Wichtige Informationen zu jedem Account befinden sich in den drei Dateien `/etc/passwd`, `/etc/group` und (meistens) `/etc/shadow`, deren Inhalt und Syntax wir nun im Detail erklären.

Die *Passwortdatei* `/etc/passwd` enthält grundlegende Informationen zu allen Accounts. Jede Zeile in der Datei definiert einen Account und ist in sieben durch Doppelpunkte separierte Felder unterteilt. Im 1. Feld ist der Benutzername (Accountname oder Loginname) gespeichert, das 2. Feld ist das das Passwortfeld. In den weiteren Feldern sind UID, GID, die GECOS-Information, das Homedirectory und die Loginshell angegeben.

Benutzernamen unter Unix haben üblicherweise maximal 8 Buchstaben und sind durchgehend klein geschrieben; prinzipiell sind Benutzernamen zwar case-sensitive, aber verschiedene Programme (zB der Mailserver Sendmail) setzen Kleinschreibung der Accountnamen voraus. Die Accountnamen sollten leicht zu merken sein und einfach mit dem Namen des Benutzers assoziiert werden können (Vorname, Nachnamen, Kombination aus beiden, etc.) und sollten (um Konflikte mit älterer Software zu vermeiden) nur aus alphanumerischen Zeichen bestehen.

Acounts

Was ist ein Account?

- Daten des Benutzers
  - Texte, Tabellen, Bilder, Mail, ...
  - persönliche Konfigurationen
    zB der Desktopsysteme, Netscape, Mailreader, ...
- Informationen über den Benutzer
  - Loginname, Passwort, Gruppenzugehörigkeit, ...
  - gespeichert in globalen Konfigurationsdateien
    - `etc/passwd`
    - `/etc/group`
    - `/etc/shadow`

Folie 20

Das *Passwortfeld* dient zur Speicherung des *verschlüsselten* Passworts. Oft wird allerdings aus Sicherheitsgründen das Passwort nicht in der Passwortdatei, sondern in `/etc/shadow` gespeichert (siehe unten). Unix verwendet standardmäßig DES-Verschlüsselung, die allerdings nur eine Passwortlänge von (unverschlüsselt) 8 Zeichen erlaubt; längere Passwörter werden zwar akzeptiert; es sind aber nur die ersten 8 Stellen signifikant. Verschlüsselten DES-Passwörter sind unabhängig von der Länge des unverschlüsselten Passworts 13 Zeichen lang. Die meisten Linux-Distributionen unterstützen auch MD5-verschlüsselte Passwörter. Hier ist die unverschlüsselte Länge mit 31 Zeichen limitiert, die verschlüsselten beginnen immer mit der Zeichenfolge 1. Da die Länge der Passwörter signifikant die Möglichkeit erfolgreicher Wörterbuchattacken beeinflusst, sollten unter Linux MD5 Passwörter verwendet werden. Einzige Ausnahme sind Systeme, wo Kompatibilität mit älteren Unix-Varianten gewahrt bleiben muss (zB NIS mit Linux und DEC Rechnern), die nur DES-Verschlüsselung unterstützen. Passwörter können mittels des Kommandos `passwd` geändert werden. Alle Benutzer außer root werden dabei aber nach dem alten Passwort des entsprechenden Accounts gefragt. Root kann also (als einziger) neue Passwörter setzen, ohne die alten zu kennen; die unverschlüsselten Passwörter kennt selbst root nicht.
Systemintern wird jeder Account durch eine eindeutige Zahl (32 Bit Integer), die *User Identity (UID)* repräsentiert, die im 3. Feld der Passwortdatei angegeben ist. Unter Linux können derzeit 65535 UIDs vergeben werden (limitiert durch die Länge des UID-Feldes im ext2 Filesystem; diese Zahl wird aber zukünftig noch steigen). Das System kennt nicht nur die „normalen“ Accounts (*Useraccounts*), die Benutzern die normale Verwendung des Systems ermöglichen, sondern sogenannte *Systemaccounts*. Der wichtigste von ihnen ist der *Rootaccount*, der Account der Systemadministrators. Dieser hat in allen Unix-Varianten die UID 0, sein Eintrag befindet sich in der ersten Zeile von `/etc/passwd`. Darüber hinaus laufen einige Systemdienstprogramme und Daemonen unter eigenen Accounts (auch privilegierte Pseudobenutzer genannt), um etwa Daten in einem reservierten Bereich ablegen zu können, oder damit spezifizierte Rechte an die Prozesse vergeben werden können. Diese Systemaccounts verfügen über niedere UIDs (unter Linux unter 100)

und können (und sollen auch) nicht zum normalen Login am System verwendet werden. Die „normalen“ Benutzeraccounts verfügen über höhere UIDs, unter RedHat ab 401.
Die Accounts am System können in *Gruppen* zusammengefasst werden, damit bestimmte Rechte (etwa im Dateisystem) an mehrere Benutzer gleichzeitig vergeben werden können. Die Information über die Gruppenzugehörigkeiten der Benutzer sind in der Datei `/etc/group` (siehe unten) festgelegt. Die Gruppen werden analog zu den Accounts systemintern über eindeutige Nummern verwaltet, die sogenannte *Gruppen Identity (GID)*. Jeder Account am System muss mindestens einer Gruppe zugeordnet sein, seiner Primary oder Login Gruppe, die im 4. Feld der Passwortdatei eingetragen ist. In vielen Linux-Distributionen ist es Standard, für jeden Benutzer eine eigene Logingruppe zu verwenden, die denselben Namen wie der Accounts selbst hat und die GID gleich der UID des Accounts ist.
Das 5. Feld der Passwortdatei ist das sogenannte GECOS (oder GCOS) Feld. (Der Name ist historisch und rührt daher, dass dieses Feld in den Bell Labs dazu verwendet wurde, batch Jobs auf den GECOS Mainframe zu überragen.) Die Syntax des GECOS Feldes ist nicht in allen Unix-Varianten gleich. Üblicherweise wird der erste Eintrag der durch Beistriche separierten Liste als voller Name des Benutzers interpretiert, dann folgen Büroadresse, Bürotelefonnummer und Heimtelefonnummer. Das `finger`-Kommando wertete (unter anderem) das GECOS Feld der Passwortdatei aus, die Einträge können mit dem `chfn`-Befehl (passwortgesichert) verändert werden.

Die Passwortdatei `/etc/passwd`

jede Zeile ein Account, 7 doppelpunkt-separierte Felder

1. Benutzername (Account- oder Loginname)
2. Passwortfeld (DES oder MD5 verschlüsselt), oft Shadowpasswörter
3. UID (User Identity): 32 Bit Integer, max. 65535
4. GID (Group Identity): definiert Logingruppe
5. GECOS: voller Name, Adresse und Telefon
6. Homedirectory
7. Loginshell (`/etc/shells`)

Folie 21

Beispieldatei `/etc/passwd`

```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
mail:x:8:12:mail:/var/spool/mail:
ftp:x:14:50:FTP User:/pusers/ftp:
nobody:x:99:99:Nobody:/:
roland:x:401:401:Roland Steinbauer,Zi 407,,:/home/roland:/bin/bash
oliver:x:402:402:Oliver Fasching:/pusers/oliver:/bin/bash
flo:x:403:511:Florian Wisser:/pusers/flo:/bin/bash
test:x:500:8076::/home/test:/bin/bash
```

Folie 22

Das *Homedirectory* des Benutzers ist im 6. Feld der Passwortdatei gespeichert und heißt meistens `/home/username`. Ist das Homedirectory nicht vorhanden wird der Benutzer unter Linux auf der Textkonsole mit Homedirectory `/` eingeloggt, im graphischen Modus ist dann kein Login möglich.
Im 7. Feld schließlich wird die *Loginshell* festgelegt, d.h. jene Shell, in die der Benutzer unmittelbar nach dem Login gelangt. Unter Linux kann die Loginshell eines Benutzers (passwortgeschützt) mittels `chsh`-Befehl geändert werden. Erlaubt sind alle Shells, die in `/etc/shells` aufgelistet sind.

Die Passwortdatei muss für alle Benutzer am System lesbar sein, damit die hier gespeicherten wichtigen Informationen allen Benutzern, bzw. den von ihnen verwendeten Programmen zugänglich sind. Aus diesem Grund (vor allem um Wörterbuchattacken zu erschweren) werden in modernen Unix-Systemen die verschlüsselten Passwörter selbst in einer anderen Datei und nicht in `/etc/passwd` gespeichert. Besitzt ein Angreifer einmal ein verschlüsseltes Passwort, so kann er eines der verbreiteten Cracker-Programme verwenden, die eines ganzen Wörterbuches verschlüsseln und die so erhaltenen Strings mit den Passwörtern vergleichen. Sind die Passwörter schlecht oder zu kurz gewählt ist ein Knacken in wenigen Minuten bis Stunden möglich (einen entsprechend schnellen Rechner vorausgesetzt).

Daher wird auf modernen Unix-Systemen das Passwort zusammen mit einigen anderen passwortspezifischen Daten in der *Shadowdatei* `/etc/shadow` gespeichert; diese ist nur für root lesbar. Im 2. Feld der Passwortdatei ist dann ein „x“ eingetragen und man ist in der paradoxen Situation, dass in der Passwortdatei (fast) alles, außer dem Passwort selbst steht.
Die Syntax der Shadowdatei ist ähnlich der Syntax von `/etc/passwd`; jede Zeile beinhaltet die Einträge zu einem Account, die neun Felder sind durch Doppelpunkte getrennt. Der erste Eintrag ist der Benutzername und stellt so die Verbindung zwischen den entsprechenden Zeilen in der Passwort- und der Shadowdatei her.

Die Shadowdatei `/etc/shadow`

je Account eine Zeile
9 doppelpunkt-separierte Felder

1. Benutzername
2. verschlüsseltes Passwort
3. Letzter Passwortwechsel (Tage seit 1.1.1970)
4. Min. Tage zwischen Wortwechsel
5. Max. Tage zwischen Passwortwechsel
6. Anzahl Tage Warnung vor Passwortablauf
7. Anzahl Tage Accountablauf nach Passwortablauf
8. Accountablauf
9. Flags (unbenutzt)

Folie 23

Beispieldatei `/etc/shadow`

```
root:$1$D1233U6v$37fJ9VUFuLc6jX3df82MQ1:11635:0:99999:7:::
bin:*:11635:0:99999:7:::
daemon:*:11635:0:99999:7:::
shutdown:*:11635:0:99999:7:::
mail:*:11635:0:99999:7:::
ftp:*:11635:0:99999:7:::
nobody:*:11635:0:99999:7:::
roland:$1$RRO2LY5n$ertgHt0lnUhZYl0PdJ2uW1:11637:0:99999:7:::
oliver:$1$3HcA/1AK$1ZJs6DRHZRweqMTEJ8QKC0:11632:0:99999:7:::
flo:4liq2wkTRWbhJ:11619:0:99999:7:::134547972
test:$1$2759ACul$ozJrregreD1OAaxaQP8g0:11686:0:99999:7:::
```

Folie 24

Im 2. Feld der Shadowdatei steht das (verschlüsselte) Passwort; für die Verschlüsselung gilt dasselbe wie für Passwörter in `/etc/passwd`. Die Bedeutung der weiteren Felder, die alle optional sind, wird auf Folie 23 erklärt.

Um von einem System ohne Shadowpasswörter (also wo die Passwörter (noch) in `/etc/passwd` gespeichert sind) auf eines mit Shadowpasswörtern umzusteigen, gibt es das Tool `pwconv`, das aus `/etc/passwd` die entsprechende `/etc/shadow` erzeugt. Die umgekehrte Richtung bewältigt man mit `pwunconv`.

In größeren Systemen (zB Universitätsinstitut) entsteht rasch eine gewisse Notwendigkeit, Benutzer in *Gruppen* (zB Professoren, Assistenten, Studenten, Sekretariat, ...) einzuteilen. So kann man ein effektives Rechtekonzept entwickeln, um zB allen Sekretärinnen die Möglichkeit zu bieten, dieselbe institutsweite Email-Adresse zu verwenden. Studenten sollte es jedoch verboten sein, die Daten der Professoren (zB Prüfungstexte) zu lesen. Information über die Gruppen am System werden in `/etc/group` gespeichert.
Die Syntax dieser Datei ist ähnlich der Syntax von Passwort- und Shadowdatei. Jede Zeile definiert eine Gruppe, die vier Felder sind durch Doppelpunkte getrennt. Der erste Eintrag ist der Name der Gruppe; unter Linux wird meistens pro Benutzer eine eigene Gruppe angelegt (siehe oben). Es können aber auch darüber hinaus Gruppen definiert werden. Für die Gruppennamen gilt Ähnliches wie für die Loginnamen. Im 3. Feld wird die GID der entsprechenden Gruppe und im 4. Feld als kommaseparierte Liste die Mitglieder (resp. ihre Benutzernamen) der Gruppe eingetragen.
Ist ein User Mitglied mehrerer Gruppen, so bestimmt die Gesamtheit seiner Gruppenzugehörigkeiten (Groupset) seine Gruppenrechte im System. Der Befehl `groups` zeigt an welchen Gruppen ein Benutzer angehört. Neuerstellte Dateien werden immer mit Gruppenbesitzer gleich der Logingruppe verwendet, es sei denn, der Benutzer loggt mittels `newgrp my2ndgrp` in die Gruppe my2ndgrp ein; er bleibt als Benutzer eingeloggt, neue Dateien sind haben dann my2ndgrp als Gruppenbesitzer.

Mittels `newgrp` kann man (ohne Passwort) nur in Gruppen einloggen, deren Mitglied man ist. Es gibt prinzipiell die Möglichkeit den Login in Gruppen (wo der Benutzer nicht Mitglied ist) mit einem Passwort zu schützen. Das 2. Feld in `/etc/group` (oder `/etc/gshadow` analog zu `/etc/shadow`) enthält dann das verschlüsselte Gruppenpasswort. Dieser Mechanismus wird aber sehr selten verwendet; meist ist im 2. Feld von `/etc/group` ein „x“ eingetragen und der Login in Gruppen ohne Mitglied zu sein ist nicht möglich.

Die Gruppendatei `/etc/group`

Jede Zeile eine Gruppe; 4 doppelpunkt-separierte Felder

1. Gruppenname
2. Gruppenpasswort (selten verwendet)
3. GID
4. Gruppenmitglieder als kommaseparierte Liste

Folie 25

Beispieldatei `/etc/group`

```
root:x:0:root
bin:x:1:root,bin,daemon
daemon:x:2:root,bin,daemon
sys:x:3:root,bin,adm
mail:x:12:mail
ftp:x:50:
roland:x:401:
diana:x:500:roland,mike,migro,diana,gue,michael,irina
cc:x:501:flo,susanne,helpdesk,roland,herman
test:x:8076:roland,test
```

Folie 26

Ändern/Abfragen der Accountinformation

- `passwd` Passwort ändern
- `chsh` Loginshell ändern
- `chfn` GECOS Feld ändern
- `finger` Benutzerinfo abfragen
- `groups` Gruppenzugehörigkeit abfragen
- `newgrp` Gruppenlogin

Folie 27

3.2 Accountverwaltung

Einige Konfigurationsarbeiten an Accounts, die jeder Benutzer selbst durchführen kann (Ändern von Passwort, Loginshell, GECOS-Einträgen) haben wir im vorigen Abschnitt behandelt. Hier besprechen wir nun die dem Administrator vorbehaltenen Konfigurationsänderungen, im besonderen, das Anlegen, Sperren und Löschen von Benutzeraccounts.

Der kleinste Nenner bei der Accountverwaltung zwischen allen Unix-Systemen ist das direkte Editieren der Konfigurationsdateien `etc/passwd, /etc/shadow` und `/etc/group`. Dies sollte jedoch nicht mit einem gewöhnlichen Editoraufruf, sondern mittels Aufruf von `vipw`, `vigr` bzw. `vipw -s` (auf manchen Systemen für `/etc/shadow`) geschehen, die die Dateien für alle anderen Prozesse während des Editiervorgangs sperren. Als Standard wird dabei der `vi` Editor verwendet; dieses Verhalten kann durch setzten der Umgebungsvariable `EDITOR` verändert werden. Diese Art der Konfiguration der Useraccounts ist allerdings sehr gefährlich und wird(/sollte) nur in Ausnahmefällen verwendet (werden). Ein zu viel weggelöschter Doppelpunkt kann zB die gesamte Passwortdatei invalidieren, sprich: Niemand – auch nicht root – kann mehr einloggen. Daher empfiehlt es sich, nach dem Abspeichern von `/etc/passwd` und `/etc/shadow` und vor dem Ausloggen aus der root-Shell auf einer parallelen Konsole zu testen, ob root noch einloggen kann.

Neben dieser „low-level“ Methode stellen alle Unix-Varianten ähnliche Kommandozeilenwerkzeuge zur Benutzerverwaltung zur Verfügung. Unter Linux weit verbreitet sind `useradd` und `userdel` zum Erstellen bzw. Löschen von Useraccounts, analog dazu `gropuadd` bzw. `groupdel` und zum Ändern der Konfiguration eines Accounts bzw. einer Gruppe `usermod` und `groupmod`. Wir besprechen diese Utilities später jeweils im Kontext ihrer Funktionen.

Accountverwaltung

- User: Ändern der Accountinformationen
  (Passwort, Loginshell, GECOS)
- root:
  - Anlegen
  - Konfigurieren
  - Sperren
  - Löschen

  von Accounts

Folie 28

Editieren der Konfigfiles

- kleinster gemeinsamer Nenner auf allen Unix-Systemen
- statt normalem Editoraufruf (Locking!)
  - `vipw`
  - `vigr`
- Gefährlich! Tippfehler können ganze Datei invalidieren
  vor root-Logout testen!!!

Folie 29

Utilities

- Kommandozeilenwerkzeuge
  - Anlegen: `useradd, passwd, groupadd`
  - Konfig: `usermod, groupmod`
  - Löschen: `userdel, groupdel`
  - Automatisierung durch Skripts
- Grafische Tools
  YaST, Linuxconf, Webmin, Kuser, ...

Folie 30

In größeren (Netzwerk-) Systemen wird der manuelle Einsatz dieser einfachen Tools schnell zu umständlich und die Praxis zeigt, dass man (zB in unserem fiktiven Institutsnetz) ziemlich bald ein angepasstes (adduser-)Script zum Anlegen von Accounts schreibt, das einen neuen Benutzer gleich in eine netzwerkweite Benutzerdatenbank einträgt und bequem aus einer Liste von Arbeitsgruppen seine Gruppenzugehörigkeit aussuchen lässt, oder etwa 100 Standardaccouts (für ein PC-Labor) mit Zufallspasswörtern inklusive der entsprechenden Anmeldeformulare erstellt.
Außerdem stellen fast alle Linux-Distributionen grafische Werkzeuge zur Benutzerverwaltung zur Verfügung, die sich allerdings schlecht für die oben angesprochen Automatisierung eignen, also nur für kleine Systeme oder das manuelle Nachbessern einiger weniger Konfigurationen in einem großen System sinnvoll zu verwenden sind (vgl. Kapitel 2).

Accounterstellung
Vor allem bei größeren Systemen ist es auf jeden Fall sinnvoll, neue Benutzer vor der Accounterstellung über die Gepflogenheiten des Systems zu informieren. Weiters ist es dringend zu empfehlen, eine Benutzungsordnung schriftlich auszuhändigen und eine Kopie vom neuen Benutzer unterschreiben zu lassen. Für weitere Überlegungen zu Benutzerordnung und Policy siehe Abschnitt 1.2.

Unabhängig vom verwendeten Tool müssen bei der Accounterstellung prinzipiell folgende Vorgänge erledigt werden: Zunächst ist ein Eintrag in der Passwortdatei nötig, der die entsprechenden Informationen über den Benutzer enthält. Weiters wird ein Eintrag im Gruppenfile und (eventuell) im Shadowfile benötigt. Ein wichtiger Punkt ist das setzten des Anfangspasswort. Hier werden oft folgende zwei Vorgehensweisen verwendet: Entweder der neue Benutzer gibt sein Anfangspasswort selbst ein (muss dazu also persönlich bei der Accounterstellung anwesend sein) oder der Administrator übermittelt dem neuen User ein (standardisiertes) Anfangspasswort, dass dieser aber beim ersten Login (per Konfiguration erzwungen) ändern muss. Schließlich muss das Homedirectory für den neuen Account erstellt und (eventuell) eine Anzahl von Standardkonfigurationsdateien (zB `~/.bashrc`) angelegt werden. Auf Mailservern müssen noch

Mailhomedirectory (enthält die Inbox des Users) und eventuell Mailaliases gesetzt werden.

Bei Verwendung der Kommandozeilenwerkzeuge geht man zweckmäßiger Weise gemäß Folie 32 vor. Zunächst wird mit `useradd username` der Eintrag in Passwort-, Gruppen- und Shadowdatei erzeugt und das Homedirectory angelegt. Außerdem kopiert `useradd` alle Dateien aus `/etc/skel/` ins neue Homedirectory; dort sollte der Administrator also alle benötigten Standardkonfigurationsdateien speichern. Unter RedHat legt `useradd` standardmäßig zu jedem neuen Benutzer eine Gruppe mit gleichem Namen und GID=UID an. Nun existiert der Account zwar, aber es ist kein Passwort gesetzt und somit noch kein Login möglich. Das Anfangspasswort muss root nun mittels `passwd username` setzen. Gegebenenfalls sind nun noch mittels `groupadd` eine neue Gruppe hinzuzufügen oder mittels `groupmod` der neue Benutzer einer bereits bestehenden Gruppe zuzuordnen. Für alle weiteren Details und vor allem die distributionsspezifischen Defaulteinstellungen siehe die Manpages der entsprechenden Befehle bzw. die lokale Dokumentation.

Account anlegen

- Benutzungsordnung!!!
- Einträge in Passwort-, Gruppen- und Shadowdatei
- Anfangspasswort setzen
- Homedirectories erstellen
- Anfangskonfigurationsdateien erstellen
- ...

Folie 31

Accounterstellung (Kommandozeile)

- `useradd` erzeugt
  - Einträge in Passwort-, Gruppen (Logingr.)- und Shadowdatei
  - Homedirectory
  - Anfangskonfigurationsdateien aus `/etc/skel/`
- `passwd` Anfangspasswort setzten
- `groupadd, groupmod` für weitere Gruppenzugehörigkeit

Folie 32

Accountkonfiguration
Neben den Konfigurationsarbeiten am Account, die der Benutzer selbst vornehmen kann, hat der Administrator die Möglichkeit alle Accountdaten zu verändern; dazu sind die Kommandozeilenwerkzeuge `usermod` und `groupmod` gedacht, die die entsprechenden Einträge in `/etc/passwd` und `/etc/shadow` bzw. in `/etc/group` modifizieren. Insbesondere können so Ablaufdatum des Accounts, Homedirectory und sogar der Name des Accounts geändert werden; letzteres ist allerdings nur dann möglich, wenn der entsprechende Benutzer keine Prozesse am System laufen hat.

Die Defaultwerte für die Usererstellung werden in der Datei `/etc/login.defs` festgelegt; eine Beispieldatei befindet sich auf Folie 33. Insbesondere werden hier die in `/etc/shadow` gespeicherten Einträge über erzwungene Passwortänderung und Vorwarnzeit festgelegt, wie auch die Mindestlänge des Passworts (für root nicht bindend) und die Bereiche für die automatisch fortlaufende UID und GID Erstellung.
Weitere Einstellungen zur Beschaffenheit des Passworts (etwa Check gegen zu einfaches Passwort) werden über das Pluggable Authentication Module (PAM) vorgenommen (siehe Kapitel 12.2 und `man passwd`).

/etc/login.defs

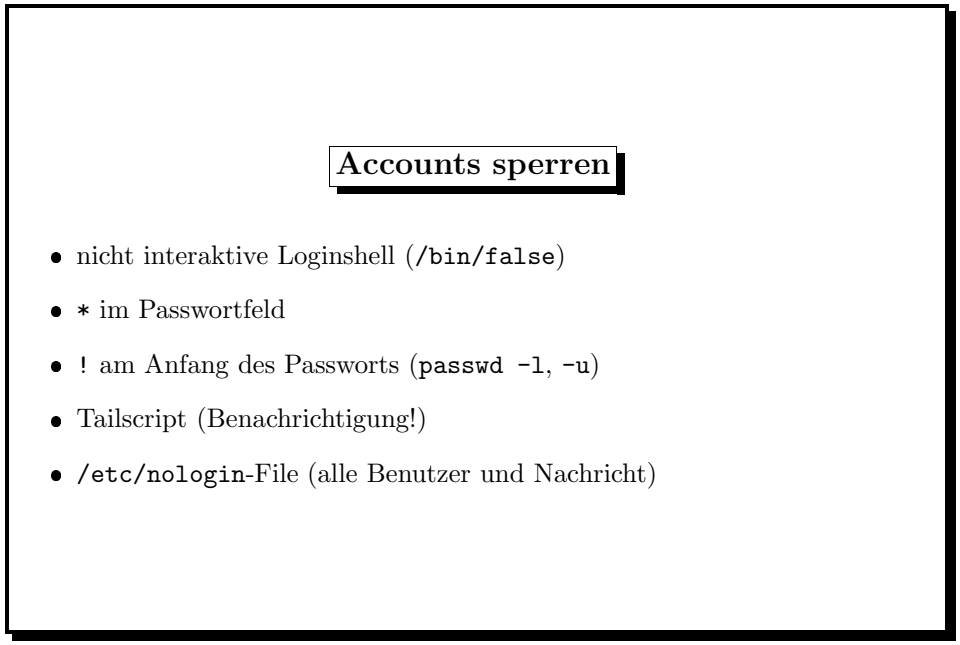
```
# Password aging controls:
#
PASS_MAX_DAYS   99999
PASS_MIN_DAYS   0
PASS_MIN_LEN    5
PASS_WARN_AGE   7
# Min/max values for automatic u/gid selection in useradd
D_MIN                   500
UID_MAX                 60000
GID_MIN                   500
GID_MAX                 60000
```

Folie 33

Accounts deaktivieren und löschen
Ist es aus gegebenen Gründen notwendig, Accounts zu *sperren* (Verstöße des Users gegen die Benutzungsordnung, Wartungsarbeiten, ...), gibt es mehrere Alternativen, zwischen denen root wählen kann. Die einfachste ist, im entspechenden Feld in der Passwortdatei eine nicht interaktive (nicht existierende) Shell (Standard: `/bin/false`) einzutragen; andererseits kann man in das Passwortfeld in `/etc/passwd` bzw. `/etc/shadow` einen `*` eintragen, oder einfacher ein Rufzeichen an den Anfang des verschlüsselten Passworts anfügen. Letzteres kann durch den Aufruf `passwd -l` (lock) geschehen und mittels der Option `-u` (unlock) wieder aufgehoben werden. Alle diese Varianten verhindern den Login des entsprechenden Benutzers, haben aber den Nachteil, dass dieser nicht erfährt, warum er nicht einloggen kann, was meistens eine Anfrage an den Administrator nach sich zieht.

Eine elegantere Methode ist es daher, eine Nachricht auszugeben zu lassen, wenn der Benutzer versucht, sich am System einzuloggen. Dazu verwendet man oft sog. „Tailscripts“ die als Loginshell in `/etc/passwd` eingetragen werden und eine bestimmten Text (zB „Your account has been temporarily disabled due to a security problem“) ausgeben.

Darüber hinaus gibt es Situationen, in denen man allen Benutzern den Zugang zum System verbieten will, zB wegen Wartungsarbeiten am Server, auf dem die Userdaten liegen etc. Man legt dann eine Datei `/etc/nologin` an, in der eine Erklärung zur Rechnersituation stehen sollte. Diese wird dann bei einem Loginversuche mit gültigem Passwort ausgegeben; zB wird bei laufendem Shutdown ein Nologinfile anlegt.



Folie 34

Ein dauerhaftes Entfernen *(Löschen)* eines Benutzeraccounts solltenur im Einverständnis mit dem Benutzer geschehen und/oder diesem rechtzeitig vorher unter Nennung von Gründen angekündigt werden. Insbesonders ist zu klären, was mit den Daten des Benutzers passieren soll.

Beim effektiven Löschen eines Accounts sollte dieser zuerst deaktiviert werden, um sicherzustellen, dass keine Daten mehr verändert werden können (die dann möglicherweise nicht mehr mit einem eventuellen Backup übereinstimmen). Sodann entfernt man entweder mit dem oben genannten Tool `userdel` oder einem anderen Werkzeug die Einträge in den drei Benutzerverwaltungsdateien. Nachdem die offensichtlich dem User zugehörigen Dateien (sein Homeverzeichnis und etwaige Mail, Croneinträge, Druckerjobs, ...) gelöscht wurden (kann mittels geeigneter Optionen von `userdel` erledigt werden), sollte man sich daran machen, auch alle übrigen dem User gehörenden Dateien zu suchen und zu löschen (`find -user`).
Obwohl das Löschen von Benutzern in vielen Umgebungen weit seltener und wegen des Backups sensibler ist, sollte auch hier ziemlich bald ein automatisiertes Script dafür sorgen, „Karteileichen“ aus dem System zu entfernen, da unbenutzte Accounts immer ein Sicherheitsrisiko darstellt. Es fällt zB niemandem auf, wenn der Account durch unberechtigte Personen verwendet wird.

Benutzer entfernen

- Deaktivieren des Accounts
- Einverständnis/Benachrichtigung des Users
- Entfernen der relevanten Zeilen aus
  `/etc/passwd`, `/etc/group` und `/etc/shadow`
  zB mit `userdel`
- Löschen des Home-Verzeichnisses (ev. vorher Backup)
- Löschen der Mailbox (in `/var/spool/mail`), anderer Daten in `/var` (Cron- und Drucker-Jobs)
- Übrige Dateien des Benutzers (`find / -user name`) (Backup!?)
- Automatisierung, Karteileichen sind Sicherheitsrisiko

Folie 35

4 Software-Installation

Selbst auf dem vollständigsten System ist (natürlich) nur eine generell nützliche Auswahl an Programmpaketen installiert und so kommt jeder Administrator (oder auch Benutzer) früher oder später in die Lage, eine Anwendung selbst in das System einspielen zu müssen. In diesem Kapitel wird erklärt, wie unter Unix Software zu Paketen zusammengefasst wird, wo man die gewünschten Pakete findet und wie man sie in die Installation integriert; insbesondere besprechen wir das Softwarepackage-Management unter Linux.

Die einfachste Form, in der in der Unix-Welt Software verteilt wird, ist ein gezipptes Tarfile, auch *Tarball* genannt, das man an der Dateiendungen `tar.gz`, `tgz` (verkürzt) oder auch `tar.bz2` erkennt. (vgl. Teil 1, Abschnitt 6.4). Meist enthält es die zum Compilieren der Anwendungen benötigten (C-)Sourcecodes mit Anleitung und Dokumentation aber auch zusätzliche Files, wie etwa Vorlagen für Konfigurationsdateien.

Die meisten Linux-Distributionen stellen weitgehende Ansprüche bezüglich vereinheitlichter Konfiguration des Gesamtsystems, Abhängigkeiten von Softwarepaketen untereinander und eigener Pfadstandards. Daher verwenden heute beinahe alle Distributionen ein eigenes *Softwarepackage-Management* mit eigenem Package-Format und dazugehörigen Managementtools statt einfacher Tarballs; diese Packages enthalten statt des Sourcecodes (wie beim Tarball üblich) die gebrauchsfertigen für genau die entsprechende Distribution (und Version) compilierten Binärdateien (genauer gesagt gibt es auch Sourcecode Packages; siehe unten). Das Package-Management vereinfacht und vereinheitlicht (De)Installation und Upgrade von Softwarepaketen.
Am weitesten verbreitet ist das `rpm`-Format (RPM Package Manager, ursprünglich RedHat Package Manager), das neben RedHat auch SuSE, Mandrake und andere Distributionen verwenden. Achtung, das bedeutet *nicht*, dass ein SuSE-`rpm`-Paket auf einem RedHat-System problemlos installiert werden kann, da oft verschiedene Pfadkonventionen gelten oder zueinander nicht kompatible Versionen von Bibliotheken installiert sind.

Softwarepakete

- Tarballs (gezippte Tarfiles)
  - Sourcecode zum selber Compilieren
  - Anleitung, Dokumentation
  - Beispielkonfigurationsdateien, ...
- Package-Management
  - distributionsspezifische Standards
  - „fertige“ Programme

Folie 36

Package-Management

- Distributionen definieren eigene Standards (Pfade, Konfiguration, ...)
- Packages für Distribution
  enthalten
  - Programmdateien, Bibliotheken
  - Dokumentation, Programminformation
  - Konfigurationsfiles, ...

  ermöglicht einfaches und vereinheitlichtes
  - (De-)Installieren
  - Paketabfrage und -verifikation
  - Upgrade
  - Abhängigkeitsinformation

  Formate
  - `rpm` RedHat, SuSE, Mandrake, ...
  - `deb` Debian, Corel

Folie 37

Initiativen wie die *Linux Standard Base (LSB)* haben es sich aber zum Ziel gesetzt, die verschiedenen Linux-Distributionen auch in Bezug auf das Package-Management aneinander anzugleichen, sodass die Möglichkeit, in Zukunft ein `rpm`-Paket für alle Distributionen verwenden zu können, immer wahrscheinlicher wird.
Unter den großen Distributionen verwendet einzig Debian (und darauf aufbauende Distributionen wie Corel Linux etc.) nicht `rpm`, sondern das `deb`-Package-Format, das in der Konzeption ähnlich ist, aber seine eigenen Stärken und Schwächen hat.

Bevor wir auf die Details im Umgang mit Softwarepaketen eingehen befassen wir uns mit der Frage: Woher bekommt frau Linux Software?

4.1 Linux-Softwarequellen

Die erste Adresse für Linux-Software ist natürlich immer die Homepage der entsprechenden Distribution resp. ihre Mirrorseiten. Oft stellen die Distributoren auf ihrer Homepage weitere nicht direkt im Umfang der Basisinstallation enthaltenen oder nicht auf den Installations CDs mitgelieferte Softwarepakete (im geeigneten Package-Format) zur Verfügung. Beispiele sind hierfür etwa die RedHat PowerTools und die RedHat Contributed Packages. Darüberhinaus bietet das Internet schier unbegrenzte Möglichkeiten Linux-Software herunterzuladen.

Der größte Index für Open Source Software im Internet findet sich unter `http://sourceforge.net`. Über eine bequeme Suchmaske ist es einfach, die gewünschte Software zu finden. Die Links zu den Homepages bzw. Downloads der Softwareprojekte werden täglich aktualisiert und viele Informationen über freie Software werden angeboten. Ein ähnliches Service bietet `http://www.freshmeat.net`.
Mittels einer Suchmaschine wie `google.com` gelangt man im Allgemeinen ebenfalls recht schnell zur Homepage des jeweiligen Programms, wo man meistens den aktuellen Source-Tarball bekommt, oft aber auch schon vorcompilierte Pakete für die verschiedenen Distributionen.
Eine übrigens besonders in Österreich sehr attraktive Möglichkeit, Programme zu finden, ist der Goodie Domain Ser-

ver der TU Wien (`gd.tuwien.ac.at`). Unzählige von großen FTP-Servern mit freier Software werden hier täglich gespiegelt. Über ein Webinterface lässt sich gezielt nach dem gewünschten Programm suchen.

Software speziell im `rpm`-Format sucht man am besten unter `http://rpmfind.net` bzw. dem Mirrorserver `http://at.rpmfind.net`. Auch hier ist eine Suchmaske verfügbar. Es gibt aber ebenso nach mehreren Kriterien geordnete Indices. Außerdem ermöglicht das Paket `rpmfind` ein automatisches Suchen im Internet nach `rpm`-Paketen.

Softwarequellen

- CDs, Homepage der installierten Distribution
  (zB Contributed RedHat-Packages und RedHat-PowerTools)
- `http://sourceforge.net` großer Open Source Index
- `http://rpmfind.net` `rpm`-Datenbank
  (Mirror `http://at.rpmfind.net`)
- Suchen mittels `rpmfind`-Paket
- Homepage der jeweiligen Anwendung
- `gd.tuwien.ac.at`

Folie 38

4.2 Sourcepackages

Obwohl die Installation von `rpm`- oder `deb`-Paketen einfacher und wegen der Einhaltung der Distributionsstandards in jedem Falle vorzuziehen ist, kommt man als Administrator (oder auch Benutzer) oft in Situationen, wo die gewünschte Software nicht im richtigen Format vorhanden ist und man so gezwungen ist, ein Sourcepackage zu installieren. Gründe für das Fehlen von `rpm`- oder `deb`-Paketen können sein, dass eine Software besonders neu ist und noch keine Packages erzeugt wurden oder es sich um eine sehr exotische oder noch im Entwicklungsstadium befindliche Software handelt. In solchen Fällen bieten die Package-Managementtools der Distributionen die Möglichkeit selbst `rpm`- oder `deb`-Pakete zu bauen, die Software selbst muss aber zuerst compiliert, installiert und getestet werden.
Unter Linux gehört die GNU Compiler Collection (GCC) zum Umfang jeder Distribution; damit ist das compilieren von C/C++ Code und auch einer Reihe weiterer wichtiger Pragrammiersprachen möglich. Der Compiler selbst heißt – wie auch das ganze Paket – `gcc`, was hier aber GNU C Compiler bedeutet.
Schließlich verwenden die meisten anderen Unix-Versionen entweder kein Package-Management oder die Packages sind proprietär, sodass etwa auf AIX oder Solaris Systemen das Compilieren von Sourcepaketen eine sehr große Rolle spielt.

Wir diskutieren die Handhabung von Sourcepackages nun am Beispiel das Quellpakets von `ascii`, einem sehr einfachen Programm, das zu einer gegebenen Taste den ASCII-Code (und andere Informationen) zurück liefert. Nachdem das Paket von der via `freshmeat.net` gefundenen Seite `http://www.tuxedo.org/~esr/software.html` heruntergeladen wurde, kann man es mit `tar xzf ascii-3.0.tar.gz` entpacken (es empfiehlt sich übrigens, dies nicht direkt im Hauptpfad des Homeverzeichnisses auszuführen, sondern zB ein Verzeichnis `packages` anzulegen, in dem man mit den Paketen arbeiten kann; als root kann man auch das Directory `/usr/src/` verwenden). Wenn wir nun in das Verzeichnis wechseln und uns seinen Inhalt anschauen, sehen wir neben dem Sourcecode `ascii.c` und weiteren Dateien (zB `ascii.1` ist das Manual, das nach der Installation des Paketes bei `man ascii` angezeigt wird) auch noch die Datei `README`, die in beinahe jedem Source-

package vorhanden sein sollte; sie enthält gewöhnlich Informationen über das Programm selbst, aber auch über die Schritte, die zum Compilieren notwendig sind. Diese Datei sollte man auf jeden Fall zumindest kurz durchschauen, damit man mögliche Probleme beim Compilieren hier schon verstehen kann; eventuell gibt es auch noch eine Datei `INSTALL`, die besonders auf den Compiliervorgang eingeht. Die für uns wichtigste Datei im Verzeichnis `ascii-3.0` ist aber das `Makefile`, das alle Regeln enthält, wie ein in C (oder auch anderen Sprachen wie C++) geschriebenes Programm aus seinen einzelnen Sourcefiles zu einer ausführbaren Datei zusammengebaut werden soll. Dessen Funktionsweise muss man aber nur verstehen, wenn man das Paket selbst verändern will. Im Normalfall reicht es aus, `make` einzugeben, das Makefile wird abgearbeitet und das Programm – hoffentlich erfolgreich – compiliert. Wenn man keine Fehlermeldung erhalten hat, ist es auch gleich möglich, mit einem ähnlichen Kommando, nämlich `make install` das erzeugte Programm inklusive Manpage etc. zu installieren. Achtung: Dazu muss man `root` sein, da man sonst nicht in Verzeichnissen wie `/usr/bin` schreiben darf, wo ja die systemweit zu verwendenden Binaries abgespeichert werden müssen.
Ein normaler Benutzer kann die mit `make` erstellten Binärfiles an einen geeigneten Platz in seinem Homedirectory (zB `$HOME/bin`) kopieren und von dort aus ausführen.

Sourcepackages installieren

- Paket herunterladen
- Mit `tar` entpacken
- In das erzeugte Verzeichnis wechseln
- `README` (und `INSTALL`) lesen
- Gibt es ein `configure`?
  Wenn ja `./configure` ausführen
- `make`
- `make install` als `root`
  sonst Binaries in eigenen Suchpfad kopieren

Folie 39

Natürlich können beim Compilieren Fehler aufgetreten sein, weil zB auf dem eigenen System Dateien nicht installiert sind, die zum Bauen unbedingt erforderlich sind (meistens C-Headerfiles) oder der Programmautor den Quellcode nicht richtig getestet hat etc. Um solche Probleme möglichst schon am Anfang des (oft sehr lange dauernden) Compiliervorgangs zu erkennen, wurde ein Tool namens `autoconf` entwickelt, das insbesondere bei moderneren und größeren Paketen zum Einsatz kommt. Dieses untersucht die aktuelle Installation auf Verträglichkeit mit dem Sourcecode (also zB unterstützt der verwendete Compiler bestimmte Optionen, sind alle Include-Dateien vorhanden, ...). Als Benutzer kann man ganz einfach erkennen, ob ein Sourcepackage `autoconf` verwendet, indem man nachsieht, ob es im Hauptverzeichnis des entpackten Tarballs eine Datei namens `configure` gibt. Wenn diese vorhanden ist, muss man sie *vor* dem Kommando `make` ausführen (also `./configure` aufrufen). Von den nun relativ schnell vorbei fliegenden Meldungen lässt man sich besser nicht irritieren, `configure` gibt bei einem wirklichen Fehler eine (aussagekräftige) Fehlermeldung, alle anderen Checks kann man gewöhnlich ignorieren. Wenn `configure` fertig ist, geht man wie oben weiter vor: nach einem `make` und `make install` ist das Paket installiert und meistens auch schon einsatzbereit.

Wenn `configure` wirklich einmal eine Fehlermeldung über eine fehlende Datei ausgibt, ist die Chance relativ groß, diese Datei in einem Paket der jeweiligen Distribution zu finden (wenn nicht in den Dateien `README` oder `INSTALL` explizit auf eine andere Möglichkeit hingewiesen wird): Die Namen von Paketen, die Headerfiles zu einer Bibliothek enthalten, enden gewöhnlich auf `-dev` (SuSE, Debian) oder `-devel` (RedHat, Mandrake); zB befindet sich die Datei `/usr/include/png.h` unter RedHat im Paket `libpng-devel`.

4.3 Softwarepackage-Management

Der *RPM Package Manager*, kurz `rpm` ist das Tool zur Verwaltung von Softwarepaketen auf `rpm`-basierten Systemen. Ursprünglich von RedHat entwickelt und GPL lizenziert, ist es heute weit verbreitet. Die Homepage befindet sich auf `http://www.rpm.org`. Das `rpm`-Format sieht vor, dass Pakete neben den (binären) Programmdateien und Dokumentation auch Pre- und Post-Installationsscripts sowie Deinstallationsskripts und vor allem Paketabhängigkeits Informationen enthalten. Eine Berücksichtigung letzterer garantiert, dass ein installiertes Paket auch richtig funktioniert, weil alle vom Paket benötigten Funktionen bereits von anderen Paketen zur Verfügung gestellt werden. Beim Upgraden von Programmpaketen kann es manchmal Probleme mit eben diesen Abhängigkeiten geben, da Zirkel entstehen können; die Abhängigkeitsprüfung kann dann mit der Option `--nodeps` abgeschaltet werden (siehe Syntax auf den Folien). Weiters überprüft `rpm` bei der Installation eines Pakets, ob Konflikte vorliegen, d.h. ob das Paket eine Datei enthält, die im System schon vorhanden ist und zu einem anderen Paket gehört. Diese Überprüfung kann mit der Option `--replacefiles` überschrieben werden. Alle Informationen über installierte Pakete werden in der `rpm`-Datenbank in `/var/lib/rpm/` am System gespeichert.

Der Dateiname von `rpm`-Paketen setzt sich aus folgenden Teilen zusammen: Paketname, Versionsnr., Releasenr., Architektur und der Endung rpm. D.h. der Name `ftp-0.17-7.i386.rpm` bedeutet, dass es sich um das FTP-Paket (File Transfer Protocol) Version 0.17, Releasenummer 7 für den Intel 80386 Prozessor (und höhere) handelt, das den `ftp`-Client enthält. Der Quellcode ist jeweils in einem eigenen `rpm`-Paket erhältlich; dass es sich dabei um ein Quellcode- und nicht um ein Programmpaket handelt, wird durch ein zusätzliches „`src`“ im Dateinamen ausgedrückt, zB `ftp-0.17-7.i386.src.rpm`; `rpm`-Pakete werden auch als RPMS bezeichnet, Quellcodepakete als SRPMS.

Der RPM Package Manager

- Homepage `http://www.rpm.org`
- entwickelt von RedHat; weit verbreitet; GPL (SuSE, Mandrake, ...)
- (De)Installieren von Programmpaketen
- Upgrade, Refresh von Programmpaketen
- Abfragen und Verifizieren von Programmpaketen
- Kommandozeile und GUI (GnoRPM, `kpackage`)
- Programmpakete als .rpm-Dateien
- `rpm`-Datenbank am System (`/var/lib/rpm/`)
- Dokumentation: Maximum RPM `http://www.rpm.org/max-rpm`

Folie 40

`rpm`-Pakete

- Paketdateiname=
  Paketname+Versionsnr+Releasenr+Architektur.rpm
  zB `diald-0.16.4-1.i386.rpm`
- enthalten
  - Name, Version, Beschreibung, Info
  - Paketabhängigkeits- (Dependency-) Information
  - Das Programmpaket selbst (gezippt)
  - Pre- und Postinstallationsskripts
- herausgegeben von RedHat oder anderen
  (mit rpm kann man selbst Pakete erzeugen)

Folie 41

`rpm` verwenden

- 5 Grundverwendungsarten:
  - Installieren
  - Upgraden und Freshen
  - Deinstallieren
  - Abfragen (query)
  - Verifizieren (verify)
- für Fortgeschrittene: Pakete erzeugen

Folie 42

Drei der grundlegenden Funktionen des `rpm` (*Installation, Upgrade, Freshen*) wurden schon in Teil 1, Abschnitt 9.3 behandelt; die Syntax ist auf Folie 43 angeben. Beim Installieren wird geprüft, ob ein Paket gleichen Namens schon installiert ist und (standardmäßig) die nochmalige Installation verweigert. Will man ein Paket durch eine neuere(n) Version/Release ersetzten, muss Upgrade oder Freshen verwendet werden. Der Unterschied zwischen diesen beiden Modi ist, dass bei letzterem nur eine Installation erfolgt, falls das alte Paket tatsächlich bereits installiert ist. Bei Upgrade erfolgt immer eine Installation des entsprechenden Pakets; falls vorhanden, wird vorher die alte Version entfernt. Bei Upgrade und Freshen werden Konfigurationsfiles des alten Pakets mit der Endung `.rpmsave` gespeichert bzw. neue Konfigurationsfiles mit der Endung `.rpmnew` erzeugt und eine entsprechende Warnung ausgegeben.

Weitere grundlegende Funktionen des `rpm` sind *Deinstallieren, Abfragen und Verifizieren* von Paketen. Die Syntax ist auf den Folien 44 – 46 erläutert.
Beim Deinstallieren eines Pakets wird natürlich geprüft, ob etwaige Abhängigkeiten verletzt und so die Funktion von anderen Programmen beeinträchtigt wird.
Das Abfragen von Paketen dient dazu, Informationen über das Paket und seine Installation zu erhalten; diese sind zB der Vertreiber des Pakets und Adresse seiner Homepage, allgemeine Informationen zum Paket, eine Liste aller im Paket befindlichen Dateien, das Installationsdatum etc. Es können sowohl installierte Pakete, als auch nicht installierte Paketdateien abgefragt werden.
Das Verifizieren eines Pakets erlaubt festzustellen, ob die Dateien des Pakets seit der Installation verändert wurden. Bei Konfigurationsfiles ist es selbstverständlich, dass diese verändert werden. Ist allerdings eine binäre Datei verändert worden, so ist das ein Alarmsignal und oft ein Zeichen für einen Hackereinbruch. Ähnliches gilt für den Fall, dass die `rpm`-Datenbank am System oder `rpm` selbst korrumpiert ist. Im Fall, dass die `rpm` Datenbank nicht mehr verlässlich funktioniert, kann die Verifikation eines installierten Packages auch gegenüber einem (Original-) `rpm`-File erfolgen.

RPMS installieren/upgraden/freshen

Syntax: `rpm -i|U|F[hv] Paketdatei [Optionen]`

- `-i|U|F` install, upgrade, freshen
- Upgrade: vor Installation altes Paket deinstalliert
  Konfigurationsdateien mit Extension:
  `.rpmsave` gesichert – `.rpmnew` erzeugt
- Freshen: detto, aber nur falls altes Paket wirklich installiert war
- Paketdatei: zB `joe-2.8-40.i386.rpm`
- Optionen: `-v(v)` (sehr) verbose
  - `-h` zeigt Verlauf mittels hash marks (#)
  - `--test`, `--nodeps`, `--replacefiles`, `--replacepkgs`, `--oldpackage`, `--force`, `--noscripts`

Folie 43

RPMS deinstallieren

- Syntax: `rpm -e Paketname [Optionen]`
- Paketname: zB `joe`
  ACHTUNG: nicht Paketdatei zB `joe-2.8-40.i386.rpm`
- Optionen:
  - `--allmatches` alle Versionen
  - `--test`
  - `--noscripts`
  - `--nodeps` (gefährlich!)

Folie 44

RPMS abfragen

- Syntax: `rpm -q Paketname [Optionen]`
- Output: Versions- und Releasenummer
- Optionen:
  - `-a` frage alle installierten Pakete ab
  - `-i` zeige Paketinformation an
  - `-l` liste alle Dateien im Paket
  - `-d` liste alle Dokumentationsfiles im Paket
  - `-c` liste alle Konfigurationsfiles im Paket
  - `-f file` zu welchem Paket gehört `file`
  - `-p Paketdatei` für nicht installierte Pakete

Folie 45

Um die Verbreitung von manipulierten `rpm`-Paketen (Trojanischen Pferden) zu verhindern, können Pakete vom Vertreiber mit einem PGP/GPG (Pretty Good Privacy/Gnu Privacy Guard, einem Public-Key-Verschlüsselungsprogramm) signiert werden. Die Authentizität dieser Pakete kann dann mittels `rpm --checksig rpm-file` getestet werden.

Schließlich kann der RPM Package Manager auch dazu verwendet werden, um `rpm`-Pakete zu erzeugen.

Der RPM Package Manager besitzt auch graphische Interfaces namens GnoRPM (für den Gnome Desktop) und `kpackage` (für KDE). Diese können alle vorher besprochenen Funktionen erfüllen und bieten ein (mehr oder weniger) übersichtliches GUI.

Eine Erweiterung des `rpm` das ein einfaches und automatisches Upgraden von Paketen (allerdings nur auf RedHat Systemen) ermöglicht und es so insbesondere erlaubt, alle Packages am System auf dem neuesten Stand zu halten ist der *Red Hat Update Agent* `up2date`. Dieser verfügt sowohl über ein Kommandozeileninterface als auch ein grafisches Interface, erlaubt aber nur das Upgraden von Packages die von RedHat selbst herausgegeben wurden. Für alle Details verweisen wir auf die RedHat Homepage.
Ein anderes Tool, das in etwa die selben Aufgaben übernehmen kann und auf allen `rpm`-basierten Systemen funktioniert ist *autorpm*; für Details siehe `http://www.autorpm.org`.

Die wahrscheinlich größte Schwäche `rpm`-basierter Systeme ist, dass es unter Umständen sehr mühsam ist, händisch ein bestimmtes Paket zu installieren; nämlich wenn eine Vielzahl von Abhängigkeiten nicht erfüllt ist und diese Pakete auch noch weitere unerfüllte Abhängigkeiten nach sich ziehen. Tools, die solche Situationen meistern sind `rpmfind` (`http://www.rpmfind.net`) und `autoget` (aus dem Autoupdate-Paket von Gerald Teschl, `http://www.mat.univie.ac.at/~gerald/ftp/autoupdate`).
Im Debian Package-Management kann die Situation der „Abhängigkeitsschleife“ beim *Installieren* von Paketen vom Updatetool `apt-get` gehandelt werden (siehe unten); es gibt auch eine Version, die das `rpm`-Format unterstützt.

RPMS verifizieren

- Syntax: `rpm -V Paketname [Optionen]`
- Output: 5STUGM
  veränderte MD5-Prüfsumme, Größe, Mtime, Besitzer, Gruppe, Mode (Berechtigung, Typ)
- Optionen:
  - `-f file` verifiziere `file`
  - `-a` verifiziere alle installierten Pakete
  - `-p package-filename.rpm` verifiziere gegenüber `package-filename.rpm` statt Datenbank

Folie 46

`rpm`-Erweiterungen

- Graphische Interfaces
  - GnoRPM (Gnome Desktop)
  - `kpackage` (KDE)
- Automatische Updates
  - `up2date` (RedHat)
  - `autorpm`
  - `autoupdate`
  - `rpmfind`
  - `apt-get` auch für `rpm`-Format

Folie 47

Das *Debian Package-Management* funktioniert ähnlich dem `rpm`; das entsprechende Tool heißt `dpkg`. Wesentliche Unterschiede zu `rpm` sind eine Staffelung der Paketabhängigkeiten auf drei Ebenen (mandatory, recommended, optional), die Endung `deb` der Paketdateien an Stelle von `rpm` und die fehlende Unterstützung für PGP/GPG-Signaturen der Paketdateien. Das `up2date` entsprechende Tool für Debian Linux heißt `apt-get` und zeichnet sich durch seine besonders problemlose und einfache Anwendbarkeit aus.

Schließlich gibt es das Tool *Alien*, das es ermöglicht, Pakete von einem Format in ein anderes und auch zwischen Distributionen zu konvertieren (siehe `http://kitenet.net/programs/alien`).

Das Debian Package-Management

- Homepage `http://www.debian.org`
- `dep`-Format: Package-Managment der Debian GNU/Linux Distribution
- `dpkg`: Äquivalent zu `rpm` Kommandozeilenprogramm für `deb`s
- Standardoperationen wie `rpm` (De/Installieren, Update, ...)
- Konfiguration in `/etc/apt`
- `deb`-Datenbank am System in `/var/lib/apt/`
- Programmpakete als `.deb`-Dateien
- `apt-get`: Automatisches Install/Update von Paketen über Internet
- Umfangreiche Dokumentation und Tools fürs Selbstbauen von Paketen

Folie 48

5 Speichermanagement

In diesem kurzen Kapitel erklären wir die Grundzüge der Speicherverwaltung unter Linux und stellen einige nützliche Tools zum Speicher- und System-Monitoring vor.

5.1 Speicherverwaltung

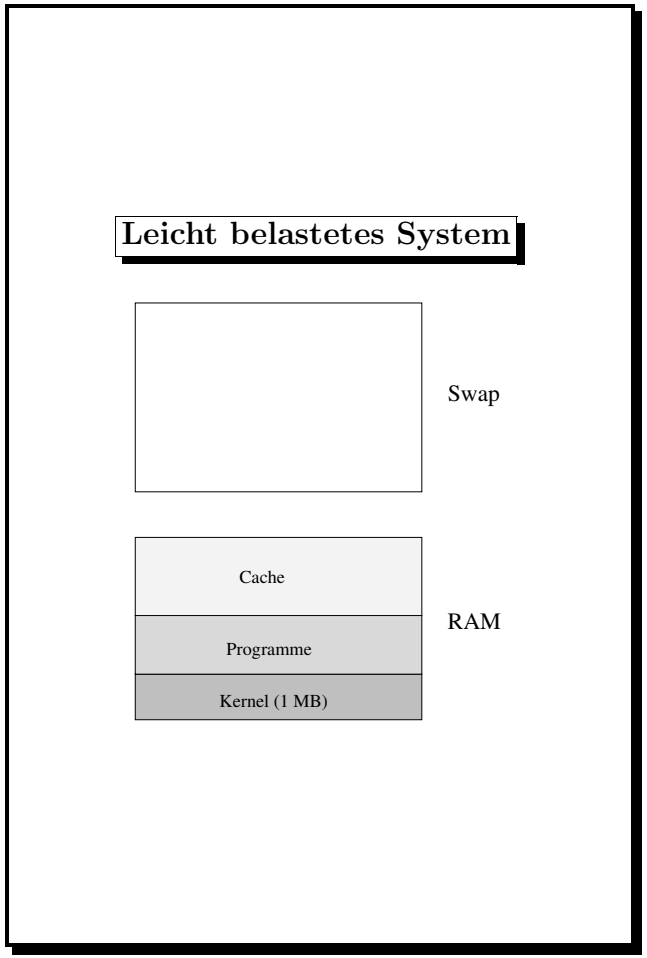
Unter Unix wird neben dem physikalisch vorhandenen Hauptspeicher (RAM) Auslagerungsspeicher (Swap oder Paging Space, meist in Form einer Swap-Partition auf einer der Festplatten des Systems) verwendet. Der so vorhandene gesamte Speicher wird in gleich große Einheiten sogenannte *(Memory) Pages* (1–8 KB, meist 4 KB) unterteilt, die vom Kernel verwaltet werden. Jedem Prozess wird bei seinem Start ein gewisser Adressbereich bestehend aus einer Anzahl von Pages zugewiesen und bleibt für diesen reserviert.
Etwas genauer wird der Hauptspeicher unter Linux wie folgt aufgeteilt: Das erste MB ist für den Kernel reserviert, der Rest des RAM wird auf die laufenden Prozesse und den Disk Cache aufgeteilt. Letzterer dient zum Zwischenspeichern von Daten, die von den Massenspeichergeräten des Systems eingelesen bzw. dorthin geschrieben werden.

Ist das RAM voll belegt (d.h. es gibt keine freien Pages mehr im Hauptspeicher) – wobei immer ein, wenn auch eventuell kleiner Teil, für den Disk Cache reserviert bleibt – beginnt der Kernel Speicherseiten in den Swap-Bereich auszulagern. Dabei wird versucht, zuletzt benutzte Pages im RAM zu behalten und weniger benutzte in den Swapspeicher auszulagern, der nur um Größenordnungen langsamer angesprochen werden kann (sog. LRU System; die least recently used Pages werden ausgelagert (paged out) und VM (Virtual memory) System; für Details und auch den (hier verschwiegenen) Unterschied zwischen Swapping und Paging siehe [1], Kap. 25).

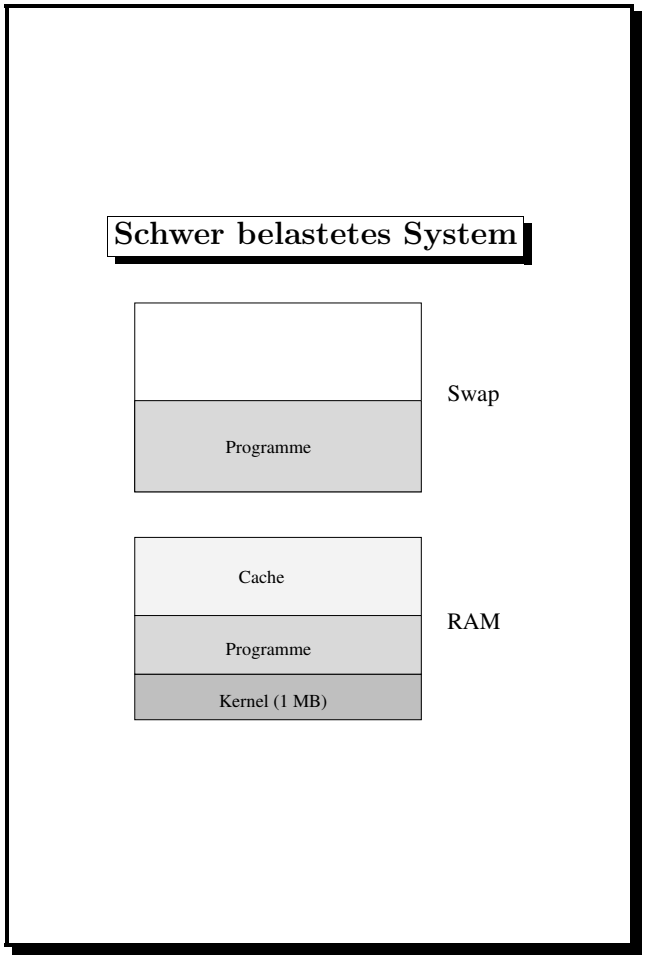
Linux Speichermanagement

- Gesamtspeicher = RAM + Swapspeicher
- unterteilt in (Memory)Pages (4 KB)
- für Prozesse verfügbarer Speicher = RAM + Swap Space − 1 MB
  - 1 MB reserviert für Kernel
  - Rest für Prozesse
- Pages im RAM werden – wenn nötig – auf HD ausgelagert
- Unbenutztes RAM wird als Disk-Cache verwendet
- effektiver Algorithmus, nicht konfigurierbar

Folie 49



Folie 50



Folie 51

Neben dem unangenehmen „Dauerrattern“ der Festplatte(n) verlangsamt das Swapping den Betrieb des Systems wesentlich, besonders dann, wenn sogar Daten von aktiven Prozessen ausgelagert werden müssen. Ist auch der Swapspeicher voll belegt, so beginnt der Kernel Prozesse (nach Zufallsprinzip) zu stoppen, eine Situation, die vermieden werden sollte!

Unter Linux kann *Swap—ßpeicher* in Form von Swap-Partitionen aber auch Swap-Files verwendet werden. Die Methode der Wahl ist die Verwendung von Swap-Partitionen, die wesentlich schneller und effektiver sind. Dazu muss eine eigens dafür vorgesehene Festplattenpartition angelegt werden (meist schon bei der Installation; siehe Teil 1, Kapitel 8). Swap-Partitionen können mit jedem der Tools zu Festplattenpartitionierung, also insbesondere zB mit `fdisk` erstellt werden. Der Partitionstyp muss dabei auf den Hex Code 82 (Linux Swap) gestellt werden. Zum Anlegen des Swapspeichers (analog zum Formatieren einer „gewöhnlichen“ Festplattenpartition) verwendet man das Kommando `mkswap partition`. Aktiviert werden kann der Swapspeicher mit dem Kommandozeilenaufruf `swapon partition`; bei Systemstart wird dies vom Script `/etc/rc.sysinit` erledigt (vgl. Teil 1, Kapitel 9). Im Unterschied zu den meisten Unix-Varianten kann unter Linux Swapspeicher im laufenden Betrieb mittels `swapoff partition` deaktiviert werden; das ist allerdings nur dann möglich, wenn im Hauptspeicher (resp. anderen Swap-Bereichen) genug Platz ist und die Daten dorthin geschrieben werden können.

Die Größe des Swapspeichers richtet sich sinnvoller Weise nach der Größe des RAM; der Swapspeicher sollte größenordnungsmäßig dem RAM entsprechen. Sinnvoll ist es daher, im Hinblick auf zukünftiges Hardwareupgrade die Swap-Partition ca. zweimal so groß wie das RAM zu wählen; es ist oft wesentlich einfacher, zusätzliches RAM einzubauen als die Formatierung der Festplatte(n) zu ändern.
Von der Verwendung von Swap-Files ist im Allgemeinen aus Performancegründen abzuraten. Im Notfall (etwa kurzfristig bedingter Speicherengpass) stellt sie aber eine gangbare Alternative dar. Wir erklären die Vorgangsweise zum Anlegen eines Swap-Files auf Folie 53.

Swap-Partition

- Größe
  - minimal 10 Pages (40KB); maximal 2GB
  - maximal 8 Partitionen
- Anlegen
  - Partition erzeugen mit `fdisk` (Typ 82)
  - Swap-Partition mit `mkswap` anlegen (formatieren)
- Management
  - aktivieren mit `swapon /dev/hdxy`
  - deaktivieren mit `swapoff /dev/hdxy`
    - ohne Reboot möglich
    - nur wenn genug Speicher vorhanden

Folie 52

Swap-File

- weniger effizient als Partition (Notfall!)
- Anlegen
  - finde Platz für Swap-File (`df`)
  - erzeuge großes File
    zB `dd if=/dev/zero of=swapfile bs=1024 count=64000`
  - verwandle es in ein swapfile `mkswap swapfile`
  - aktivieren `swapon swapfile`

Folie 53

Gegenwärtig (Februar 2002) kann der Linux Kernel bis zu 64 GB Hauptspeicher verwalten. Dazu muss er aber mit High-Memory-Support compiliert werden (erlaubte Werte der entsprechenden Option sind: OFF, 4 GB und 64 GB, vgl. Kapitel 10). Die Standardkernels der meisten Distributionen (High-Memory-Support OFF) können bis zu 960 MB RAM adressieren.
Darüber hinaus sind bis zu 8 verschiedene Swap-Bereiche (Partitionen und Dateien) möglich. Ihre Größe muss mindestens 10 Pages betragen und ist nach oben mit 2 GB limitiert. Für den aktuellen Stand dieser sich stetig ändernden Werte empfiehlt es sich, immer in der aktuellsten Dokumentation nachzusehen.

5.2 Monitoring

Zum Schluss dieses Kapitels stellen wir einige einfache Tools zur Überwachung der Speicherverwendung bzw. der Systemperformance vor.

Das einfachste Kommando, das eine Statistik über die laufenden Prozesse ausgibt ist der `ps`-Befehl. Etwa gibt `ps aux` eine Statistik aller laufenden Prozesse geordnet nach PID (Prozess Identity; siehe Teil 1, Abschnitt 6.3) aus. Angezeigt werden neben dem Besitzer eines Prozesses vor allem Speicher- und CPU-Nutzung. Die Prozesshierarchie kann mittels `pstree` angezeigt werden. Beide Kommandos haben den Nachteil, dass sie nur einen Snapshot zu einem bestimmten Zeitpunkt wiedergeben. Abhilfe schafft das `top`-Kommando, das eine periodisch aktualisierte Statistik der laufenden Prozesse anzeigt. Außerdem können interaktiv Signale an die Prozesse gesendet werden.

Die Speicherstatistik kann mittels `free` abgefragt werden; Belegung von Haupt- und Swapspeicher, sowie Größe des Festplattencaches werden angezeigt. Um detaillierte Information über die Statistik des Virtual Memory System auszugeben, kann der Befehl `vmstat` verwendet werden.

Das `uptime`-Kommando gibt die *Uptime* des Systems aus, also die Zeit, die seit dem letzten Systemstart vergangen ist. `uptime` zeigt aber auch die *Systemlast* an. Die Systemlast ist die Zahl der „lauffähigen“ Prozesse, also der Prozesse, die auf CPU Zeit oder I/O Operationen warten. `uptime` gibt 3 Werte gemittelt über die letzten 1, 5 und 15 Minuten aus. Steigt die Systemlast signifikant über 1 an, so ist das System schwer belastet und für den Benutzer entsteht der Eindruck, das System arbeite langsam.

Schließlich geben die graphischen Tools `xosview, xload` und `xsysinfo` einen bunten Überblick über die Systemnutzung; weitere Tools sind in die Desktopsysteme KDE und GNOME integriert.

Monitoring-Tools

- `top` zeigt Speicher-, CPU- und Prozessstatistik an
- `ps, pstree` zeigt Prozesse/Prozesshierarchie an
- `free` zeigt Speicherstatistik an
- `vmstat` detaillierte VM Statistik
- `uptime` zeigt Uptime und Systemlast

fürs GUI

- `xosview` zeigt Systemüberblick an
- `xload` zeigt Systemlast
- `xsysinfo` zeigt Systeminformationen an
- ...

Folie 54

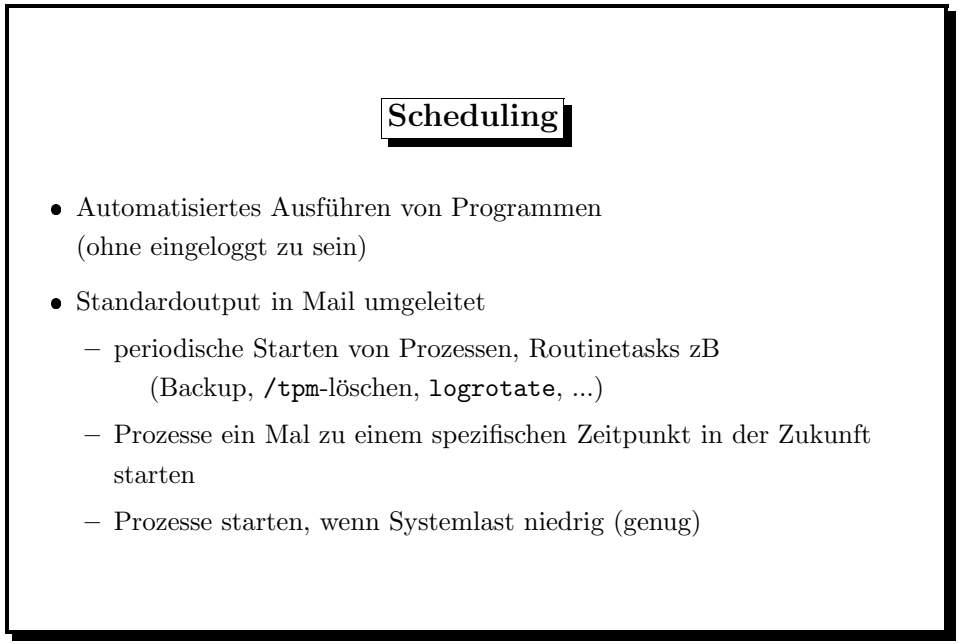
6 Scheduling

Eine wichtige Aufgabe des Systemadministrators ist es Routineaufgaben verlässlich durchzuführen; Automatisierung ist hier die Methode der Wahl. In diesem Kapitel beschreiben wir wie sich (periodische) Routineaufgaben mittels Scheduling automatisieren lassen und wie Programme ausgeführt werden können, ohne dass der Benutzer interaktiv am System angemeldet ist.

Durch den konsequenten Einsatz von Automatisierungen lassen sich viele Aufgaben am System – unter der Voraussetzung der richtigen Implementierung – sehr effizient und bequem durchführen. Eine mögliche Form ist das Schreiben von Scripts (zB zum Hinzufügen von Benutzern, vgl. Kapitel 3), eine andere, der wir uns hier zuwenden wollen, ist das sogenannte *Scheduling*. Es kann im Wesentlichen in zwei Gruppen eingeteilt werden:

- regelmäßig wiederholtes Starten bzw.
- einmaliges Ausführen von Programmen (Scripts) (möglicherweise unter speziellen Randbedingungen).

Für den ersten Punkt steht unter Unix das Programm `cron` zur Verfügung, für den zweiten allgemein `at`, im speziellen `batch`, das Jobs ausführt, sobald die Systemlast (siehe Abschnitt 5.2 unter einen gewissen Wert (default 0.8) gefallen ist.
Alle drei Varianten werden durch Daemonen gesteuert (`crond` bzw. `atd` für `at` und `batch`), die jede Minute überprüfen, ob ein „Auftrag“ erledigt werden muss. Das Einsenden solcher Jobs an die Warteschlange (ähnliches Konzept wie beim Drucken, siehe Kapitel 7) geschieht bei `at` und `batch` direkt über die Kommandozeile. `cron` bezieht die Informationen aus einer Crontab genannten Datei. Es gibt einerseits die globale Crontab des Systems `/etc/crontab`, andererseits kann jeder Benutzer eine persönliche Crontab in `/var/spool/cron/$USER` anlegen.



Folie 55

Scheduling aber wie?

- periodische Aufgaben
  - in Crontab-Dateien festgelegt
    `/etc/crontab` fürs System,
    `/var/spool/cron/$USER` für Benutzer
  - `crond` liest diese und startet Prozesse
  - `anacron`: auch wenn Rechner nicht durchgehend in Betrieb
- einmalige Aufgaben
  - zu einem bestimmten Zeitpunkt: `at`-Kommandozeileninterface
  - wenn Systemlast gering: `batch`-Kommandozeileninterface
  - beide vom `atd` gemanagt

Folie 56

Verschiedene Distributionen (darunter RedHat) verwenden außerdem folgenden Standard: Der Administrator kann Programme und Scripts, die vom System stündlich, täglich, wöchentlich oder monatlich ausgeführt werden sollen in die Verzeichnisse `/etc/cron.{hourly,daily,weekly,monthly}` legen. Programme in diesen Verzeichnissen werden nach dem in `/etc/crontab` festgelegten Schema einmal pro Stunde, Tag, Woche bzw. Monat ausgeführt.

Weiters gibt es unter Linux noch das Service `anacron`, das ähnlich wie `cron` funktioniert, aber dafür sorgt, dass Jobs auch dann ausgeführt werden, wenn der Rechner nicht durchgehend in Betrieb ist. `anacron` überprüft nach seiner Aktivierung (meist beim Booten), ob gemäß seiner Konfiguration (in `/etc/anacrontab`) unerledigte Jobs vorhanden sind und startet diese (jeweils mit einer kleinen Zeitverschiebung, sodass nicht alle Jobs aufeinmal ausgeführt werden und die Systemlast plötzlich aus für den Benutzer nicht ersichtlichen Gründen ansteigt). Ist der letzte Job erledigt wird `anacron` beendet. Außerdem wird `anacron` (meist) einmal täglich von `cron` selbst aufgerufen, um die Checks vorzunehmen.

Wir wollen uns nun anhand eines einfachen Beispiels aus der täglichen Praxis die grundlegende Funktionsweise von `cron` ansehen.

Systemcrontab (1)

- in `/etc/crontab` festgelegt
- führt standardmäßig Scripts in den folgenden Verzeichnissen aus
  - `/etc/cron.hourly`
  - `/etc/cron.daily`
  - `/etc/cron.weekly`
  - `/etc/cron.monthly`

Folie 57

6.1 Ein „Real World“ Beispiel

In einem großen (meistens auch räumlich getrennten) Netzwerksystem kann man nicht jedes Problem eines Benutzers vor Ort lösen. In einer solchen Situation nützt man die Stärke eines textbasierten Systems, wie es nun einmal Unix/Linux ist, aus, um mittels eines geeigneten Mechanismus Rechner aus der Ferne zu administrieren. War hier bis vor einigen Jahren hauptsächlich `telnet` in Verwendung, setzt man heute wegen ihrer höheren Sicherheit auf die *Secure Shell* (`ssh`). Um sich so zu einem anderen Rechner zu verbinden, muss dort der `sshd` Daemon laufen, der einkommende Verbindungsanfragen übernimmt (siehe Kapitel 15). Sollte dieser Daemon aber einmal aus irgendeinem Grund (zB Absturz) nicht laufen, bleiben einem im Wesentlichen nur zwei Alternativen: Selbst zum betroffenen Rechner gehen und manuell den `sshd` neu starten bzw. hoffen, dass jemand vor dem Rechner sitzt und ihn bitten, die Maschine zu rebooten (den `sshd` darf nur root starten). Beide Möglichkeiten kommen nicht immer in Frage (zB Rechner ist weit entfernt bzw. ein Server, den man nicht einfach so rebooten darf). Es wäre in der Tat schön, gäbe es einen Mechanismus, der zweimal täglich nachsieht, ob der `sshd` ordnungsgemäß läuft, ihn gegebenenfalls neu startet und dann eine Mail über den Status des Daemonen an den Administrator schickt.
Ein Script, das diese Aufgabe erledigt (und das man unbedingt zuerst einmal manuell genügend testen sollte), lautet (siehe auch Kapitel 11):

```
#!/bin/sh
#/sbin/check-sshd (restarts sshd if down)
if [ -z "‘pidof sshd‘" ]; then
 /etc/init.d/sshd restart >/dev/null 2>&1
 echo "sshd restarted" | mail -s "‘hostname --fqdn‘"\
                          root@logserver
fi
```

Kurze Erklärung: `pidof sshd` ermittelt die `PID`, unter der der `sshd` läuft; wenn aber kein `sshd` läuft, muss das Ergebnis leer (`-z`) sein, was hier ausgenutzt wird. Sodann wird der Daemon neu gestartet und letztendlich noch eine Mail an root auf einem zentralen Logserver gesendet.

Nun wollen wir erreichen, dass dieses Script zweimal täglich, nämlich um 11.30 und 23.30 Uhr, ausgeführt wird. Dazu rufen wir die globale `cron` Konfigurationsdatei `/etc/crontab` in einem Editor auf oder (besser!) editieren sie mit dem Kommandoaufruf `crontab -e` (siehe auch Abschnitt 6.2) und fügen am Ende die Zeilen

```
30 11 * * * /sbin/check-sshd
30 23 * * * /sbin/check-sshd
```

ein. Das (etwas sperrige) Format der `crontab` Dateien verdient nähere Aufmerksamkeit; die Bedeutung der sechs leerzeichengetrennten Felder (siehe auch Folie 58) ist der Reihe nach: Minute (0-59), Stunde (0-23), Tag des Monats (1-31 oder Name), Monat (1-12), Tag der Woche (0-7 oder Name), auszuführendes Programm.
Mit einem `*` – wie in unserem Fall – zeigt frau an, dass das jeweilige Feld alle Werte annehmen kann. Weitere Möglichkeiten des Feldformats sind

- Explizite Auflistung (zB `5,9,13` für die Stunde)
- Intervalle (`5-9`)
- Kombinationen daraus (`4,7-19,23`)
- eigene Schrittweiten mittels `wert/schritt` (`5-10/2` in Spalte 2 bedeutet von 5 bis 10 Uhr in 2 Stunden-Abständen)
- Kombination von `*` und Schrittweiten (`*/2` jede 2. Stunde)
- Kombinationen aus allen obigen

Mit diesem Wissen können wir unser Beispiel auf eine einzige Zeile reduzieren:
`30 11,23 * * * /sbin/check-sshd`
oder auch
`30 */12 * * * /sbin/check-sshd`.

Crontab-Syntax

Min	Std	T/M	Mo	T/W	
1	*	*	*	*	jede Stunde
/5	*	*	*	*	alle 5 Minuten
0,30	4	*	*	*	zweimal am Tag
22	17	1	*	*	einmal im Monat
17	17	*	*	1	einmal pro Woche
15,45	9-18	*	*	*	24 mal am Tag
11	11	11	11	*	einmal im Jahr
59	23	1	1	6	jeden Samstag und jeden 1.1.

Folie 58

Systemcrontab (2)

```
# less /etc/crontab
  SHELL=/bin/bash
  PATH=/sbin:/bin:/usr/sbin:/usr/bin
  MAILTO=root
  HOME=/
  # run-parts
  01 * * * * root run-parts /etc/cron.hourly
  02 4 * * * root run-parts /etc/cron.daily
  22 4 * * 0 root run-parts /etc/cron.weekly
  42 4 1 * * root run-parts /etc/cron.monthly
```

Folie 59

6.2 Benutzung von `cron`, `at` und `batch`

Wie oben erwähnt, kann jeder User ein eigenes Crontab File anlegen und so Cronjobs ausführen lassen. Zum Bearbeiten von Crontab Dateien verwendet man am besten das Werkzeug `crontab`, das dem direkten Editieren der Datei in `/var/spool/cron` vorzuziehen ist. `crontab` kennt mehrere Optionen, darunter `-e` zum Editieren der `cron` Tabelle des Benutzers, die – sobald gespeichert – auch aktiviert wird. Mit dem Parameter `-l` kann man sich die `cron` Einträge ansehen (listen) und mit `-r` die gesamte Datei löschen (remove). KDE bietet auch einen grafischen „Taskmanager“ names `kcron` zur Verwaltung von Cronjobs an.

`at` und `batch` werden über ein Spool System verwaltet. Dadurch ergeben sich ähnliche Bedienungsmuster wie beim Drucken (vgl. Kapitel 7). Man kann zB durch `at -f script zeit` ein Script zu einer bestimmten Zeit ausführen. Es sind mehrere Zeitformat erlaubt zB HH:MM (2-stellige Stundenangabe: 2-stellige Minutenangabe), DD.MM.YY (2-stellig Tag.Monat.Jahr) und das handliche `now + n min` oder `4pm + 3 days`. Auf jeden Fall lohnt sich ein Blick in die Manpage.
Das `batch` Kommando funktioniert völlig analog. Die `at` Queue kann man mittels `atq` bzw. `at -l` ansehen. Aufträge löscht man mit `atrm`.

Den Output eines `cron-`, `at-` oder `batch-` Jobs erhält der entsprechende Auftraggeber, sofern (etwa wie im Script oben) nichts anderes angegeben ist als Mail an den lokalen Account; d.h. der Standardoutput eines solchen Jobs wird in eine Mail umgeleitet.
Oft ist es wünschenswert, bestimmten Usern zu verbieten, eigene `cron` oder `at` Einträge bzw. Jobs anzulegen. Dazu existieren die Dateien `/etc/{cron|at}.{allow|deny}`, wobei jeweils die `allow` Datei stärker ist, d.h. was in den `allow` Dateien steht, hat höhere Priorität. Ein Eintrag in diesen Dateien besteht einfach aus einem Usernamen. Standardmäßig ist es den privilegierten Pseudobenutzern (zB `bin`, `daemon`, ...) aus vernünftigen Gründen verboten, `at` Jobs auszuführen, allen anderen Benutzern erlaubt.

`crontab` bearbeiten

- crontab listen
  `crontab -l`
- crontab editieren
  `crontab -e`
  default=`vi`, mittels Umgebungsvariable EDITOR konfigurierbar
- crontab löschen
  `crontab -r`
- GUI: `kcron` (Taskmanager des KDE)

Folie 60

at-Jobs

- Jobs in Queue eintragen:

```
# at 4am (now+xx min)
  who
  CTRL d
# at -f myatjob 16:00 + 2 days
```

  Output als Mail an Auftraggeber
- Queue listen: `atq, at -l`
- Job löschen: `atrm jobnr, at -d jobnr`

Folie 61

batch-Jobs

- Kommando ausgeführt wenn Systemlast gering (default < 0.8)
- Jobs in Queue eintagen: analog `at`

```
$ batch
at> echo System wenig ausgelastet
<CTRL d>
```

- Output als Mail an Auftraggeber
- Jobs listen/löschen: `atq, atrm`
- Zugangsbeschränkung zum `atd`
  - `/etc/at.allow` (stärker)
  - `/etc/at.deny`

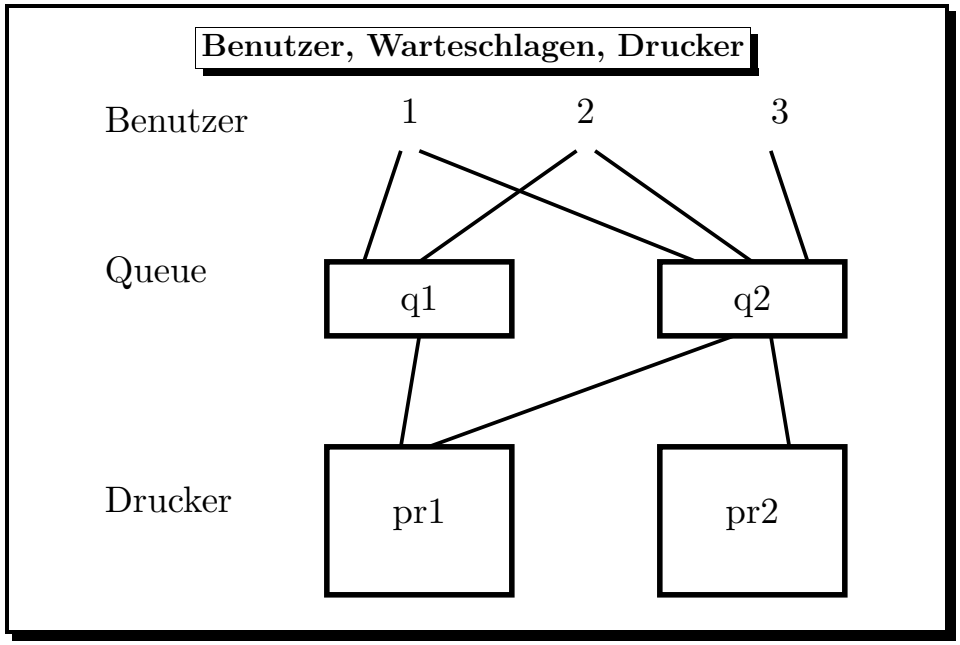
Folie 62

7 Drucker

In diesem Kapitel erklären wir die Grundlagen des Druckerwarteschlangenkonzepts (Queuings) unter Unix/Linux und besprechen den unter Linux häufig verwendeten BSD Druckerdaemon `lpd` sowie seine Erweiterungen LPRng und Cups. Außerdem erklären wir das praktische Vorgehen beim Installieren sowohl eines lokalen wie auch eines Netzwerkdruckers und das Verwalten von Druckerwarteschlangen.

Oft kann es zweckmäßig sein, die eigenen Kreationen, Dokumentation oder Konfigurationsdateien nicht nur am Bildschirm zu betrachten, sondern als „Hardcopy“ in Händen zu halten, also auszudrucken. In Multiusersystem wie Unix sind folgende Überlegungen relevant: Was geschieht, wenn zwei User gleichzeitig eine Datei an den Drucker senden. Welcher der beiden sollte im System die höhere Priorität haben? Wie kann man sicherstellen, dass die Ausdrucke der beiden nicht durcheinander geraten?
Überlegungen wie diese führen zum Konzept des *Druckservers*. Man schickt die zu druckende Datei nicht direkt an den Drucker, sondern an einen Druckerdaemonen (*Spooler*), der in einer FIFO- (First In First Out) Warteschlange (engl.: Queue) die Druckaufträge verwaltet und (je nach Priorität) alle Aufträge abarbeitet, bis die Queue leer ist. Unter Linux kommt hier meistens ein Daemon namens *lpd* (Line Printer Daemon) bzw. ein Paket namens `lpr` (Line Printer) zum Einsatz, der ursprünglich für *BSD* Unix entwickelt wurde. Meist wird der vom Server `lpd` definierte Standard als LPD Protokoll bezeichnet.

Trotz des Namens unterstützt LPD beinahe alle Arten von Druckern, die sich einerseits durch die Art, wie sie drucken (Tintenstrahler, Laserdrucker, ...), andererseits durch die Art des Anschlusses an den Rechner (parallele Schnittstelle, Netzwerkdrucker) charakterisieren lassen. Einzig von sogenannten *GDI*-Druckern (Graphical Device Interface) sollte man unter Unix/Linux die Finger lassen. Verschiedene Hersteller wollten diese Drucker möglichst kostengünstig produzieren und haben daher beinahe die gesamte Steuerung des Druckvorganges dem PC überlassen; daher benötigt man unbedingt die Hersteller-Treiber, die aber – bis auf wenige Ausnahmen – nur für Windows-kompatible Betriebssysteme existieren.



Folie 63

Auf neueren Linux-Systemen (zB RedHat ab 7.0) wird anstatt des BSD-Systems der LPRng (lpr Next Generation) verwendet, der eine Erweiterung von LPD darstellt und (fast) 100%ig rückwärtskompatibel ist.

Ein anderes modernes Drucksystem ist *Cups* (Common Unix Printing System), das das Internet Printing Protocol (IPP) benutzt und (eingeschränkte) Kompatibilität mit sowohl lpd als auch SMB und AppSocket (a.k.a. JetDirect) besitzt. Es besteht eine hohe Wahrscheinlichkeit, dass IPP respektive Cups in Zukunft die Standards für Drucken in Netzwerksystemen resp. auf Unix-Systemen setzen werden.

Drucksysteme unter Linux

- BSD Drucker-Spooling-Mechanismus (`lpr`)
  - gut dokumentiert und verstanden
  - wenig flexibel
- LPRng (lpr Next Generation)
  - Erweiterung des BSD-Systems
  - rückwärtskompatibel
  - `http://www.lprng.com`
- Cups (Common Unix Printing System)
  - verwendet Internet Printing Protocol (IPP)
  - einfach konfigurierbar/administrierbar
  - `http://www.cups.org`

Folie 64

7.1 Das Drucksystem

Das *BSD* Drucksystem ist – wie viele andere Unix-Dienste – ein Client/Server System. Wenn der Server (beim Bootvorgang) gestartet wird, liest er seine Konfigurationsdatei `/etc/printcap` ein, in der alle dem System zur Verfügung stehenden Drucker mit ihren jeweiligen Optionen (lokal, remote, ...) aufgelistet sind.

Wie sieht nun ein typischer Linux-Druckvorgang aus? Als erstes teilt man dem Client-Prozess *lpr* die zu druckende Datei mit; das geschieht entweder direkt an der Kommandozeile oder aus einer beliebigen Anwendung heraus. `lpr` überprüft nun, in welche Queue er den Auftrag stellen soll. Dazu sieht er zuerst nach, ob diese explizit dem *lpr* Kommando übergeben wurde (Syntax: `lpr -P Queue file`). Wenn dem nicht so ist, wertet er die Umgebungsvariable `PRINTER` aus. Falls diese nicht gesetzt sein sollte, nimmt er den Drucker aus `/etc/printcap`, der `lp` heißt bzw. wenn dieser auch nicht vorhanden sein sollte, den ersten Druckereintrag in dieser Datei.
Hat der Client auf diesem Weg nun die Queue bestimmt, sieht er in der `/etc/printcap` nach, welches *Spool*-Verzeichnis der Queue zugeordnet ist. Dieses Directory befindet ist gewöhnlich `/var/spool/lpd/`. Er legt dort jeweils eine Kontrolldatei mit Informationen über den Druckjob und die eigentlich zu druckende Datei ab und benachrichtigt den Druckerdaemon davon. Dieser entscheidet durch den Druckereintrag in der Konfigurationsdatei die weitere Vorgehensweise. Wenn der Drucker remote (über Netzwerk) angesteuert wird, dann leitet er den Auftrag an den entfernten Druckserver weiter. Wenn lokal (also zB über die parallele Schnittstelle) gedruckt wird, dann übergibt er den Auftrag, wenn er in der Queue an der Reihe ist, direkt oder über einen Druckfilter, der die Daten möglicherweise in ein anderes Dateiformat (zB Postscript) konvertieren muss, an die Druckerhardware. Die in `/var/spool/lpd/` temporär angelegten Dateien werden nach dem erfolgtem Ausdruck wieder gelöscht.

Drucksystem: Grundlagen

- Client/Server System `lpr/lpd(cupsd)`
- Benutzer erzeugt Druckauftrag mittels `lpr`
- `lpr`-Syntax: `lpr [-P Queue] file`
  Kommandozeile oder aus Anwendung
- `lpr` sendet Druckauftrag an Warteschlange `/var/spool/lpd/`
- `lpd` wartet auf Benachrichtigung von `lpr`
- `lpd` arbeitet Druckaufträge in der Reihenfolge des Eintreffens gemäß seiner Konfiguration über die Drucker ab

Folie 65

Drucksystem: Weitere Funktionen

- mehrere Warteschlangen für einen Drucker
- mehrere Drucker von einer Warteschlange bedient
  (nur LPRng, Cups)
- Verschieben von Aufträgen zwischen Warteschlangen
- Prioritätensetzung für Druckaufträge
- Authentifizierung
- Accounting

Folie 66

Der *LPRng Druckserver* – der ebenfalls schlicht und einfach `lpd` heißt – berücksichtigt neben `/etc/printcap` auch die Konfigurationsdatei `/etc/lpd.conf`, die eine wesentlich umfangreichere und feinere Konfigurationsabstimmung erlaubt; siehe dazu die entsprechende Manpage. Eine wesentliche Neuerung von LPRng ist, dass der Druckserver in der Lage ist, Warteschlangen zu verwalten, die mehr als einen Drucker bedienen und dass das Verschieben von Druckaufträgen zwischen verschiedenen Queues wesentlich erleichtert wurde. Die Clientkommandos des LPRng sind gegenüber den BSD-Kommandos nur minimal verändert.

Der *Cups Druckserver* heißt `cupsd` und wird grundlegend anders konfiguriert als der BSD-Server und seine Abkömmlinge. Die Konfigurationsfiles befinden sich im Verzeichnis `/etc/cups/` und die primäre Konfigurationsdatei heißt `/etc/cups/cupsd.conf`; ihre Syntax ist der Syntax der Konfigurationsdateien des Webservers Apache (siehe Kapitel 17) verwandt. Cups speichert alle verfügbaren Queues in `/etc/cups/printers.conf` und in `/etc/cups/ppd/` wird die Konfiguration für jede Queue in einem eigenen File namens `queue.ppd` verwaltet. Cups verfügt über ein Webinterface zur Druckerverwaltung, das auf Port 631 (also unter `http://myhost:631`) erreichbar ist, per Default aber nur vom lokalen Rechner aus angesprochen werden kann. Cups emuliert die BSD Clientkommandos; sie können also ganz wie unter BSD verwendet werden (und nicht nur mit dem Cupsserver zusammenarbeiten, sondern auch mit einem LPR(ng) Server, der auf einem entfernten Rechner in einem Netzwerk läuft; siehe unten). Darüber hinaus bietet Cups auch weitere unter BSD nicht verfügbare Clientkommandos; nähere Information dazu findet sich unter `http://myhost:631/documentation.html`.

Schließlich bietet KDE ein eigenes Drucker Clientkommando namens `kprinter`, das sich im Wesentlichen genau wie `lpr` verhält.

Benutzerkommandos (BSD, LPRng, Cups)

- Drucken
  - `lpr [-P queue] filename`
  - `pr filename | lpr [-P queue]` (formatiert Textdateien)
- Warteschlange listen `lpq [-P queue]`
- Druckaufträge löschen `lprm [-P queue] jobnr`
- Standarddrucker festlegen `export PRINTER=queue`

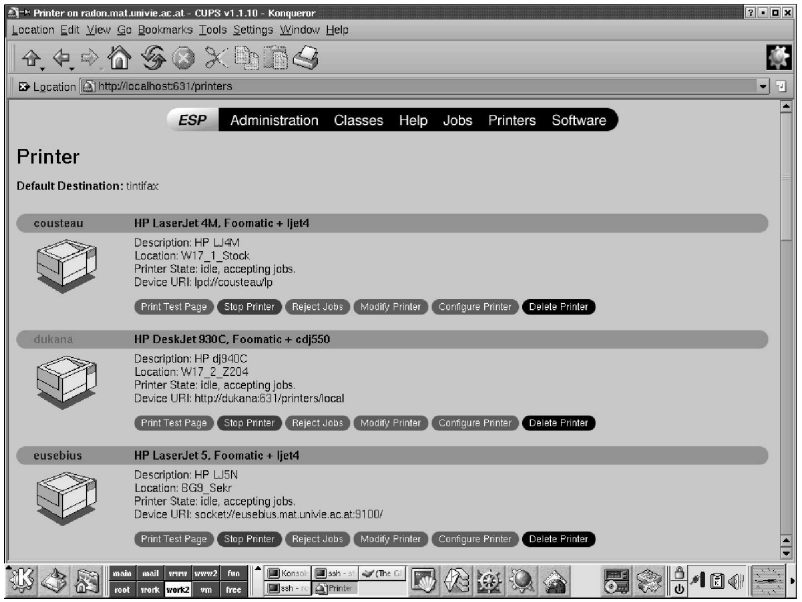
Folie 67

Die Printcap-Datei (BSD, LPRng)

```
# /etc/printcap
#
# Please don't edit this file directly unless you
# know what you are doing!
#
lp|local|Local Printer:\
       :sd=/var/spool/lpd/local:\
        :mx\#0:\
        :sh:\
        :lp=/dev/lp0$:\
        :if=/var/spool/lpd/local/filter:
#
lp|zra|W17 2.Stock|HP 2000 TN:\
        :sd=/var/spool/lpd/zra:\
        :mx\#0:\
        :sh:\
        :rm=zra.mat.univie.ac.at:\
        :rp=lp:\
        :if=/var/spool/lpd/zra/filter:
```

Folie 68

Cups Web-Interface



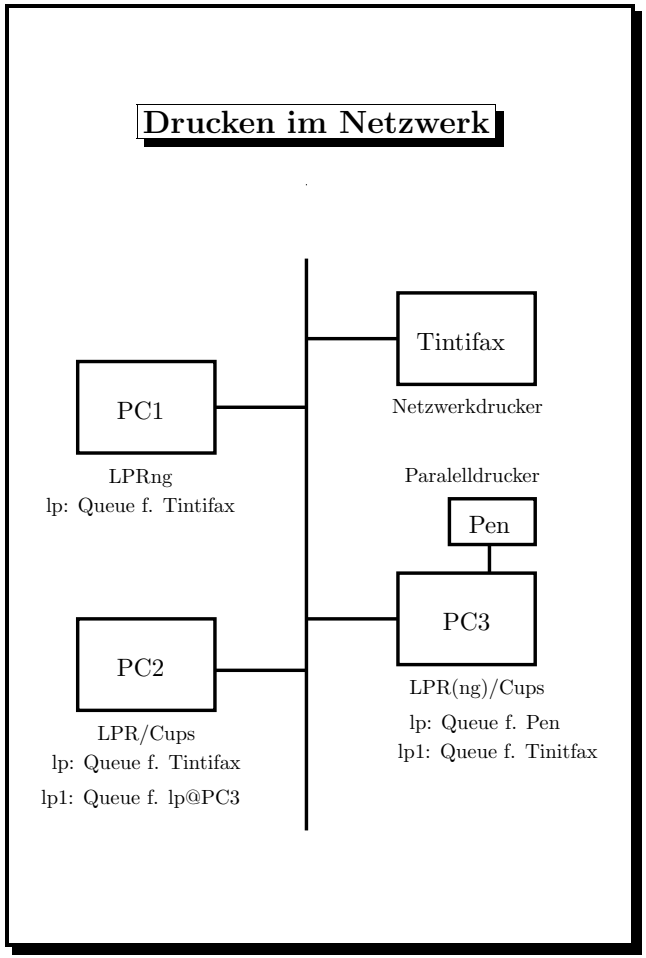
Der BSD Druckserver `lpd` kann eine lokale Druckerqueue nicht nur lokalen Benutzern zur Verfügung stellen, sondern auch den Zugang über ein *Netzwerk* ermöglichen. Dieser wird über die Dateien `/etc/hosts.lpd` oder `/etc/hosts.equiv` (regelt auch den Zugang zu den „alten“ Unix-„r-Diensten“, wie `rlogin` und `rcp`; siehe Kapitel 15) und einen Eintrag in `/etc/printcap` geregelt. In einem der beiden ersteren Files werden die Hostnamen der berechtigten Druckerclients angegeben. Wird zusätzlich in der Printcapdatei eine Queue mit der Option `rs` versehen, so wird die Verwendung ebendieser nur Benutzern erlaubt, die auch auf dem lokalen System einen Account besitzen. Unter LPR muss aber immer am lokalen Rechner eine Queue eingerichtet werden, die den entfernten Druckserver bedient (siehe auch Folie 70).
Die Netzwerk-(und auch die lokalen Berechtigungen) für den LPRng `lpd` können sehr fein abgestuft in der Datei `/etc/hosts.perms` vergeben werden; siehe auch dazu die entsprechende Manpage. Wesentliche Neuerung des LPRng `lpr`-Clientkommandos ist, dass damit auch Remotequeues bedient werden können, d.h. mit der Syntax `lpr -P Queue1@serverhost file` kann ein Druckauftrag an die Queue1 an den `lpd` auf dem Host mit Namen serverhost (das Vorhandensein der entsprechenden Berechtigung vorausgesetzt) gesendet werden. Das hat zur Folge, dass der LPRng Druckerdaemon nur auf Systemen laufen muss, auf denen das tatsächliche Queuing oder Drucken stattfindet und die unter BSD nötige Einrichtung einer lokalen Queue entfällt.
Der Netzwerkzugang zum Cups Druckerserver wird in `/etc/cups/cupsd.conf` (über eine Allow-Directive) geregelt.

Netzwerkdrucker – also Drucker die nicht an der parallele oder sonstige Schnittstelle eines PCs angeschlossen sind, sondern über eine Netzwerkkarte (etwa: JetDirect) oder einen eigenen (Hardware)Printserver (etwa Print Mate) verfügen – unterstützen in (fast) allen Fällen LPR und können vom einem Clientrechner wie ein LPD Druckserver angesprochen werden. Es sollte aber auf jeden Fall eine lokale Queue für den Netzwerkdrucker eingerichtet werden.

Netzwerkdruckserver

- BSD `lpd`
  Clients müssen am Server explizit angegeben werden
  `/etc/hosts.lpd` (nur Druckerclients)
  `/etc/hosts.equiv` (lpd, rlogind, ect...)
  `rs` Option im Printcapfile
- LPRng `lpd` feinere Abstimmung
  `/etc/lpd.perms`
  `/etc/lpd.conf`
- LPRng `lpr` Client kann Remotequeues bedienen
  `lpr -P Queue1@host file`
  LPRng `lpd` daher nur nötig auf Hosts wo Drucker oder Queue
- `cupsd` Netzwerkzugang in `/etc/cups/cupsd.conf` geregelt

Folie 69



Folie 70

7.2 Druckeradministration

Steht ein Druckjob einmal in der Queue, die man mittels `lpq` ansieht, kann er einerseits mittels `lprm Jobnr` auch wieder daraus entfernt werden (wenn der Druckauftrag dem User gehört, der diesen Befehl ausführt; root darf durch Eingabe von `lprm -` alle Jobs löschen). Die Jobnummer erfährt man durch das `lpq`-Kommando, das den Inhalt der Druckerqueue, also die anstehenden Druckjobs ausgibt. Siehe dazu auch Folie 71. Bei jedem dieser Befehle muss die zu bearbeitende Queue (falls es nicht die Defaultwarteschlange ist) explizit mittels der Option `-P queue` angegeben werden.

Die Kommandos `lpq` und `lprm` stehen sowohl unter LPD, LPRng als auch Cups zur Verfügung. Ebenso das generelle Kommandozeilen Administrationstool `lpc` (Line Printer Control Programm), mit dessen Hilfe der Administrator Druckaufträgen eine höhere Priorität als anderen einräumen, die Reihenfolge der Aufträge in der Queue verändern oder den Status (Drucken, Queuing en/disablen) einer Warteschlange verändern und abfragen kann. Für die `lpc` Syntax siehe Folie 73; das Kommando bietet auch einen interaktiven Bedienmodus an. Das Cups `lpc` bietet nur eine sehr eingeschränkte Funktionalität; *das* Kommandozeilentool unter Cups zum Konfigurieren und Administrieren von Druckerwarteschlangen ist `lpadmin`, die Queues können aber selbstverständlich auch über das Webinterface verwaltet werden. Für Details siehe die entsprechenden Manpages und die Cups Online Dokumentation unter `http://localhost:631/documentation.html`.

Darüber hinaus gibt es grafische Programme zur Verwaltung der Warteschlangen (aller Server) wie etwa `klpq` im KDE.

Druckerwarteschlange manipulieren

```
[roli@pablo tmp]$ lpq
ken is ready and printing
Rank    Owner   Job     File(s)                 Total Size
active  roli    35      blue_angle_swirl.jpg    12288 bytes
1st     roli    36      bluegreencrisscross.jpg 19456 bytes
2nd     roland  65      yp.conf                  1024 bytes
3rd     root    66      cupsd.conf              18432 bytes
[roli@pablo tmp]$ lprm 36
[roli@pablo tmp]$ lpq
ken is ready and printing
Rank    Owner   Job     File(s)                 Total Size
active  roli    35      blue_angle_swirl.jpg    12288 bytes
1st     roland  65      yp.conf                  1024 bytes
2nd     root    66      cupsd.conf              18432 bytes
```

Folie 71

Druckermanagement

- mit dem `lpc` Kommando
  - Druckerstatus anzeigen
  - Drucker en/disablen
  - Queue en/disablen
  - Druckaufträge löschen
  - Druckauftrag an die Spitze einer Queue stellen
  - Signale an lpd senden
- GUI `klpq`, ...

Folie 72

lpc-Syntax

- Kommandozeile: `lpc [Optionen] [Kommando [Argument]]`
  - Optionen: `-P Queue, -a=-P all`
  - Kommandos: start, stop, status, redirect, topq, lprm
    (nur LPRng): move Queue1 [jobid] Queue2
- Interaktiver Modus

```
$ lpc
lpc$>$ start lp
lpc$>$ status lp
lpc$>$ exit
$
```

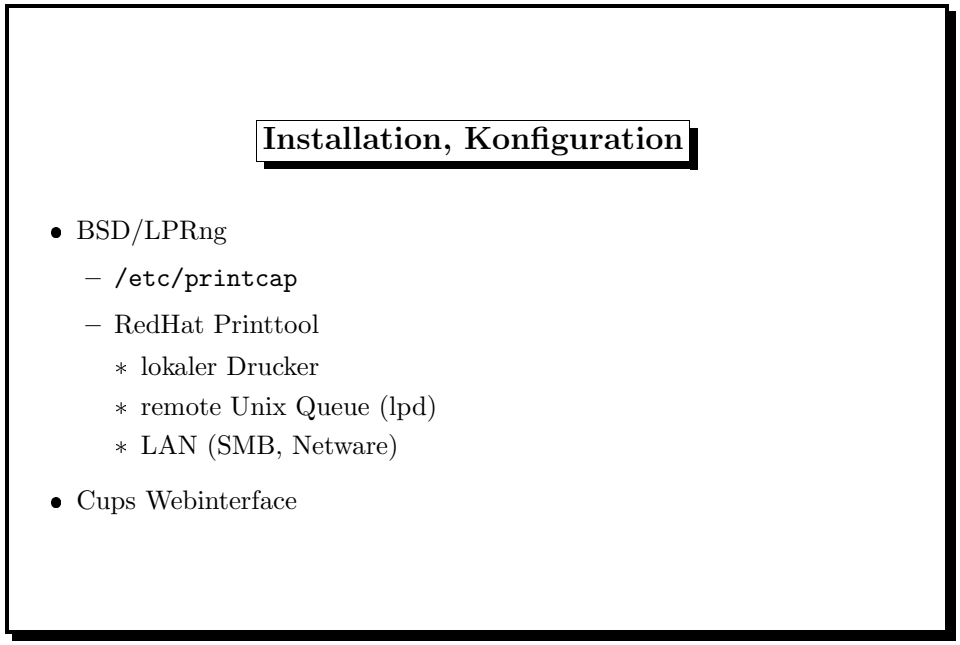
Folie 73

Das direkte *Einrichten eines neuen Druckers* über die Datei `/etc/printcap` ist eine eher komplizierte Angelegenheit. Daher bietet sich der Weg über zusätzliche (graphische) Tools wie `printtool` (RedHat) oder Administrationsschnittstellen anderer Distributionen (zB YaST) oder anderer zB auf `freshmeat.net` verfügbarer Programme an.
Wer dennoch den „steinigen“ Weg gehen will, muss über die Syntax der Datei Bescheid wissen. Das erste Feld enthält die Namen, unter denen die Queue ansprechbar sein soll, jeweils durch | separiert. Die darauf folgenden Optionen haben die Form `keyword=value` und müssen durch Doppelpunkte getrennt sein. Jeder Druckereintrag sollte mindestens die Felder (siehe auch Folie 68)

```
:sd=/pfad/zur/queue
:lf=/var/log/lpd-errors
:lp=/dev/parport0
```

enthalten, wobei `sd` für das Spool Directory, `lf` für Logfile und `lp` für die Hardwareschnittstelle zum Drucker steht. Handelt es sich um einen nichtlokalen Drucker (Netzwerkdrucker; Druckserver auf entferntem Rechner) so ist der `lp`-Eintrag durch `rm=hostname` (Remote) und `rp=queue` (Remote Printer) zu ersetzen. Weitere wichtige Felder (etwa `if` oder `sh`) können bei Bedarf in der Manpage von `printcap` nachgesehen werden. Anschließend muss man noch das Spoolverzeichnis erstellen und die Rechte dort richtig setzen.

LPRng bietet auch die Möglichkeit, mittels `checkpc` zu überprüfen, ob der Druckereintrag korrekt ist. Unter Cups schließlich kann das Installieren eines neuen Druckers einfach über das Webinterface erfolgen.



Folie 74

8 Dateisysteme

Hier wiederholen wir kurz die Festplattenpartitionierung, erklären den praktischen Umgang mit Dateisystemen, stellen das Standard-Linux-Dateisystem `ext2` vor und erwähnen andere von Linux unterstützte Dateisysteme. Wir besprechen die Grundlagen von Journaling-Filesystemen und die zwei Beispielsysteme `ext3`, und ReiserFS.

8.1 Praktischer Umgang mit Dateisystemen

Partitionierung
Auf Intel-basierten Systemen werden Festplatten in logische Bereiche unterteilt; diese *Partitionen* (vgl. Teil 1, Abschnitt 8.2) können wie eigene Festplatten angesprochen werden und unterschiedliche Dateisysteme beinhalten. Achtung beim Partitionieren gehen alle Daten auf dem Datenträger verloren (es gibt auch Tools, bei denen in eingeschränktem Ausmaß Daten erhalten bleiben; es ist aber empfehlenswert, trotzdem ein Backup zu machen). In der Regel wird die Partitionierung beim Installationsvorgang erledigt und später nur freigelassener Plattenplatz oder neue Platten partitioniert.
Unter Linux ist `fdisk` das Standardwerkzeug zur Partitionierung (vgl. Teil 1, Abschnitt 8.3); ein etwas einladenderes Look and Feel bietet `cfdisk` und der RedHat-Installer verwendet per Default den Disk Druid. Beim Partitionieren muss der Typ der Partition angegeben werden. Dieser Typ entspricht dem auf dieser Partition einzurichtenden Dateisystem – also zB Linux (für ext2) oder FAT für DOS und VFAT für Windows 9x.
Eine kurze Wiederholung der Grundlagen der Partitionierung (unter Linux) findet sich auf Folie 75.

Dateisysteme erzeugen
Auf einer neu erstellten Partition muss nun ein (zunächst leeres) *Dateisystem* erzeugt werden, auf dem die Daten gespeichert werden können; dieser Schritt wird auch *Formatieren* genannt. Klarerweise muss der Partitionstyp mit dem Filesystemtyp übereinstimmen. Details über den Aufbau von Dateisystemen und vor allem den Standardtypen, die unter Linux verwendet werden besprechen wir in eigenen Abschnitten.

Partitionierung

- maximal vier primäre Partitionen
- davon maximal eine als erweiterte Partition
- Erweiterte Partitionen sind Behälter für (max. 12) logische Partitionen
- alle Partitionen (logisch oder primär) lassen sich gleich ansprechen
- Partitionstypen bezeichnen das verwendete Dateisystem
- Namensgebung unter Linux
  - IDE: `/dev/hd[a-h]`, SCSI: `/dev/sd[a-z]`
  - primär: `/dev/?d?[1-4]`
  - logisch: `/dev/?d?[5-16]`

Folie 75

Unter Linux können nicht nur eine Vielzahl verschiedener Dateisysteme (Überblick auf Folie 81, genaueres in Abschnitt 8.2) verwendet, sondern auch erstellt werden. Das Programm `mkfs` (Make File System) ist ein Front-End für die verschiedenen Programme, die dann tatsächlich die Dateisysteme verschiedenen Typs erzeugen: Die Syntax ist:

```
mkfs [-t FsType] [FsOptions] Device
```

Das `Gerät` (Device) ist üblicherweise eine spezielle *Gerätedatei*, über die die Hardware (zB Festplattenpartition `/dev/hda1` oder Floppy `/dev/fd0`) angesprochen wird. Der Filesystemtyp `FsType` wird hier ein für alle mal festgelegt und kann später im laufenden Betrieb nicht verändert werden (ohne die am Filesystem gespeicherten Daten zu verlieren).
Festplattenpartitionen unter Linux werden meist mit dem 2nd extended Filesystem (Option `ext2`; wird in Abschnitt 8.3 detailliert behandelt) formatiert, Disketten mit der Option `msdos` für DOS-formatierte Floppies, oder (wenn Dateiberechtigungen verwendet werden sollen) mit der Option `minix`.
Die `FsOptions` hängen freilich von `FsType` ab; unterstützt werden meistens: `-v` (verbose) für ausführliche Meldungen und `-c` (check) zum Prüfen auf defekte Blöcke.

Eine Liste der Blöcke eines Mediums, die sich nicht lesen lassen, erhält man auch durch `badblocks Gerät`; Schreibtests werden nur dann durchgeführt, wenn man die Option `-w` einsetzt. `mkfs -c` oder `badblocks` werden üblicherweise nur bei Disketten eingesetzt oder wenn man Probleme erwartet, da das ein sehr, sehr langes Lesen des gesamten Mediums erfordert (das DOS-Tool `format` macht dies immer). Bei vielen Dateisystemen ist das überflüssig, da defekte Blöcke beim Schreiben von Daten im laufenden Betrieb erkannt werden und dann nicht benutzt werden.

Man kann statt des Aufrufs des Front-Ends `mkfs` auch direkt die Programme verwenden, die die Formatierung durchführen zB `mkfs.ext2` = `mke2fs`, `mkfs.msdos`, etc. Die jeweiligen Optionen sind ausführlich in den Manpages dokumentiert.

Erstellen von Dateisystemen/Formatieren

- erstellt Strukturen des FS auf Partition
- bereitet die Partition auf den Einsatz vor
- Filesystemtyp muss mit Partitionstyp übereinstimmen
- kann später nicht mehr geändert werden
- Front-End für alle Typen:
  `mkfs [-t type] [-c] Device`
- Einzelne Tools:
  `mke2fs = mkfs.ext2 [Optionen] device` für Feintuning

Folie 76

Mounten
Einer der großen Vorzüge des Konzepts des Unix/Linux Verzeichnisbaums ist, dass er vollständig unabhängig von der zu Grunde liegenden Partitionierung der Festplatten des Systems immer die gleichen Verzeichnisse aufweist (vgl. das Laufwerk-Konzept unter MS-Windows). Verschiedene Festplattenpartitionen (sogar mit verschiedene Dateisystemtypen) können an beliebigen Punkten des Verzeichnisbaums „eingehängt“ oder „montiert“ werden; etwas technischer spricht man vom *Mounten* von Dateisystemen.
Dem Zugrunde liegt das sog. *virtuelle Dateisystem* von Unix/Linux, das den Zugriff auf die verschiedensten Medien vereinheitlicht, die für alle Programme völlig transparent als Verzeichnisse dargestellt werden. Ein Programm muss nicht wissen (und weiß auch nicht!), auf welchem Medium die Datei liegt, die es gerade schreibt oder liest. Ein weiterer Vorteil dieses Konzepts liegt darin, dass sich der Zugriff auf jedes Medium einfach über die Dateiberechtigungen steuern lässt.

Das Mounten von Dateisystemen ist prinzipiell root vorbehalten (Ausnahmen siehe unten) und wird mittels `mount`-Kommando bewerkstelligt; Syntax:

```
mount [-t FsTyp] Device Mountpoint
```

Hier Bezeichnet `Device` wieder die Hardwaregerätedatei für das entsprechende Medium. `Mountpoint` bezeichnet den Platz im Verzeichnisbaum, wo das entsprechende Gerät eingefügt werden soll. Dabei sollte es sich um ein *leeres* Directory handeln; ist es nicht leer, sieht man die darin befindlichen Dateien solange nicht, wie ein Medium auf das Verzeichnis gemountet ist. Üblicherweise reicht ein `mount Gerät Mountpoint`, um ein formatiertes Medium auf `Gerät` unter dem Namen `Mountpoint` ansprechen zu können, da `mount` den Dateisystemtyp selber festzustellen versucht. Andernfalls muss man mit `-t Typ` nachhelfen. Bei Medien, die man nicht schreiben kann (CDROMs) oder will (Backups), setzt man die Option `-r` für „read only“.

Braucht man ein Medium nicht mehr, hängt man es per `umount Gerät` oder `umount Mountpoint` (kein *n* obwohl „unmount“) wieder aus dem Verzeichnisbaum aus. Verwendet ein Programm noch Dateien auf diesem Medium oder ist sein Arbeitsverzeichnis (pwd) noch in einem Unterverzeichnis des Mediums, verweigert der Kernel das Aushängen. Da es *keine* `--force`-Option gibt, die ein Unmounten erzwingt (würde die Konsistenz des Filesystems gefährden), muss man zuerst die das Medium benutzende Programme schließen (oder töten). Die Tools `fuser` und `lsof` (List Open Files) zeigen, welche Programme das sind.

Die standardmäßig vom System verwendeten Festplattenpartitionen müssen natürlich nicht (mit oben beschriebener Syntax) händisch gemountet werden, sondern werden automatisch beim Systemstart gemountet. Genauer wird das Wurzelverzeichnis `/` in einem sehr frühen Stadium vom Kernel gemountet (vgl. Teil 1, Abschnitt 9.1, der Bootloader übergibt die Informationen über die Rootpartition an den Kernel, der einen Fallback-Default fix eincompiliert hat, der aber mit `rdev` geändert werden kann). Die weiteren Dateisysteme werden von `/etc/rc.sysinit` nach eventuell durchzuführenden Filesystemchecks gemäß dem in der Datei `/etc/fstab` vorgegebenen Schema an die entsprechenden Stellen im Verzeichnisbaum gemountet (mit einem Aufruf von `mount -a`). Eine Beispiel-Fstab befindet sich auf Folie 78. Jede Zeile beschreibt die Verwendung eines Gerätes; als Trennzeichen zwischen den Einträgen können Leerzeichen und Tabs verwendet werden. Die Reihenfolge ist: Gerät, Mountpoint, Dateisystem, Optionen, dump-Eintrag (veraltet), fsck-Eintrag. der Geräteeintrag kann die Gerätedatei (zB `/dev/hda7`), `none` (für virtuelle Dateisysteme wie `proc` oder ein *Label* sein. (Jede `ext2`-Partition kann durch ein sog. Label identifiziert werden; siehe `man e2label`). Der fsck-Eintrag bestimmt die Reihenfolge eventuell durchzuführender Filesystemchecks; 0 bedeutet keinen Prüfung. Einträge mit der Option `noauto` werden nicht automatisch (von `mount -a`) gemountet, sondern dienen zum definieren von Standardmountpoints zB für Floppy und CDROM, d.h. ruft man `mount` auf und lässt `Gerät` oder `Mountpoint` weg, wird das fehlende Argument mit Hilfe der `/etc/fstab` ergänzt.

Üblicherweise erlaubt der Kernel nur `root` Medien zu mounten, das SUID-Programm `mount` erlaubt aber auch normalen Benutzern `/etc/fstab`-Einträge zu nutzen, falls die Option `user` eingetragen ist. Ist die Option `owner` gesetzt, so kann außer root auch (und nur) der Besitzer der Gerätedatei den Mount ausführen; dieser Mechanismus wird von den Desktopsystemen genutzt: Loggt sich ein Benutzer auf der grafischen Oberfläche ein, wird er Eigentümer einiger Gerätedateien aus `/dev`, so zB von `/dev/cdrom` und `/dev/fd0`. `mount` erlaubt es dann diesem Benutzer die CDROM und die Floppy zu mounten, allerdings nur *genau* mit den Optionen in `/etc/fstab`; ist für `/dev/cdrom` als Dateisystem `iso9660` eingetragen ist, kann der Benutzer nur dann den Mount ausführen, wenn es sich wirklich um ein solches Dateisystem handelt. Für die Floppy ist meist `auto` für Dateisystemtyp eingetragen, was die Verwendung beliebiger Dateisysteme auf der Diskette ermöglicht. Für weitere Details siehe `man fstab`.

Das `mount`-Kommando schreibt bei jedem erfolgreichen (U)Mount eines Mediums eine Zeile nach dem Muster der `/etc/fstab` in die Datei `/etc/mtab`; diese enthält daher immer den aktuellen Stand über alle verwendeten Medien; ein `mount`-Aufruf ohne Optionen und Argumente wertet genau diese Informationen aus. Komfortabler zeigt `df` (Display Filesystem) die gemounteten Medien und eine Statistik über ihrer Benutzung.

Mounten/Unmounten

- mounten: `mount [-t FsType] Gerät Mountpoint`
- gemountete Dateisysteme listen
  - `mount`
  - `df`
  - `less /etc/mtab`
- unmounten: `umount Gerät` *oder* `Mountpoint`
  - FS darf nicht geöffnet sein (Files, Programme, Directories)
  - `fuser`, `lsof` zeigt Prozesse, die FS verwenden
  - kann **nicht** erzwungen werden!!

Folie 77

/etc/fstab

```
/dev/hda2     /              ext3    defaults         1 1
/dev/hda1     /boot          ext3    defaults         1 2
none          /dev/pts       devpts  gid=5,mode=620   0 0
none          /proc          proc    defaults         0 0
none          /dev/shm       tmpfs   defaults         0 0
/dev/hda3     swap           swap    defaults         0 0
/dev/cdrom    /mnt/cdrom     iso9660 noauto,owner,ro  0 0
/dev/fd0      /mnt/floppy    auto    noauto,owner     0 0
```

Folie 78

8.2 Dateien und Dateisysteme

Einschub: Gerätedateien
Jeder (unterstütze) Datenträger – wie prinzipiell jedes Hardwaredevice – wird unter Unix durch eine sogenannte Gerätedatei (Devicefile, eine spezielle Datei im Verzeichnis `/dev/`) dargestellt, über die der Zugriff auf das entsprechende Gerät erfolgt. Auf diese Weise sind keine speziellen Programme nötig, um (low-level) auf die Geräte zuzugreifen. Zum Beispiel kann man mittels

```
$ cat foo > /dev/lp0
```

den Inhalt der Datei `foo` auf dem Drucker (genauer der ersten parallelen Schnittstelle) ausgeben. Die Daten müssen klarerweise in einem Format sein, das der Drucker auch versteht. Da es, wie schon erwähnt, keine gute Idee ist, dass mehrere Benutzer direkt ihre Daten an den Drucker schicken, schaltet man eine Druckerwarteschlange (Queue) dazwischen (vgl. Kapitel 7). Das gilt für auch für die meisten anderen Geräte, weshalb man nur in den seltensten Fällen direkt auf die Gerätedateien zugreifen muss bzw. warum normalen Benutzern dafür auch die Rechte fehlen. Wir diskutieren im Folgenden kurz die Grundlagen im Umgang mit Gerätedateien.

Linux unterscheidet zwischen zwei Gerätearten: *Random-Access Block Devices* (zB Festplatte, CD-ROM) und *Character Devices* (zB Bandlaufwerk, Tastatur, Maus oder serielle Schnittstellen). Ein langes Listing zeigt bei jeder speziellen Datei, ob es sich um eine Block Device (b) oder ein Character Device (c) handelt; zB:

```
stein@dukana:stein;-) ls -l /dev/hda1 /dev/cua1
crw-rw----    1 root     uucp     5,  65 Aug 30  2001 /dev/cua1
brw-rw----    1 root     disk     3,   1 Aug 30  2001 /dev/hda1
```

Bei den meisten Systemen sind alle Gerätedateien vorhanden, unabhängig davon, ob das Gerät tatsächlich vorhanden ist. Nur weil man eine Datei `/dev/sda` am System hat, bedeutet das also nicht, das tatsächlich eine SCSI-Festplatte eingebaut ist. Die Dateien werden vom Installationsprogramm automatisch erstellt, sodass man sie beim Einbau eines neuen Geräts nicht „von Hand“ erzeugen muss (was auch eher kompliziert ist; das entsprechenden Kommando heißt `mknod`).

Gerätedateien

- jedes Gerät wird über eine Gerätedatei angesprochen
- es gibt zwei Arten von Geräten:
  - Random-Access Block Devices
  - Character Devices
- die Gerätedatei existiert auch, wenn es das Gerät nicht gibt
- Gerätedateien besitzen ganz normale Berechtigungen

Folie 79

Konsequenterweise haben auch die Gerätedateien Berechtigungen und können gelinkt werden. Dadurch kann man bestimmten Benutzern die Verwendung zB des Modems sehr leicht verbieten. Besitzer ist meistens root, bei Wechselmedien allerdings der lokal (unter X) angemeldete Benutzer. Symbolische Links bieten bequem eine Möglichkeit ein Standardgerät festzulegen; zB ist `/dev/cdrom` oft ein Link auf das entsprechende IDE-Gerät also etwa `dev/hdc`.

Was genau ist eine Datei?
Ein gewöhnliches File enthält ein Dokument (Text, Graphik, Datenbankfile) oder ein Programm. Die Files besitzen keine Satzstruktur, sondern werden als sequentielle Ströme von einzelnen Zeichen behandelt. Eine Blockstruktur, wie sie auf Disketten oder Festplatten vorhanden ist, ist für die Anwendung/den Benutzer nicht erkennbar. Jede Anwendung kann so ihre eigene Struktur definieren.

Was genau tut ein Dateisystem?
Die Aufgabe eines Dateisystems besteht darin, die einzelnen Datenblöcke einer Datei auf die Festplatte (oder einen anderen Datenträger) abzulegen. Es legt fest, an welcher Stelle des Datenträgers sie gespeichert werden sollen und archiviert diese Informationen – die sog. *Metadaten* – gleichzeitig in einer Tabelle.
Die Zugriffs- und Lokalisierungsstrategie eines Dateisystems hat direkten Einfluss auf die Durchsatzrate der Schreib- und Lesezugriffe auf das Medium und auf die Zuverlässigkeit des Dateisystems an sich.

Files und Filesysteme

- Eine Datei ist eine fortlaufende Anzahl von Bytes
  - unabhängig vom tatsächlichen Ort auf dem Speichermedium
  - kein interner Aufbau
- Ein Dateisystem verwaltet die Dateien auf einem Speichermedium
  - unabhängig von der Art der Speicherung
  - Metadaten beinhalten Verwaltungsüberbau

Folie 80

Dateisysteme unter Linux
Obwohl `ext2` das Standard Dateisystem unter Linux ist, kommt das Betriebssystem mit einer ganzen Reihe von Dateisystemen zurecht. Hier eine etwas ausführlichere – aber beileibe nicht vollständige – Übersicht (vgl. Folie 81):

- `ext2`: 2nd extenden Filesystem; der Standard unter Linux (Details siehe Abschnitt 8.3)
- `ext3`: 3rd extended Filesystem; Weiterentwicklung von `ext2`, Journaling (siehe Abschnitt 8.4)
- ReiserFS: Reiser-Dateisystem, nach seinem Schöpfer Hans Reiser benannt; Journaling (siehe auch Abschnitt 8.4
- JFS: Von IBM entwickeltes Journaling-Filesystem, ursprünglich für AIX (IBMs UNIX) entwickelt; seit Februar 2000 ist eine Open Source Version für Linux verfügbar. Die Entwicklung geht dank finanziellem Hintergrund von Big Blue sehr rasch von statten.
- XFS: Journaling-Filesystem unter UNIX. Ursprünglich von SGI für IRIX, aber mittlerweile unter der GPL in einer Beta-Version als Patch für Linux verfügbar. Ist neben JFS und ReiserFS ein weiterer aussichtsreicher Kandidat für den nächsten Journaling-Filesystem Standard.

- iso9660: Standardformat für CD-ROMs und DVDs. Es gibt hier verschiedene Erweiterungen (zB Rock Ridge Interchange Protocol), um etwa die 8.3 Beschränkungen aufzuheben.
- udf: Universal Disk Format (CDRWs und DVDs) ist die Weiterentwicklung von ISO9660 und heißt eigentlich ISO13346
- MS-DOS: Dateisystem für MSDOS-Partitionen (FAT12, FAT16, FAT32) und -Disketten (kurze Dateinamen). Es gibt, trotz gleichen Namens (FAT), einen Unterschied zwischen FAT12 und FAT16. Ersteres ist nur für Dateisysteme mit weniger als 16 MB, also für Disketten brauchbar.
- VFAT: DOS/Windows 9x-Dateisystem (lange Dateinamen)

- NTFS: Windows NT/2000 Dateisystem (nur Lesezugriff empfohlen)
- UMSDOS: Ein unixartiges FS das auf einer FAT Partition angelegt werden kann.
- minix: Dateisystem von Minix, wird oft für Linux-Disketten verwendet; war das erste Dateisystem für Linux, kann aber nur Dateisysteme mit max. 64MB und Dateinamen mit 30 Zeichen anlegen.
- NCPFS: Novell FS
- HPFS, HFS, AFFS: FS von OS/2 (wie schon OS/2 selbst, (fast) ausgestorben), MAC und Amiga
- Weitere in der Unix-Welt verbreitete FS wie `ext`, System V, Xenix, ...

- proc: virtuelles Dateisystem zur Prozessverwaltung (`/proc`).
- swap: Swap-Partitionen oder -Dateien; siehe Kapitel 5.
- autofs: für das automatische Mounten eines Dateisystems bzw. Datenträgers ins Gesamtsystem – also ebenso kein echtes Dateisystem
- usbdevfs: Einbinden und Verwalten von USB-Geräten
- devpts: für Pseudoterminals (nach UNIX-98-Spezifikation)

- NFS: Netzwerkdateisystem für UNIX, um Daten von anderen Rechnern zu lesen (siehe Kapitel 16)
- SMBFS: Samba (Netzwerkdateisystem unter Windows); siehe Kapitel 19

Wir besprechen in den folgenden Abschnitten das Standarddateisystem unter Linux, das 2nd extenden Filesystem (`ext2`), sowie die Journaling-Dateisysteme `ext3` (3rd extenden Filesystem) und ReiserFS.

Unterstützte Filesysteme

- `ext2`... 2nd extended FS, Linux-Standard
- ReiserFs, `ext3`... Journaling-FS für Unix/Linux
- JFS, XFS... Journaling-FS von IBM, SGI
- iso9660, udf ... (CDROM)
- FAT-12, -16, -32, VFAT... (WIN 3x, 9x)
- NTFS... Win NT (read only !?)
- minix, ext, xiafs, System V, Xenix, Coherent... Unix
- HPFS, HFS, AFFS... OS/2, Mac, Amiga (read only)
- UMSDOS... Unix like on top of MSDOS
- `/proc`... Linux Kernel und Prozessinfo (virtuelles FS)
- NFS... Network File System
- SMBFS... SMB
- NCPFS... Novell

Folie 81

8.3 Das `ext2`-Dateisystem

In diesem Abschnitt besprechen wir die Interna des 2nd extended Filesystems, d.h. die Art und Weise wie unter `ext2` die Dateien verwaltet werden und stellen einige Tools vor, mit denen ins Dateisystem eingegriffen werden kann.

Das `ext2`-Filesystem bewältigt seine Verwaltungsaufgabe, indem es den vorhandenen Speicherplatz in *Blöcke* gleicher Größe (Defaultwert 1024 Byte) einteilt und diese Blöcke durchnummeriert. Die Menge der Blöcke wird anschließend in verschiedene *Gruppen* aufgeteilt, die jeweils zur Speicherung unterschiedlicher Datentypen genutzt werden.
Wichtigste dieser Gruppen sind neben den Datenblöcken (wo die eigentlichen Daten gespeichert werden) die *Inodes* (Index Nodes, oder auch Informationsknoten), die mit Ausnahme des Dateinamens alle relevanten Daten über die gespeicherten Dateien enthalten, nämlich: Benutzer- und Gruppen-ID; Zugriffsrechte; Größe der Datei; Anzahl der (harten) Links, die auf diese Datei verweisen; Daten der Erstellung, der letzten Änderung oder des Löschens dieser Datei und Verweise auf die (ersten zwölf) Datenblöcke wo die Datei gespeichert ist. Die *Dateinamen* schließlich sind in den Verzeichnissen gespeichert; diese sind im Prinzip wie in Zeilen gegliederte Textdateien: jede Zeile beinhaltet den Name einer Datei (oder eines Unterverzeichnisses) und die zugehörige Inode-Nummer (siehe Folie 83). Zusätzlich findet sich in jedem Verzeichnis ein Verweis auf das Verzeichnis selbst (`.`) und das übergeordnete Verzeichnis (`..`).

Eine Datei besteht also aus ihrem entsprechenden Inode und aus mehreren Datenblöcken, die die eigentlichen Daten enthalten. Die Verwaltungsinformationen im Inode und der eigentliche Dateninhalt der Datei sind vollkommen getrennt und können auch unabhängig voneinander bearbeitet werden. Wird zB eine Datei in ein neues Verzeichnis verschoben, wird der Inode und die entsprechenden Verzeichniseinträge verändert, aber niemals werden Datenblöcke direkt verändert.

Das ext2-Filesystem

- aufgeteilt in Blöcke gleicher Größe (Defaultwert 1024 Bytes)
- 6 Gruppen von Blöcken: Bootblock, Superblock, Inode Bitmap, Datablock Bitmap, Inodes, Datablocks (Redundanz!)
- Wichtigste Bestandteile:
  - Superblock
  - Inode (Index Node, Informationsknoten)
  - (double, triple) indirekter Block
  - Datenblock

Folie 82

Mit diesem Hintergrundwissen sehen wir uns ein langes Listing eines Verzeichnisses an und Diskutieren die Dateiverwaltung an diesem Beispiel.

```
bash-2.04$ ls -ail
223244 drwxr-xr-x 4 jj users 1024 Jan 21 17:00 .
180247 drwxr-xr-x 3 jj users 1024 Jan 21 17:03 ..
 84002 drwxr-xr-x 2 jj users 1024 Jan 21 17:00 dir1
223245 drwxr-xr-x 2 jj users 1024 Jan 21 17:01 dir2
```

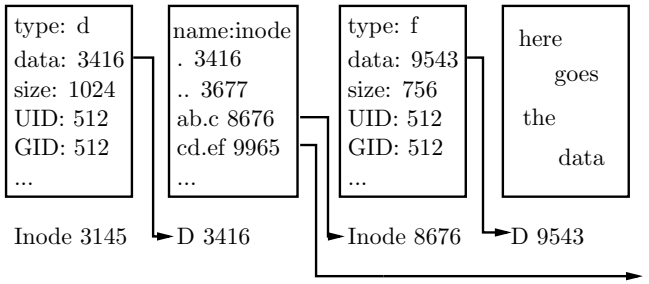
Von links nach rechts erklärt: Die linke Spalte gibt die Inode-Nummern an, unter der die Zeiger, Unterverzeichnisse oder Daten abgelegt sind. In der nächsten Spalte werden die Zugriffsrechte aufgelistet. Darauf folgt die Spalte mit der Anzahl harter Links, die auf diese Dateien oder Verzeichnisse zeigen (Linkcount). Eine Datei hat zwar nur einen Inode, aber in diesem können mehrere (harte) Links auf diese Datei gespeichert werden. Beispielsweise ist für das Unterverzeichnis `dir1` die Zahl von zwei Hardlinks angegeben. Konkret besagt dies: auf `dir1` verweist einmal `dir1` in `jj` und einmal `.` in `dir1`. Explizit:

```
bash-2.04$ cd dir1; ls -ail
 84002 drwxr-xr-x 2 jj users 1024 Jan 21 17:00 .
223244 drwxr-xr-x 4 jj users 1024 Jan 21 17:00 ..
```

Ein Inode kann mittels *Pointer* maximal 12 Datenblöcke direkt adressieren. Umfasst eine Datei mehr als 12 KByte (12 mal 1024 Byte oder zwölf Datenblöcke), kommt ein indirektes Adressierungsschema zum Einsatz. Jeder der 12 Pointer kann statt auf einen Datenblock auf einen *indirekten Block* zeigen, der weitere Pointer enthält. Nachdem ein Pointer 4 Bytes Speicherplatz verbraucht, kann jeder der indirekten Blöcke maximal 256 Pointer beinhalten, die entweder auf Datenblöcke oder auf weitere indirekte Blöcke verweisen. Letztere enthalten wiederum maximal 256 Pointer, die entweder auf Datenblöcke oder indirekte Blöcke zeigen. Nach dem dritten Level der indirekten Referenzierung ist aber Schluss: Man nennt Blöcke deren Pointer nur auf Datenblöcke zeigen *(einfach) indirekte Blöcke*, Blöcke deren Pointer auf (einfach) indirekte Blöcke zeigen *doppelt indirekte Blöcke* und schließlich Blöcke, deren Pointer auf doppelt indirekte Blöcke zeigen *dreifach indirekte Blöcke*; vierfach indirekte Blöcke sind nicht erlaubt.

Dateien und Verzeichnisse

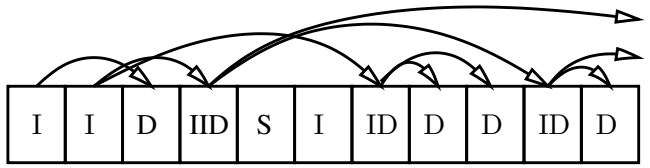
Verzeichnisse enthalten Tabellen: Dateiname – Inode



Folie 83

Indirekte Adressierung

- Inode zeigt auf ersten 12 Datenblöcke
- Indirekte Blöcke (ID): 256 Zeiger auf Datenblöcke
- Doppelt indirekte Blöcke (IID): 256 Zeiger auf ID
- 3-fach indirekte Blöcke (IIID): 256 Zeiger auf IID
- theoretische Maximalgröße für Dateien 16 GB; praktisch 2 GB



Folie 84

Rechnet man nun alles richtig zusammen, so ergibt sich eine theoretische Maximalgröße für Dateien von 16 GB. Aufgrund verschiedenen anderer Beschränkungen kann eine Datei auf einem `ext2` System allerdings nur höchstens 2 GB groß sein; (das ist natürlich für Datenbankanwendungen etwas klein und man wird hier zu einem anderen Dateisystem greifen müssen).

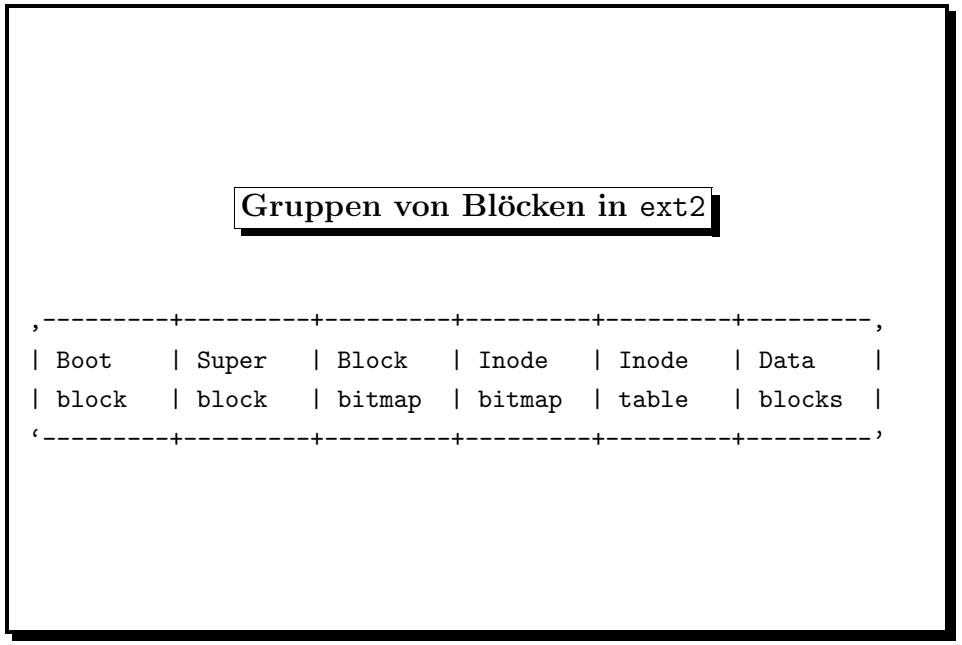
Neben den Inodes und Datenblöcken kennt das `ext2`-Layout noch weitere (Gruppen von Blöcken). Der wichtigste ist der *Superblock*. Er enthält wichtige Informationen über das Layout des Dateisystems, wie zB die Größe der Blöcke und der folgenden Gruppen, Informationen über den letzten Mount und Filesystemcheck, etc. Beim Mounten wird auf Informationen im Superblock zurückgegriffen; ist der Superblock korrumpiert, so kann das Dateisystem nichtmehr gemountet werden. Daher wird der Superblock repliziert und mehrere Kopien davon an verschiedenen Stellen im Dateisystem aufbewahrt (vgl. Folie 85).
Der *Bootblock* enthält eine Menge von Minimaldaten, die benutzt werden, falls von der entsprecheden Partition gebootet wird.
Schließlich werden die Nummern von freien Datenblöcken und freien Inodes in sog. Bitmaps gespeichert; diese *Block Bitmaps* und *Inode Bitmaps* stellen die 4. und 5. Gruppe von Blöcken im `ext2`-Dateisystem dar (vgl. Folie 86).

.

Superblocks, Inodes und Datenblöcke

- Superblock
  - 1. Block des FS, Kopien (8193, 16385)
  - Info über FS (letzter Mount, Blockgröße, Zeiger auf freie B/I)
- Inode
  - 256 Bytes (4/Block)
  - Benutzer, Gruppe, Berechtigungen, s/c/a/m-time
  - Zeiger auf Datenblöcke (max 12)
  - Zeiger auf indirekte Blöcke (3 Levels)
- Datenblöcke
  - eigentliche Daten der Dateien
  - Verzeichnisse (Inode-Tabellen)

Folie 85



Folie 86

Finetuning des Dateisystems
Man kann – allerdings nur beim Erstellen des Dateisystems – einige Finetuning vornehmen. Die *Inode-Dichte* gibt an, welche Dateigröße für ein Dateisystem erwartet wird. Die Anzahl der Inodes bestimmt, wie viele Dateien angelegt werden können. Ist die Zahl zu klein, kann es vorkommen, dass die Partition als voll gilt, obwohl durchaus noch Datenblöcke frei sind.
Wird zum Beispiel ein Wert von 4096 Bytes pro Inode (Standardwert) gewählt, bedeutet dies, dass im Schnitt alle Dateien 4 kB groß sein werden. Werden auf diesem Dateisystem ausschließlich Dateien mit einer Größe von nur einem Kilobyte angelegt, so kann man nur ein Viertel der Platte verwenden, da das Dateisystem dann als voll gilt.

Die Blockgröße ist die kleinste adressierbare Einheit in einem Dateisystem. D.h. jede Datei verbraucht ein Vielfaches dieser Blockgröße, unabhängig von ihrer eigentlichen Größe. Die Blockgröße beeinflusst die Dauer des Dateisystemchecks; sie steigt exponentiell mit der reziproken Blockgröße. Für Partitionen mit mehr als 4 GB wird oft eine Blockgröße von 4096 Bytes gewählt.

Nützliche Kommandos

- `fsck` überprüft das Dateisystem auf kleinere Fehler und kann diese beheben. Meistens wird fsck automatisch gestartet, zum Beispiel beim Booten von `/etc/rc.sysinit` nach einem Systemabsturz. Das funktioniert so: Im Superblock (Gruppe 2) wird beim Mounten des Dateisystems ein sogenanntes Valid Bit gelöscht, das nach einem sauberen Unmount wieder gesetzt wird. Fehlt dieses Bit beim nächsten Start des Systems, bedeutet dies, dass das System nicht ordnungsgemäß heruntergefahren wurde. Jetzt wird ein Programm gestartet, e2fsck, das die Daten auf Konsistenz überprüft und wenn nötig zu reparieren versucht. Dies ist nicht immer erfolgreich, Dateien (oder Datenblöcke), die nicht ordnungsgemäß wiederhergestellt werden konnten oder nicht richtig referenziert werden können, landen in einem extra dafür vorgesehenen `/lost+found` Verzeichnis der Partition.

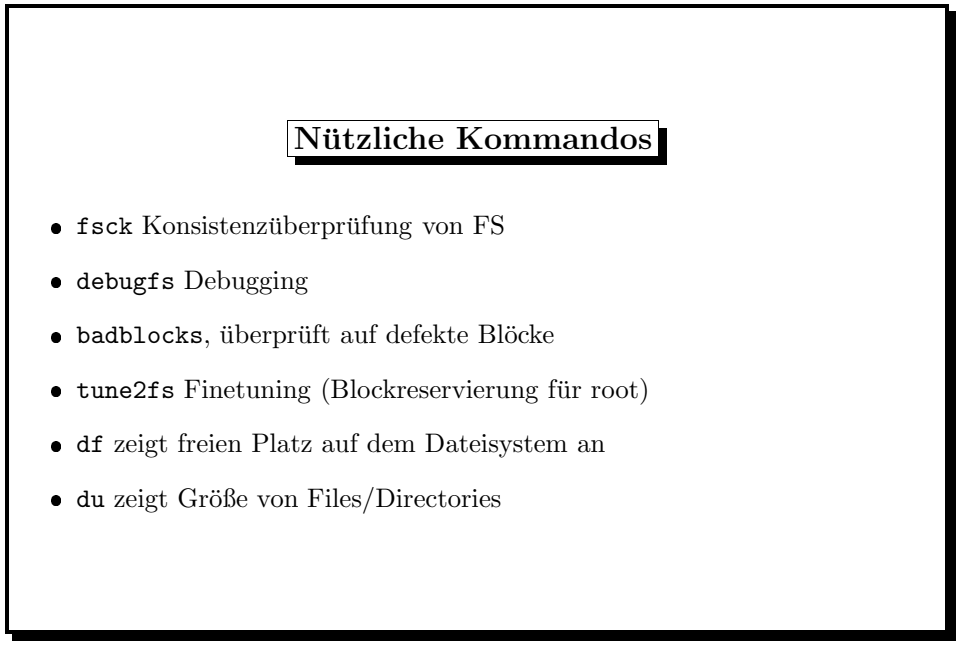
Da `fsck` über die gesamte Partition (oder Platte) laufen muss, kann diese Prozedur unter Umständen je nach Größe des Dateisystems einige Minuten kostbarer Uptime in Anspruch nehmen. Ist man auf eine effizientere (schnellere) Art der Dateiverwaltung angewiesen, sollte man eine andere Art der Dateiverwaltung in Betracht ziehen (Journaling, Abschnitt 8.4).

- `debugfs:` Dieses Programm setzt dort an, wo fsck aufgibt. Bevor man allerdings Zeit und Mühe investiert um verloren gegangene Daten vielleicht zu retten, wäre ein regelmäßiges Backup eine Überlegung wert.
- `tune2fs:` kann einige Parameter für fsck setzen:
  - Die maximale Anzahl der Mounts, nachdem eine gründliche Überprüfung erzwungen wird (meistens beim Booten)
  - Die maximale Zeit zwischen zwei Checks
  - Anzahl der Blocks, die für root reserviert sind. Dadurch kann man auch auf einer an sich vollen Platte noch Administrationsarbeiten durchführen, ohne dass man etwas löschen muss.
- `dumpe2fs:` zeigt Informationen über das Dateisystem, ausgehend vom Superblock, an.

Inode-Dichte, Blockgröße

- wichtigste Komponenten: Inodes und Datenblöcke
- FS voll, wenn
  - keine freien Datenblöcke, ODER
  - keine freien Inodes
- Finetuning des Filesystems (nach Bytes/File)
  - Blockgröße (1024, 2048, 4096)
  - Bytes/Inode (4096)

Folie 87



Folie 88

8.4 Journaling: `ext3` und ReiserFS

Wie werden Daten korrumpiert?
Stellen wir uns vor, wir editieren gerade eine Textdatei. Angenommen, das System stürzt ab, bevor wir eine Änderung abgespeichert haben, so ist diese verloren, aber die alte Version ist noch vorhanden; so haben wir zwar Daten verloren, aber das Malheur hält sich in Grenzen. Stürzt allerdings das System ab, gerade während die Datei geschrieben wird, ist der Schaden möglicherweise viel größer. Teile der neuen Datei sind schon überschrieben, Teile noch nicht und eventuell geht die gesamte Datei verloren.
Noch schlimmer ist es, wenn das System beim Schreiben von Verwaltungsinformationen, (der Metadaten) abstürzt, im Falle von `ext2` etwa der Inodes. Geschieht dies zB beim Verschieben eines Directories, so kann der ganze Verzeichnisbaum darunter verloren gehen. Daher bauen alle modernen Dateisysteme Redundanzen bei der Speicherung von Metadaten ein. Nach einem Systemcrash wird beim nächsten Booten das gesamte Filesystem einem Check unterzogen (zB `fsck`), wobei die Metadaten aus der redundanten Information rekonstruiert werden; trotzdem können unter Umständen gewisse Blöcke nicht mehr richtig referenziert werden. Dann gehen einzelne Dateien verloren und die respektiven Blöcke landen (unter `ext2`) in `lost+found/` im obersten Verzeichnis des Filesystems. Bei Dateisystemen mit einigen GB Größe kann dieser Vorgang mehr als 10 Minuten in Anspruch nehmen.

Journaling

- Herkömmliches FS
  - Metadaten redundant
  - Langer Dateisystemcheck nach Fehlern
- Journaling
  - Journal/Log für Metadatenänderungen/alle Schreibzugriffe
  - Dateisystemprüfung durch Auswerten des Journals
  - mehr Schreibzugriffe
- Journaling-Filesysteme
  - `ext3` (3rd extended FS; Nachfolger von `ext2`)
  - ReiserFS
  - JFS, XFS

Folie 89

Journaling
ist nun ein Verfahren, das die Filesystemchecks ersetzt. Es ist zwar im Betrieb manchmal langsamer als herkömmliche Dateisysteme, aber die Datenintegrität ist wesentlich verbessert und Filesystemchecks sind wesentlich verkürzt bzw. unnötig.
Im Gegensatz zu den unproblematischen Lesezugriffen werden Schreibzugriffe besonders behandelt. Bevor die eigentlichen Änderungen am Dateisystem vorgenommen werden, wird ein „Backup“ der zu überschreibenden Daten in eigens reservierten Bereichen, dem sog. *Journal* oder *Log*, gemacht. Erst dann werden die tatsächlichen Änderungen durchgeführt und nach Erfolg der eine Journal-Eintrag gelöscht. Stürzt der Rechner während einer solchen Prozedur ab, sind entweder noch die alten Daten vorhanden oder sie können aus dem Log rekonstruiert werden.

Dieser Zugang erfordert also keinen vollen Scan des Filesystems beim Checken und ermöglicht auch bei großen Partitionen Überprüfungszeiten im Sekundenbereich. Außerdem können die `lost+found`-Verzeichnisse entfallen. Der Nachteil des Journaling ist wegen der zusätzlichen Schreibarbeit eine eventuell geringere Geschwindigkeit. Die `fsck`-Programme könnten zwar theoretisch weggelassen werden; sie sind aber zur Sicherheit vorhanden um Hardwarefehler und etwaige Programmierfehler im Kernel zu mildern.
Prinzipiell wird für Metadaten Journaling gemacht, um immer ein konsistentes Dateisystem zu haben. Weiters unterscheidet man Journaling-FS wo auch ein Daten-Journal existiert.

ReiserFS
ist ein Filesystem, das Journaling nur für die Metadaten macht: Das bringt einen Geschwindigkeitsvorteil aber auch schlechtere Datenintegrität. Da es zur Verwaltung der Dateien datenbankähnliche Strukturen wie Hash-Werte und balancierte B^*-Bäume nutzt, kann auf kleine Dateien schnell zugegriffen werden. Bislang fehlt ein ausgereiftes `fsck.reiserfs`.

Das Dateisystem `ext3`
macht Journaling für Daten und Metadaten. Sehr nützlich ist die Abwärtskompatibilität zu `ext2`: Die Daten werden genauso wie unter `ext2` gespeichert, weshalb man sofort alle Werkzeuge wie zB `fsck.ext2` = `e2fsck` einsetzen kann und – falls notwen-

dig – eine ext3-Partition auch als ext2 mounten kann. Da ext3 durch das Journaling die Möglichkeit hat, die Bewegung der Festplattenköpfe zu optimieren, erzielt es einen höheren Durchsatz als ext2, was sich für große Dateien positiv auswirkt; für kleinere Dateien kommt es durch das Journaling selbst aber zu einer geringeren Geschwindigkeit.

Das Umsteigen von ext2 auf ext3 ist sehr einfach: Egal ob gemountet oder nicht lässt sich ein ext2-Dateisystem durch

```
tune2fs -j /dev/Gerät
```

umstellen. Ein neues ext3-Dateisystem lässt sich mit

```
mke2fs -j /dev/Gerät
```

einrichten; soll das Journal nicht mit dem Dateisystem sondern auf einem anderen Medium gespeichert werden, macht man das mit

```
mke2fs -O journal_dev /dev/myLog
mke2fs -J device=/dev/myLog /dev/myDisk  .
```

Allerdings muss bei mount stets -t ext3 bzw. in der fstab stets ext3 als Typ eingegeben werden. Um auf einem nicht gemounteten ext3-System nicht nur das Dateisystem zu überprüfen sondern auch das Journal durchzugehen, verwendet man

```
e2fsck -fy /dev/Gerät  .
```

Möchte man die Annehmlichkeit nutzen, dass fsck niemals (vor dem Mounten) aufgerufen werden muss, dreht man das mit

```
tune2fs -i 0 -c 0 /dev/hdxx
```

ab. Durch Optionen in fstab bzw. für mount kann beeinflusst werden, welcher Grad des Journaling verwendet werden soll. Die Voreinstellung ist data=ordered, womit Daten und Metadaten ins Journal kommen. Um dies mit data=writeback und data=journal teilweise auszuschalten, sehe man in der Online-Dokumentation nach.
Will man auch die Partition die auf / gemountet wird mit ext3 betreiben, so muss entweder der ext3-Treiber fix in den Kernel compiliert oder eine Initramdisk verwendet werden (siehe man mkinitrd).

9 Backup

In diesem kurzen Kapitel erklären wir warum das Backup von Daten wichtig ist, stellen grundlegende Backupstrategien und einfache Backupwerkzeuge vor.

Die Daten auf einem System sind oftmals wesentlich wertvoller und schwieriger (wieder-) zu beschaffen, als die Hardware. Eine der wichtigsten Aufgaben des Systemadministrators ist daher die Sicherung von (Benutzer)daten und Konfigurationsdateien, kurz auch *Backup* genannt. „Irren ist menschlich“, sagt man; daher kann es schon einmal passieren, dass ein Benutzer zB seine Diplomarbeit löscht. Andererseits ist ein Backup auch ein guter Schutz vor Datenverlust durch Hardwaredefekte (zB Ausfall einer Serverfestplatte), Softwarefehler oder Hackereinbrüche. Weiters sind Backups auch hervorragend geeignet, Daten von einem System auf ein anderes zu migrieren. Schließlich dienen Backups zum Archivieren von Daten über längere Zeiträume hinweg; zB Wirtschaftsbetriebe, Versicherungen, Banken, etc. müssen ihre Buchhaltungen einige Jahre lang aufbewahren.

9.1 Backupstrategien

Bei der Planung von Backups sind einige grundlegende Dinge zu bedenken und Entscheidungen zu treffen, die voneinander nicht unabhängig sind und die von der Art und dem Einsatzbereich des Systems bestimmt werden (*Backupstrategie*):

- Zu allererst muss man sorgfältig die *Frequenz und Art* des Backups für die verschiedenen Daten und Datenbereiche des Systems überlegen. Hierbei unterscheidet man zweckmäßigerweise zwischen den *Benutzerdaten* und den *Systemdaten*, wie etwa Konfigurationsdateien, wichtigen Scripts etc. Die Benutzerdaten werden in der Regel häufiger zu sichern sein als die Systemdaten; zB die Benutzerdaten täglich, die Systemdaten zB nur vor und nach Eingriffen in das System, mindestens aber monatlich.

Warum Backup?

- Daten teurer/schwerer (wieder) zu beschaffen als Hardware
- Disasterrecovery
  - Hard-/Softwareschaden
  - Schaden aufgrund von Installation/Upgrade
  - unabsichtliches Löschen
  - böse Benutzer, Hacker
- Langzeitarchiv
- Systemadministration
  - Datentransfer zwischen Systemen
  - Reorganisation des Filesystems
  - Checkpoint vor und nach Upgrade

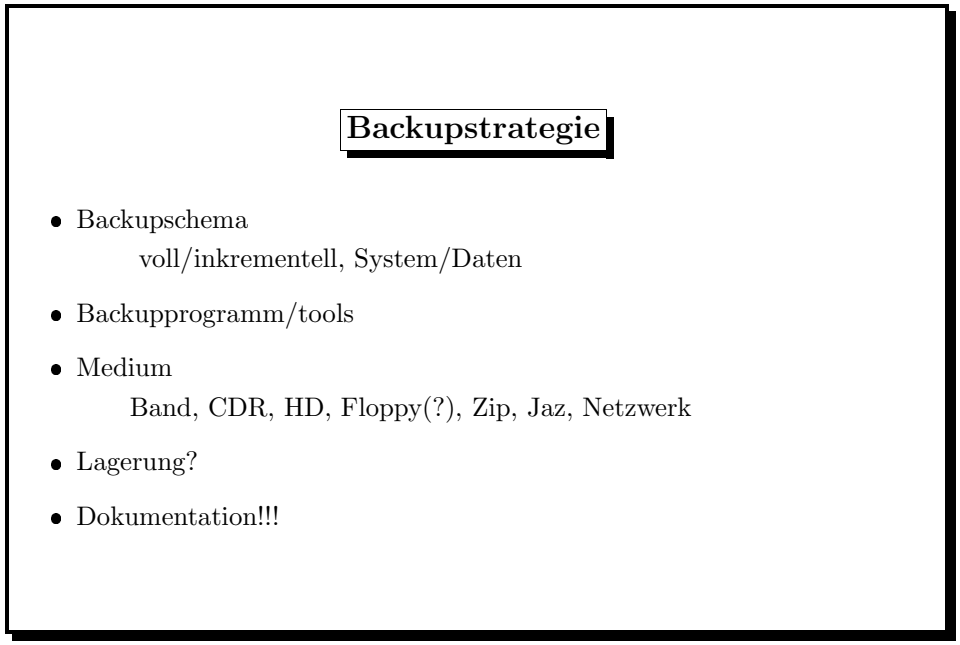
Folie 90

Weiters gibt es verschiedene Arten des Backups: Bei *vollen Backups* wird der gesamte Datenbestand gesichert, bei *inkrementellen Backups* nur die Änderungen seit der letzten Sicherung; dazu muss natürlich eine entsprechende Software verwendet werden. Vorteil des inkrementellen Backups ist der geringere Zeitaufwand beim Sichern, das Zurückspielen der Daten wird aber prinzipiell komplizierter und daher langsamer.

- Als nächstes sollte man sich für *Backupmedien bzw. die Hardware* entscheiden. Prinzipiell stehen hier viele Möglichkeiten offen. Bandlaufwerke sind aufgrund ihrer hohen Speicherkapazität weit verbreitet. Backups auf (Wechsel-) Festplatten sind sehr schnell und effizient aber teuer. Zip- und Jaz-Drives haben unter Umständen den Nachteil, dass sie nicht wirklich „Standard“ sind. Schließlich kann man auch Backups auf CD machen, was sich positiv auf die Transportierbarkeit auswirkt; im Gegensatz zu Bandlaufwerken verfügt fast jeder PC über ein CD-Laufwerk. Backups auf Disketten sind aufgrund der geringen Speicherkapazität nur für sehr kleine Datenmengen bzw. einzelne Dateien möglich. In großen Installationen gibt es Möglichkeiten Backups über das Netzwerk zu machen, was meist eine spezielle (kommerzielle) Software erfordert.

- Schließlich muss man natürlich ein geeignetes *Backupprogramm* finden. Meistens ist ein einfaches `tar` nicht ausreichend sondern man muss zu fortgeschritteneren und intelligenteren (möglicherweise) kommerziellen Anwendungen greifen, was fast immer auch mit größerer Benutzerfreundlichkeit einhergeht. Um die Belastung des Administrators gering zu halten, ist es zB wünschenswert, dass die Benutzer die Wiederherstellung ihrer (und zwar nur ihrer) Daten selbst vornehmen können.

- In kritischen Umgebungen darf man Backups nicht am Aufstellungsort des Rechners lagern. Im Falle eines Feuers, Wasserschadens oder anderer „mittlerer Katastrophen“ sollten wenigstens die Backupmedien „überleben“.



Folie 91

Hat man sich nun einen Backupplan zurechtgelegt, ist auf sorgfältigste Dokumentation desselben zu achten, um auch anderen (eventuell Administratoren) während eigener Abwesenheit (Urlaub, Wochenende, ...) die Möglichkeit zu geben, in Krisenfällen sofort und richtig zu reagieren.
Schließlich ist ein wichtiger aber oft unterschätzter Punkt das Erproben und Testen des Restorevorgangs (Zurückspielen der Daten vom Backup auf das System), sowie die geordnete Lagerung (inkl. Dokumentation) der Backupmedien. Schließlich sollten Backupmedien auch regelmäßig erneuert (Bänder!), bzw. geprüft werden.

Ein Beispiel für eine ausgearbeitete Backupstrategie inklusive einiger weiterer Tipps ist auf den Folien 92 und 93 zu finden.

Ein Beispielbackupschema

- volles Gesamtbackup: jeden Monat
- Systemdaten: volles Backup
  - vor und
  - nach Systemumstellungen
- Userdaten:
  - volles Backup jedes Wochenende
  - inkrementell jede Nacht

Folie 92

Wichtige Tipps

- nicht nur Sysadmin soll Backup machen können, DOKUMENTATION
- immer mit dem schlimmsten Fall rechnen
- Hardcopies aller verwendeten Scripts aufheben
- Installationsmedien und Backuptools mit Backup aufheben
- Backupmedien beschriften
- regelmäßig neue Medien benutzen
- Recovery testen !!!
- alte Backups regelmäßig prüfen

Folie 93

9.2 Werkzeuge

An einfachen Unix-Werkzeugen zum Backup stehen `tar`, `cpio` und `dump` zur Verfügung, jedes mit seinen spezifischen Vor- und Nachteilen.

Das Kommando `tar` (vgl. auch Teil 1, Abschnitt 6.4) dient nicht nur zum Backup sondern auch dem einfachen Archivieren und Transportieren größerer Datenmengen und von ganzen Verzeichnisbäumen.
Allerdings ist es schwierig, mit `tar` komplette Festplattenpartitionen sichern, was mit `dump` dagegen einfach ist. `cpio` wiederum hat Probleme mit symbolischen Links. Außerdem unterstützt `dump` im Gegensatz zu den beiden anderen Tools inkrementelle Backups. Die Syntax der Befehle und einige Beispiele dazu können entweder den jeweiligen Manpages bzw. den folgenden Folien entnommen werden.
Dort findet man auch Hinweise auf einige kommerzielle Produkte, die, wie bereits erwähnt, meistens wesentlich leistungsfähiger und dabei einfacher zu verwenden sind. Für welches Werkzeug man sich im Endeffekt entscheidet, hängt wesentlich von der benötigten Sicherheit und einer Abwägung der Kosten und Nutzen ab.

Linux-Backuptools

- `tar`
  - Backup individueller Files
  - weit verbreitet (Unix-Standard)
  - Datentransfer zwischen Plattformen
- `cpio`
  - Backup individueller Files
  - weit verbreitet
  - Probleme mit Symlinks
- `dump`
  - Backup ganzer Filesysteme
  - inkrementelle Backups

Folie 94

tar

- traditionelles UNIX Tape-Archiv Kommando
- Basis-Syntax
  - backup: `tar cvf tarfile.tar directory_or_file_to_tar`
  - restore: `tar xvf tarfile.tar`
  - listen: `tar tvf tarfile.tar`
  - zusätzlich komprimieren: `tar xvzf tarfile.tar`
  - komprimieren mit `bzip2`: `tar xvjf tarfile.tar`
  - Multivolume: `tar cvMf /dev/fd0 files_to_tar`
    keine Komprimierung, alternativ: `split`

Folie 95

cpio

- Unix-Standard
- backup: `cpio -ov files > device`
  `find /home | cpio -ov > /dev/fd0`
- restore: `cpio -iv[-dum] [files] < device`
  `cpio -ivdum "/home/j*≪ /dev/fd0`
- listen: `cpio -itv < device`

Folie 96

dump

- Backup kompletter Filesysteme
- auch Symlinks und spezielle Files (`/dev`)
- inkrementelles Backup bis zu 9 Stufen
- backup: `dump -0 -a -u -f /dev/fd0 /home`
- inkrementell: `dump -5 -a -u -f /dev/fd0 /home`
- restore: `cd /home; restore -r -f /dev/fd0`

Folie 97

Weitere Tools und Tipps

- Taper: menügesteuertes Band-Backup
- BRU2000: `http://www.bru.com`
- Lone-Tar: `http://www.cactus.com`
- ADSL/TSL: Netzwerkbackup, IBM
- `http://www.linux-backup.net`
- Linux Backup HOWTO
  `http://www.biochemistry.unimelb.edu.au/pscotney/backup/Backup-HOWTO.html`

Folie 98

10 Kernel compilieren

Hier erklären wir warum es manchmal sinnvoll ist, selbst einen Kernel zu compilieren. Wir gehen auf die Verwendung von Kernel-Modulen ein und erklären kurz die wichtigsten Schritte beim Konfigurieren und Compilieren eines Linux-Kernels.

Der Linux-Kernel ist nichts anderes als ein ca. 1 MB großer Code, der vom Bootmanager (zB `lilo`, `grub`) in den Speicher geladen und ausgeführt wird und die Grundfunktionen des Betriebssystems implementiert (vgl. auch Teil 1, Kapitel 2).
Nach wie vor koordiniert *Linus Torvalds* das riesige Projekt der Weiterentwicklung des Linux-Kernels: Neben Bugfixes für die aktuelle Version wird gleichzeitig auch an sog. Entwicklerkernels getüftelt, in denen neue Konzepte entwickelt und getestet werden und die daher nicht (so) stabil sind.

Da ein Kernel einen möglichst großen Leistungsumfang bieten und sich schnell an neue Hardware und an neue Problemstellungen anpassen lassen soll, kann man ihn nicht monolithisch (als einen großen Programmklotz) programmieren, sondern muss die verschiedenen Aufgaben klar in weitgehend unabhängige Teile trennen. Durch diese *Modularisierung* des Quellcodes können viele Leute gleichzeitig an der Kernelentwicklung mitarbeiten. zB ist ein Festplattentreiber (zB IDE oder SCSI) völlig unabhängig von einem Dateisystemtreiber (zB `ext3` oder ReiserFS), solange ein vereinbartes Programmierinterface benutzt wird; daher kann man schnell und einfach zB Treiber für neue Dateisystemformate programmieren, ohne Änderungen in anderen Quellcodeteilen vornehmen zu müssen. Werden gewisse Treiber, Protokolle, etc. überhaupt nicht benötigt oder sollen sie nicht benutzt werden (Performance- und Sicherheitsaspekt), lässt man sie entweder beim Compilieren des Kernels weg oder lädt und entlädt die entsprechenden *Module* bei Bedarf (im laufenden Betrieb): dies lässt sich auch automatisieren; der Kernel lädt zB die Module für die Floppyhardware und das DOS-Dateisystem erst, wenn eine DOS-Diskette gemountet wird, und entlädt sie selbständig kurz nach dem Unmounten (Details in Abschnitt 10.1).

Ein weiterer Vorteil der Modularisierung ist, dass sich Linux relativ rasch auf andere Hardware-Architekturen übertragen lässt: Die wenigen Prozeduren, die stark von CPU, Motherboard, Bus-System, etc. abhängen, sind in der Assemblersprache des jeweiligen Systems maßgeschneidert programmiert, sind klein und übernehmen nur ganz elementare Aufgaben (in Protected Mode umschalten, Festplattensektor lesen, ...). Der andere Teil des Quellcodes ist hardwareunabhängig, in C geschrieben und implementiert die ganze Funktionalität des Kernels (Netzwerkprotokolle, Dateisysteme, ...) und schließlich die Funktionen, die die Anwendungsprogramme aufrufen dürfen (sog. System Calls; zB Lese/schreibe Datei, ...). Jener Teil kann also ohne wesentliche Änderungen auf ein neues System übernommen werden (Recycling), allerdings braucht man dazu zuerst einen C-Compiler (den man aber ohnehin benötigt, um Anwendungsprogramme zu compilieren).

Die *Nachteile* dieses Konzepts der Linux-Kernelprogrammierung liegen auf der Hand: Eine perfekt funktionierende C-Compilermaschinerie, die optimierten Code für eine neue Hardware-Architektur erzeugen soll, ist ein aufwändigeres Projekt als der Kernel selbst.
Bei der Programmierung des Kernels muss man sich strengstens an gewisse Konzeptionen und Spielregeln halten, da sonst seine Stabilität leidet und der Quellcode (noch) unübersichtlicher. Schließlich bringt die Vielfalt der Konfigurationsmöglichkeiten des Kernels und der Treiber einen „Overhead“ in Form eines nicht unwesentlichen Verwaltungsaufwands einerseits *im* Quellcode andererseits des Quellcodes *selbst* mit sich.

Kernel-Versionsnummern

`uname -r` und `dmesg | head -1` zeigen die Versionsnummer des laufenden Kernels an. `2.4.9-12` bedeutet zB, dass wir mit der *Version* 2, *Patchlevel* `4` und *Sublevel* `9` arbeiten. Die gerade Patchlevel-Nummer (`4`) zeigt an, dass dies ein stabiler Kernel (auch: *Produktionskernel*) ist; eine ungerade steht für Entwicklerkernel, die instabil sind. Manche Distributoren ändern einen Kernel leicht ab und hängen eine Zahl oder Zeichenkette an, (hier die RedHat-Releasenummer `12`). Innerhalb der stabilen Versionen wird nur dann ein neuer Kernel veröffentlicht und das Sublevel weitergezählt, wenn Fehler im Code ausgebessert („Patches“ herausgegeben) werden (beachte die nicht ganz schlüssige Benennung des Patchlevels).

Grundsätzlich Neues (wie Restrukturierung des Kernelaufbaus; Hardwareunterstützung, Protokolle, ...) wird in Entwicklerkernels ausprobiert und getestet und erst beim nächsten Versionssprung „freigegeben“, d.h. in einem Kernel mit geradem Patchlevel veröffentlicht.

Heutiger Stand (2002-03-13) ist die Version `2.4`, die aus der Entwicklerversion `2.3` entstanden ist. Das aktuelle Sublevel ist `18` und somit hat der neueste Produktionskernel die Versionsnummer `2.4.18`; der neueste RedHat-7.2-Kernel hat die Versionsnummer `2.4.9-31`.

Derzeit läuft dazu parallel die Entwicklung der Version 2.5, aus der später die stabile Version 2.6 werden soll. Der neueste Entwicklerkernel ist `2.5.7`.

Kernel-Versionen

```
[oli@sqirrel ~] uname -r 2.4.10-4GB
[oli@sqirrel ~] dmesg | head -1
  Linux version 2.4.10-4GB (gcc version 2.95.3)
  #1 Tue Sep 25 12:33:54 GMT 2001
```

- Version: 2
- Patchlevel: 4; (un)gerade bedeutet (in)stabil
- Sublevel: 10; (Bugfixes innerhalb 2.4)
- Release: SuSE-Kernel mit Unterstützung für 4 GB RAM

Folie 99

10.1 Kernel-Module

Der Linux-Kernel bietet die Möglichkeit, viele Treiber als sogenannte Module zu verwenden. Diese Treiber sind dann nicht fix in den Kernel hineincompiliert, sondern können im laufenden Betrieb geladen werden. Prominente Beispiele hierfür sind Netzwerkkartentreiber und Soundkartentreiber (vgl. auch oben). Die Module befinden sich in `/lib/modules/kernel-versionsnr/` und enden auf `.o` (Objektdatei, i.e., eine Sammlung compilierter C-Funktionen).
Die Vorteile beim Verwenden von Modulen sind, dass der Kernel weniger Speicher benötigt und schneller bootet. Der Nachteil dabei ist allerdings, dass das Laden der Module selbst eine gewisse Zeit in Anspruch nimmt. Außerdem sollten Treiber nicht als Module verwendet werden, die beim Booten benötigt werden. Es gibt zwar die Möglichkeit, sogenannte *Initial Ramdisks* (Initramdisks) zu verwenden und etwa den SCSI-Treiber modular zu verwenden, obwohl man von einer SCSI-Platte bootet. Wir gehen hier darauf aber nicht ein; siehe zB `http://sdb.suse.de/en/sdb/html/initrd.html` und `man mkinitrd`.
Die Module eines Kernels können nicht mit einem anderen Kernel verwendet werden, selbst bei gleicher Versionsnummer und selbem Quellcode. Wenn man einen Kernel installiert/compiliert, der die gleiche Versionsnummer wie der laufende hat, muss man selbst ein Backup der Module machen und selbst dafür sorgen (zB Symlink auf Backup), dass der Kernel die richtigen Module lädt.

Im Folgenden stellen wir die Werkzeuge vor, mit denen Module gehandelt werden; im Wesentlichen sind das die die Programme `lsmod`, `modprobe`, `insmod`, `rmmod`, `depmod` in `/sbin/` und die Datei `/etc/modules.conf` (siehe auch Folie 101).
Mit `lsmod` kann man die gerade in Verwendung befindlichen Module auflisten. `depmod` bestimmt die Modulabhängigkeiten und schreibt diese in die Datei `/lib/modules/kernel-versionsnr/modules.dep`. Üblicherweise wird dieser Befehl nach dem Booten von `/etc/rc.sysinit` ausgeführt.

Kernel-Module

- Teile (Treiber) des Kernels als Module
- können im laufenden Betrieb geladen werden
- Vorteile: kleinerer Kernel, schnelleres Booten
- Nachteil: Laden braucht Zeit
- Nur für Hardware, die nicht beim Booten benötigt wird

Folie 100

Umgehen mit Modulen

- Listen: `lsmod`
- Laden: `insmod` (einfach), `modprobe` (clever)
- Entfernen: `rmmod` (nur wenn unbenutzt)
- Weiters: `depmod`, `modinfo`
- Automatisch: `/etc/modules.conf`

Folie 101

Um Module in den Kernel zu laden hat man zwei Alternativen: `insmod` ist einfach und brutal, `modprobe` intelligenter; es prüft Modulabhängigkeiten und lädt vorher alle benötigten Module wobei die Information aus `/etc/modules.conf` bezogen wird. `insmod` reagiert in so einem Fall mit einer Fehlermeldung; man muss hier also wissen, in welcher Reihenfolge die Module zu laden sind. Beiden Befehlen kann man Parameter übergeben, z.B. IRQ oder IO-Port. Üblicherweise finden die Module die notwendigen Einstellungen allerdings durch Probieren (*Autoprobe*) selbst heraus; Hat man den Kernel-Quellcode unter `/usr/src/linux` installiert, findet man dort in `Documentation/` detaillierte Informationen zu Modulparametern. Eine störrische Sound-Blaster-Karte kann vielleicht mit

```
modprobe sb io=0x220 irq=5 dma=1 dma16=5
```

zum Arbeiten überredet werden; stimmen die Optionen nicht, kann sich das System aber auch aufhängen.
Module aus dem Kernel entfernen kann man nur, wenn sie nicht benutzt werden und zwar mit `rmmod`; ggf. muss man zuerst davon abhängige Module entfernen, Medien unmounten oder Programme schließen.

Wirklich bequem wird das Verwenden von Modulen durch die Automatisierung des Ladevorgangs (und des Entfernens). Dazu muss die Datei `/etc/modules.conf` (oder je nach Distribution auch `/etc/conf.modules`) angelegt werden, in der angegeben wird, welches Modul (eventuell mit welchen Parametern) für welches Hardwaregerät zu verwenden ist. Üblicherweise wird diese Datei bereits vom Installer richtig geschrieben, und braucht nur im Falle, dass man eine neue Hardwarekomponente einbaut verändert zu werden. Eine typische `/etc/modules.conf`-Datei befindet sich auf Folie 102.

/etc/modules.conf

```
alias eth0 rtl8139
alias eth1 3c59x

alias scsi_hostadapter aic7xxx
alias parport_lowlevel parport_pc

alias sound-slot-0 sb
options sb io=0x240 irq=7 dma=0

alias midi opl3
options opl3 io=0x388
```

Folie 102

10.2 Kernel compilieren – Warum?

Auf jedem funktionierenden Linux-System ist natürlich (mindestens) ein Kernel vorhanden. Warum sollte man dann einen neuen Kernel compilieren (außer aus Faszination an der Sache selbst)?
Nun, dafür gibt es mindestens drei gute Gründe: der verwendete Kernel hat entweder zu wenig oder zu viel Hardwareunterstützung, oder es muss auf einen neuen Kernel-Release upgegraded werden (und es steht noch kein neues, bzw. adäquates Kernel-Paket der entsprechenden Distribution zur Verfügung).
Der erste Grund tritt ein, wenn etwa am System ein Hardwaregerät vorhanden ist, das vom gegenwärtig verwendeten Kernel nicht oder nicht optimal unterstützt ist.
Andererseits haben die Standardkernel der einzelnen Distributionen viele Treiber fix eincompiliert, die man üblicherweise nicht benötigt. Dann kann durch Herstellen eines auf die spezifische Hardwarekonfiguration des Systems getrimmten Kernels die Performance verbessert werden. Insbesondere belegt ein kleinerer Kernel, der keine unnötigen Treiber beinhaltet, weniger Speicher und bootet schneller. Manchmal kann es auch wichtig sein, wegen verbesserter Features (neue Treiber, neu unterstützte Hardwarekomponenten) oder ausgebesserter Bugs (vor allem, wenn sicherheitsrelevant) auf einen neuen Kernel-Release upzugraden. Das kann auch – falls vorhanden – mittels `rpm`-Pakets geschehen, was einem das Compilieren erspart; Kernel RPMS sollten aber niemals mit den Upgradeoptionen `-U` oder `-F` installiert werden, da sonst der alte Kernel und seine Module überschrieben werden. Das kann dazu führen dass der laufende Kernel nicht mehr richtig funktioniert, weil er keine brauchbaren Module mehr findet. Außerdem wird der Bootloader nicht entsprechend upgedatet. Das muss man zwar auch dann händisch machen, wenn man `rpm -i` verwendet, allerdings bleibt der alte Kernel funktionstüchtig und kann auch später noch gebootet werden („beliebte”’ Fallgrube bei automatischen Updates). Für weitere Detials siehe zB `http://www.redhat.com/support/resources/howto/kernel-upgrade`.

Kernel compilieren – Warum?

- Standard-Kernel nicht adäquat, weil
  - vorhandene Hardware nicht unterstützt
  - zu viel nicht benötigte Hardwareunterstützung
    - Speicherverbrauch
    - Booten dauert länger
- Upgrade auf neuere Version
  - neue Hardwareunterstützung
  - neue Protokolle, Dateisysteme, ...
  - Bugs, Sicherheistlücken
- Rechner-Spezialeinsatz zB: Nur-Firewall; alter Rechner mit wenig RAM
- Experimentellen Kernel verwenden ?!? Spaß !?!

Folie 103

10.3 Kernel-Quellcode

Für den Fall, dass nur neue Hardwareunterstützung ins System integriert werden soll, können die Kernel-Quellcode Pakete der Distribution verwendet werden (z.B. `kernel-source-2.2.17-14.i386.rpm`). Achtung, diese dürfen weder mit den Kernel RPMS selbst (z.B. `kernel-2.2.17-14.i586.rpm`), noch mit den Kernel SRPMS (z.B. `kernel-2.2.17-14.src.rpm`) verwechselt werden. Letztere enthalten die Quellen um das Kernel RPM und das Kernel-Source RPM (mittels `rpm`) neu zu bauen. Die Kernel-Quellcode Pakete sind allerdings meist nur für den Standardkernel und eventuell ein bis zwei Upgrades für den entsprechenden Release der Distribution verfügbar.

Will man eine dadurch nicht abgedeckte Kernel-Version verwenden, so muss man die Kernel-Source selber aus dem Internet herunterladen; diese findet man auf `http://www.kernel.org` resp. auf dem Mirror `http://www.kernel.at` oder auf der Originalsite `ftp://ftp.funet.fi/pub/Linux/PEOPLE/Linus`. Im Directory für jedes Patchlevel befindet sich jeweils eine Datei namens `LATEST-IS-x.y.z`, die auf die neueste Kernel-Version verweist. Man kann die gesamte Kernel-Source im `gz`- oder `bz2`-Format, wobei letzteres stärker komprimiert ist, herunterladen. Die Größe von z.B. `linux-2.4.3.tar.bz2` ist 19.9 MB. Um nicht den gesamten Quellcode herunterladen zu müssen, wenn man bereits einen älteren hat, kann man Patches verwenden; diese enthalten nur die Änderungen seit der letzten Version und können zB mittels des Kommandos `zcat patch-2.4.3.gz | patch -p0` eingespielt werden; dadurch wird der 2.4.2er Sourcetree in einen 2.4.3er verwandelt. `patch-2.4.3.bz2` hat z.B: nur 1 MB. Will man allerdings von einem 2.4.1er Kernel auf einen 2.4.3er upgraden, braucht man beide Patches, d.h. `patch-2.4.2.bz2` und `patch-2.4.3.bz2`.

Kernel-Quellen

- Kernel RPMS
  nur installieren, nicht compilieren
  z.B. `kernel-2.2.17-14.i686.rpm`
  NUR: `rpm -i`, NIEMALS: `-F|U`
- Kernel-Source RPMS
  installieren dann compilieren
  z.B. `kernel-source-2.2.17-14.i386.rpm`
- NICHT: Kernel SRPMS
  Quelle zum Neupaken der RPMS mit `rpm`
  z.b. `kernel-2.2.17-14.src.rpm`
- Kernel-Quellcode Tarballs
  als `tar.gz` oder `tar.bz`
  - `http://www.kernel.org`
  - `http://www.kernel.at`
  - `ftp://ftp.kernel.at`
  - `ftp://ftp.funet.fi/pub/Linux/PEOPLE/Linus`

Folie 104

Schließlich kann man noch mittels der ebenfalls im Download Directory befindlichen Signatur (z.B. `linux-2.4.2.tar.bz2.sign`) die Authentizität des Codes prüfen. Dazu muss man von `http://www.kernel.org/signature.html` den Kernel PGP Public Key herunterladen und mittels `gpg --import` in den Keyring aufnehmen. Sodann verifiziert man das `tar.gz`-file etwa mit `gpg --verify linux-2.3.9.tar.gz.sign linux-2.3.9.tar.gz`.

Achtung jedes `tar.gz` oder `tar.bz2` Kernel-Quellcode File entpackt sich nach `/usr/src/linux`, sodass man aufpassen muss, einen eventuellen vorhandenen älteren Sourcetree nicht zu überschreiben. Man kann nach dem Entpacken den Sourcetree auf `/usr/src/linux-versionsnr` umbenennen; dann sollte man aber immer in `/usr/src/` einen Link `linux` anlegen, der auf das aktuellen Quellcodeverzeichnis zeigt.

10.4 Kernel compilieren – Eine Kurzanleitung

Die folgende Anleitung ist als Kochrezept zu verstehen, wo man die eine oder andere Zutat hinzugeben oder weglassen muss, da sich von Version zu Version Dinge ändern können. Folgende Pakete müssen installiert (und upgedatet) sein um den Kernel erfolgreich compilieren zu können; meist sind diese bei der Systeminstallation in der Gruppe Development und/oder Kernel-Development zu finden.

- Gnu Compiler Collection (`gcc`)
- `binutils`, `modutils`, `make`

Führt man die Konfiguration unter der Konsole durch:

- `ncurses`, `ncurses-devel`[opement]

Für X-Window-Konfiguration:

- `Tcl/Tk`

Viele der folgenden Schritte (Ausnahme: Konfiguration und Compilierung) brauchen `root`-Rechte. Wenn man nicht paranoid ist, führt man der Einfachheit halber alles als `root` aus.
Bevor es richtig losgeht, macht man Backups von `/lib/modules/` und ggf. `/usr/src/linux/`; weiters informiert man sich möglichst genau über die Hardware des Computers. Anhaltspunkte sind `/proc/cpuinfo`, `/proc` allgemein, das BIOS-Menü, etc.

Sodann wechselt man ins Kernel-Sourcedirectory `/usr/src/linux/` und führt der Reihe nach folgende Schritte durch.

1. Die *Kernelkonfiguration* erfolgt über einen der drei Befehle `make config` (Frage Antwort-Spiel), `make menuconfig` (menügesteuert) oder `make xconfig` (GUI). Der längeren Beschreibung der Kernel-Optionen und -auswahlmöglichkeiten ist der ganze Abschnitt 10.5 gewidmet. Hat man die Konfiguration abgeschlossen, sichert man sicherheitshalber die Konfigurationsdatei `.config` per Menü oder per `cp` zB nach `/root/kernel.config`

2. Zum *Compilieren des Kernels und der Module* müssen der Reihe nach folgende Befehle ausgeführt werden: `make dep, (make clean), make bzImage, make modules, make modules_install`. Dadurch wird der Kernel compiliert, die neuen Module compiliert und installiert. Das neue Kernel Image liegt dann in `usr/src/linux/arch/i386/boot/bzImage`. Mittels

   ```
   $ make clean dep bzImage modules modules_install \
     2>&1 | tee mylogfile
   ```

   erfolgt alles in einem Aufwaschen und wrnungen und fehlermeldungen werden in `mylogfile` gespeichert. Der gesamte Compiliervorgang kann je nach Hardware und Konfiguration einige Minuten oder (mehr als) eine Stunde dauern.

3. Um den Kernel zu *installieren* muss er nach `/boot/` kopiert werden; zB mit

   ```
   $ cp /usr/src/linux/arch/i386/boot/bzImage \
        /boot/meinvmlinuz
   ```

   und der Bootloader `lilo` für das neue Image eingerichtet werden; als Vorlage kann man die bestehende Konfiguration nehmen, wobei man unbedingt die alte Konfiguration beibehalten und die neue (als alternatives Image) hinzufügen sollte – für den Fall, dass der neue Kernel nicht richtig funktioniert kann man so immer noch den alten verwenden, um einen weiteren Compilierversuch durchzuführen. Um den Bootsektor neu einzurichten, ruft man schließlich `lilo` auf.

   Folgender Schritt ist noch empfehlenswert, um harmlose Fehlermeldungen des neuen Kernels zu eliminieren, aber nicht unbedingt notwendig:

   ```
   $ cp /usr/src/linux/System.map \
        /boot/meineSystem.map
   $ mv /boot/System.map /boot/System.map.old
   $ ln -s /boot/meineSystem.map System.map
   ```

4. Rebooten und die Bootmessages sehr genau beobachten (und die Daumen drücken).

Troubleshooting: Treten beim Compilieren Probleme auf, sollte man seine Konfiguration auf Widersprüchlichkeiten überprüfen; manchmal ist es auch sinnvoll zu testen, ob sich die benutzte Version des `gcc` bzw. die der `binutils` mit der Kernel-Version verträgt (siehe Internet).

Die Fehlersuche, wenn sich der neue Kernel anders verhält als erwartet, beginnt mit einer Inspektion der `/var/log/messages`. Hier sollte man vergleichen, welche Meldungen der vorher installierte Kernel ausgegeben hat. Die Dateien und Unterverzeichnisse von `/proc/` geben sehr detailliert Auskunft darüber, welche Teile des Kernels funktionieren. Auf Informationen über Bugfixes, etc. sei wegen der Aktualität generell auf das Internet verwiesen.

Kernel compilieren

```
cd /usr/src/linux

make xconfig
   (auch: make menuconfig, make config)
make dep
(make clean)
make bzImage
   (auch: make zImage)
make modules
make modules_install

vi /etc/lilo.conf
lilo
reboot
```

Folie 105

10.5 Kernel-Konfiguration – Einige Details

Da sich die Optionen bei der Kernelkonfiguration ständig ändern, ist eine vollständige Aufzählung aller Konfigurationsmöglichkeiten hier nicht sinnvoll. Für Detailfragen sei auf `/usr/src/linux/Documentation/`, die Online-Dokumentation während der Kernelkonfiguration und das Kernel-HOWTO verwiesen.
Generell steht „y/∗“ für „fix in den Kernel einbinden“, „m“ für „als Modul“, „n“ für „Unterstützung weglassen“. Zu beachten ist, dass sich einige Punkte erst dann „aufklappen“, wenn man frühere Fragen mit „y“ oder „m“ beantwortet hat.

Auf folgende Fragen sollte man **yes** sagen, wenn man kein sehr außergewöhnliches System hat und wenn man (noch) nicht so genau weiß, was man tut.
Code maturity level options: *Enable loadable module support*, *Kernel module loader*; **nein** bei *Prompt for development and/or incomplete code/drivers*;
Für **Processor type and features** befragt man das BIOS oder `/proc/cpuinfo`. Nur Besitzer von Multiprozessor-Systemen nehmen *Symmetric multi-processing support*.
Bei **General Setup** muss man sich Zeit nehmen und genau durchlesen. *Networking Support*, *PCI support*, *System V lpc*, *BSD Process Accounting*, Sysctl support, *Kernel support for Elf binaries*. Notebook-Besitzer wählen üblicherweise PCMCIA-Unterstützung.
Parallel port support: *PC-style hardware*.
Plug and Play support: *ISA Plug and Play support* (zumindest schon wegen einer Soundkarte).
Block devices: *Normal PC floppy disk support*, *Loopback device support*.
Networking options: Vorsicht: Auch auf Rechnern ohne Netzwerkkarte verwenden X Window und andere Programme intern TCP/IP!!! Unbedingt: *Packet socket*, *Network Packet Filtering*, *Unix domain sockets*, *TCP/IP networking*, *Advanced Router*, *Verbose route monitoring*, *TCP/IP syncookie support*, *Ip Multicasting*;
bei *Netfilter Configuration* (Firewalling) unbedingt: *Connection tracking*, Unterstützung für *FTP protocol*, *Iptables*, *MAC address match*, *Connection state match*, *Owner match*, *Packet*

filtering, *Reject target*, *Full Nat*, Masquerade target, Redirect target, *Log target* und weitere Optionen bei Bedarf. Unbedingt Fast Switching abschalten. Vorsicht: Auch auf Rechnern ohne Netzwerkkarte verwenden X Window und andere Programme intern TCP/IP!
Auf **Ata/Ide/Mfm/Rll support** dürfen bloß die Nur-SCSI-Besitzer verzichten. IDE-Besitzer aktivieren hingegen den Support/die Option für *Enhanced IDE/MFM/RLL disk/...*, IDE/ATA-2 Disk, IDE/ATAPI CDROM, *Generic PCI IDE chipset*, *Sharing PCI IDE interrupts*, *Generic PCI bus-master DMA*, *Use PCI DMA by default*.
Ggf. **Scsi**-Unterstützung. Achtung: Wer einen IDE-Brenner hat, muss hier „y“ sagen (siehe unten).
Ggf. **Network device support** für seine Netzwerkkarte. Für Modem-Verbindungen aktiviert man PPP.
In **Character Devices** zu *Virtual terminal*, *Support for console on virtual terminal*, *Unix98 PTY support* sowie ggf. *Parallel printer support*. Auch eine nicht-serielle Maus lässt sich hier konfigurieren. Der *Direct Rendering Manager* unter XFree86 $\geq$4.1 für eine gehobenere Grafikkarte lässt sich hier einstellen.
In **File systems** hat man unbedingt das Dateisystem der `/`-Partition fix einzubinden (und nicht als Modul); für DOS-Disketten, Win-Partitionen bzw. CDROMs sind VFAT bzw. *iso9660* auszuwählen.
Bei **Sound** nehmen Sound-Blaster-64-Besitzer *Creative Ensoniq AudioPCI 97*; weiters sollte man neben den Alsa-Treibern auch die (proprietären) OSS-Treiber enablen.
Bei **Usb** ist i.a. (nur) der UHCI-Treiber zu aktivieren; in Zukunft sind hier sicher Änderungen zu erwarten.

Hier erwähnen wir einige **speziellere Details**, die weniger oft relevant sind.

Kerneloptionen: Ähnlich wie man jedem Programm auf der Kommandozeile Optionen übergeben kann, kann man dies auch für den Kernel in Form eines Eintrags in `/etc/lilo.conf` per `append="`*Option*`"`. Diese „Kernelkommandozeile“ sieht man in `/proc/cmdline`. Da man diese Optionen üblicherweise nur benutzt, wenn spezielle Hardware beim Booten konfiguriert werden muss, sei dazu auf die Kernel-Dokumentation verwiesen.

CD-Brenner: SCSI-Brenner werden wie ganz normale SCSI-Geräte unterstützt. Da es bis jetzt noch keine echten Treiber für IDE-Brenner gibt, muss man dafür die SCSI-Emulation einschalten:
Man wähle *SCSI support*, *SCSI CDROM support*, *SCSI generic support* und füge in `/etc/lilo.conf` bei dem Boot-Eintrag für Linux hinzu: `append="`*`hdx`*`=scsi"`, wobei *`hdx`* für den IDE-Namen des Brenners steht, zB `hdc`. Sollte es dennoch Probleme geben, streicht man den *IDE CDROM support*. In `/etc/fstab` sollte man berücksichtigen, dass der Brenner jetzt mit `/dev/sr0` o.ä., angesprochen wird. `cdrecord -scanbus` zeigt, ob man erfolgreich war. Für weitere Details siehe das augezeichnete CD-Writing-HOWTO.

11 Shell Scripts (Bash)

In diesem Kapitel geben wir eine kleine Einführung in die (Bash) Shell Programmierung. Unterwegs wiederholen und erweitern wir viele Konzepte aus Teil 1, Kapitel 6.

11.1 Wozu Shell Scripts?

Shell Scripts bieten die Möglichkeit schnell und einfach Aufgaben unter Unix zu automatisieren; eine Shell kann als Programmierinterface verwendet werden. Jedoch unterscheiden sich Shell Scripts von Programmen in Sprachen wie C beträchtlich. Im Shell Script sind alle Systemprogramme direkt verwendbar. Es gibt nur einen Typ von Variablen; diese müssen nicht initialisiert werden, etc. Statt einer langen Liste weiterer Unterschiede sei hier nur Folgendes gesagt: Shell Scripts eignen sich besonders gut um Aufgabe „quick and dirty“ zu lösen. Ein Systemadministrator, der vor einer größeren Aufgabe steht – etwa der Erzeugung von 100 durchnummerierten Accounts – wird in der Regel versuchen, dies mit einem Script zu lösen. Wird die Aufgabe größer, so gehen die Überlegungen in Richtung Perl und letztlich zu einer Compilersprache. Shell Scripts sollte man nicht verwenden, wenn

- die Geschwindigkeit des Programms eine große Rolle spielt.
- komplizierte Aufgaben gelöst werden sollen, die ein stark strukturiertes Programmieren erfordern.
- Sicherheitsmechanismen verwendet werden sollen.
- viele Dateien gelesen und geschrieben werden sollen.
- man ein GUI haben will – GUI's are for wimps anyway.

Wozu Shell Scripts?

- Automatisierung von Aufgaben
- „quick and dirty“
- **nicht** wenn:
  - Geschwindigkeit wichtig
  - Sicherheitsmechanismen wichtig
  - hohe Komplexität
  - GUI
- Alternativen:
  - Perl
  - Compilersprachen

Folie 106

Was ist ein Shell Script?

Ein Shell Script ist eine Textdatei bestehend aus

- Programm- und Funktionsaufrufen
- Shell internen Kontrollstrukturen
- Variablenzuweisungen

Das Schreiben von Shell Scripts verlangt Wissen über

- shell-interne Kontrollstrukturen
- möglichst viele Unix Programme und
- deren Optionen

Folie 107

Verschiedene Shells

sh	Bourne shell, die erste Unix-Shell von S. R. Bourne
bash	Bourne Again Shell, Standard auf Linux, von der FSF
csh	Berkeley Unix C Shell, C-ähnliche Syntax, Standard auf BSD
tcsh	TENEX C Shell, erweiterte csh
ksh	Korn Shell, proprietäre Shell von David Korn
pdksh	Public Domain Korn Shell
rc	Shell für Plan 9-OS
es	Erweiterbare Shell auf Basis von rc
zsh	Z Shell von Paul Falstad
ash	kleine, POSIX konforme Shell, /bin/sh auf NetBSD
esh	Easy Shell, kleine, leicht bedienbare Shell
kiss	Karel´s Interactive Simple Shell
lsh	Shell mit DOS Kommandos für Umsteiger
osh	Operator´s Shell, mit erweiterten Sicherheitsmechanismen
sash	Standalone Shell, braucht keine Libraries
psh	Perl Shell, Perl Syntax

Folie 108

Die Shell unserer Wahl
Shells gibt es sehr viele. Die Aufstellung auf Folie 108 erhebt keinerlei Anspruch auf Vollständigkeit. Die Bourne Shell (*sh*), benannt nach ihrem Erfinder, ist die Mutter aller Shells auf UnixSystemen. Die Bourne Shell bot schon zu Anfang fast alle Möglichkeiten der Programmierung, die die *bash* heute bietet; die interaktive Bedienung war allerding nicht sehr bequem. Dieser Umstand führte zur Geburt der *csh*. *csh*-Scripts folgen einer anderen Syntax, die der Programmiersprache C ähnlich ist. Ein weiterer Meilenstein in der Geschichte der Shells war die Korn Shell *ksh*, ebenfalls nach ihrem Erfinder benannt. Diese war ein sehr erfolgreiches proprietäres Produkt. Die *bash* (Bourne Again Shell) ist der Versuch einer Zusammenmischung der Vorzüge verschiedener Shells, wobei die Programmierung in einer erweiterten *sh*-Syntax erfolgt.
Im weiteren werden wir unser Hauptaugenmerk auf die *bash* legen, die heute wohl die meistverwendete Shell unter Linux und vielleicht auch Unix ist. Die meisten unserer Konstruktionen werden allerdings ohne weiteres auch mit einer *sh* funktionieren.

Ein Shell Script schreiben
Ein Shell Script ist eine Textdatei, die Kommandos enthält. Welchen Texteditor man zur Erzeugung dieser Datei verwendet ist egal, aber... `http://www.thinkgeek.com/images/products/zoom/vi-emacs.jpg`.

Beginnt diese Textdatei mit der Zeichenfolge
`#!/bin/bash`
und wird die Datei ausführbar gemacht
`$ chmod 755 scriptname`
so kann das Script direkt mit seinem Namen aufgerufen werden.
`$ ./scriptname`
Das Script wird dann Zeile für Zeile, vom Interpretor, in unserem Fall der Bash, abgearbeitet. Im Unterschied dazu müssen Programme, die in Compilersprachen geschrieben sind, erst compiliert werden, bevor sie ausgeführt werden können.
Wie in allen Programmiersprachen ist das Kommentieren eines Scripts ein oft ignoriertes Merkmal guten Programmierstils. Zeilen die mit `#` beginnen gelten als Kommentare und werden ignoriert. Unser erstes Shellscript befindet sich auf Folie 110.

Die Login Shell

Nach dem Login landet man auf Unix-Systemen in einer Shell. Welche Shells auf einem System als mögliche Login Shell installiert sind steht in der Datei `/etc/shells`.

```
$ cat /etc/shells
```

Die Login Shell jedes Users steht in der Datei `/etc/passwd`.

```
$ grep $USER /etc/passwd | cut -d : -f 7
```

ändern kann man seine Login Shell mit dem Befehl `chsh` (aka change shell). Die Standard Login Shell auf Linux-Systemen ist die **bash**.

Folie 109

Hello World

Das obligate Hello World Programm ist als Shell Script denkbar einfach.
Folgender Text soll in der Datei `helloworld` gespeichert sein.

```
#!/bin/bash
echo "hello world"
```

Ist es ein Shell Script?

```
$ file helloworld
helloworld: Bourne-Again shell
  script text executable
```

Ausführbar machen mit
`$ chmod 755 helloworld`
und ausführen mit

```
$ ./helloworld
hello world
```

Folie 110

Kommentare & Interpreter

- Kommentare: Zeilen, die mit `#` beginnen werden beim Ausführen ignoriert.

  ```
  # Kommentare koennen helfen die
  # Lesbarkeit von Shell Scripts
  # wesentlich zu erhoehen.
  ```

- Interpreter: Angabe des Interpreters am Anfang des Scripts durch `#!`
  macht Scripts direkt ausführbar und gilt für beliebige Interpretersprachen.
  - `#!/bin/bash`
  - `#!/bin/csh`
  - `#!/bin/sh`
  - `#!/usr/bin/perl`

Folie 111

11.2 Variablen

Variablenname bestehen aus Buchstaben, dem Underscore (_) und Zahlen, wobei oft auf Kleinbuchstaben verzichtet wird. Die Zuweisung eines Wertes funktioniert folgendermaßen:
`$ VARIABLENNAME=wert`
Auf den Wert einer Variable greift man mit `$VARIABLENNAME` zu:
`$ echo $VARIABLENNAME`
`unset` nimmt einer Variable ihren Wert:
`$ unset VARIABLENNAME`
In Shell Scripts gibt es nur einen Variablentyp. Man unterscheidet also nicht wie in anderen Programmiersprachen Integer-, Gleitkomma- und Stringvariablen. Wenn ein Script davon abhängt, dass in einer Variable ein Integerwert steht, so ist der Autor dafür verantwortlich, dass dem auch so ist. Variablen müssen nicht initialisiert werden. Dies bereitet oft Probleme bei Tippfehlern. Folgendes Beispiel führt zu keiner Fehlermeldung:

```
$ TEST=Legasthenie
$ echo $TSET

$
```

Der Befehl `set` gibt eine Liste der von der Bash gesetzten Variablen. Neben anderen befindet sich darunter die Variable `PS1` die das Aussehen des Prompts bestimmt. MS-DOS Nostalgiker könnten sich über Folgendes freuen:

```
$ PS1="C:\> "
C:\>
```

In Scripts sind vor allem die Variablen `$1-$9` von großer Bedeutung. Diese enthalten die an das Script übergebenen Parameter (auch *Positionsparameter*). Dazu folgendes Beispiel, das in der ausführbaren Datei *parameters* gespeichert sein soll:

```
#!/bin/bash/


# Ausgabe des ersten Parameters
echo "Erster Parameter:  $1"
# Ausgabe des zweiten Parameters
echo "Zweiter Parameter: $2"
```


Und das kommt dabei heraus:

```
$ ./parameters foo bar
Erster Parameter:  foo
Zweiter Parameter: bar
```

Subshells, Variablen exportieren und einlesen
Ein grundsätzliches Konzept des Unix Prozessmanagments ist, dass jeder Prozess von einem Parentprozess abstammt. Dieser Text entsteht in einer Instanz des Editors `vim`. Ein Auszug aus der Ausgabe des Kommandos `pstree` soll dieses Konzept verdeutlichen:

```
$ pstree
init-+-arpwatch
   [...]
     |-xdm-+-XF86_SVGA
     |     `-xdm---fvwm2-+-FvwmCommandS
     |                   |-xterm---bash---vim
   [...]               [...]
```

Der Prozess *init* ist „Ahne“ aller Prozesse. Der Loginmanager *xdm* wartet auf Benutzerauthentifizierung und startet einen Windowmanager *fvwm2*, aus dem ein *xterm* gestartet wurde in dem eine *bash* läuft, aus der ein *vim* gestartet wurde.
Eine Subshell ist eine Shell, die aus einer anderen gestartet wurde. Ruft man ein Shell Script via

`$ ./script` oder
`$ bash script`

auf, so wird es in einer Subshell gestartet. Ruft man es via

`$ . script` oder
`$ source script`

auf, so werden die darin enthaltenen Befehle in der aktuellen Shell ausgeführt. Besonders beachten sollte man, dass die Verwendung von Pipelines auch innerhalb eines Shell Scripts zu Subshells führt. Ein Überblick über verschiedene Möglichkeiten ein Shellscript aufzurufen befindet sich auf Folie 112.

Die Unterscheidung ob Befehle in einer Subshell oder der aktuellen Shell asugeführt werden ist wichtig, weil Variablenzuweisungen auf eine `bash` Instanz beschränkt sind. Die Zuweisung kann in alle Subshells mit dem Befehl `export` exportiert werden. Folgende Kommandoabfolgen sollen das verdeutlichen, wobei man sich durch `pstree -h` einen Überblick über die aktuelle Situation machen kann.

```
$ # Test wird nicht exportieren
$ TEST=rose
$ echo $TEST
rose
$ bash
$ echo $TEST

$ TEST=eros
$ echo $TEST
eros
$ exit
exit
$ echo $TEST
rose
$ unset TEST
$ exit
$ # Test wird exportiert
$ TEST=rose
$ echo $TEST
rose
$ export TEST
$ bash
$ echo $TEST
rose
$ TEST=eros
$ echo $TEST
eros
$ exit
exit
$ echo $TEST
rose
$ unset TEST
$ exit
```


Setzt man also in der Shell eine Variable und startet dann ein Shell Script, so ist diese Variable – so sie nicht exportiert wurde – im Script nicht gesetzt.

Interaktiv kann man Variablem mit dem `read` Kommando definieren. Folgendes Beispielscript `what` liest interaktiv eine Variable ein und gibt sie dann wieder aus.

```
$ cat what
#!/bin/bash

# lese variable ein
echo "What do you want to do next?"
read todo

# ausgabe
echo "You said you will $todo"

$ ./what
What do you want to do next?
fall alseep
You said you will fall alseep
$
```

Shellscripts aufrufen

- Interpreteraufruf:
  - `bash helloworld`
    oder `sh helloworld`
  - in Subshell ausgeführt
  - nur r-Bit nötig
  - überschreibt Interpreterangabe im Script
- direkter Aufruf
  - `./helloworld`
  - in Subshell ausgeführt
  - r- und x-Bits nötig
  - Interpreterangabe im Script verwendet, wenn keine angegeben, dann in verwendeter Shell
- Sourcen
  - `. helloworld`
    oder `source helloworld`
  - in aktueller Shell ausgeführt
  - nur r-Bit nötig

Folie 112

Variablen

- Variablennamen bestehen aus Buchstaben, Underscore (_) und Ziffern.
- Zuweisung über

  ```
  $ VARIABLENNAME=wert
  ```
- Auf den Wert zugreifen mit `$`

  ```
  $ echo $VARIABLENNAME
  ```
- Unterschiedliche Variablenarten mit Beispielen
  - selbstdefinierte Variablen:
    `$FOO, $BAR, ...`
  - systemweite Variablen:
    `$HOSTNAME, $HOSTTYPE, ...`
  - built-in Variablen:
    `$HOME, $PS1, $PATH, ...`
- Variablen exportieren
  `$ export VARIABLENNAME`
- interaktiv einlesen:
  `$ read VARIABLENNAME`

Folie 113

Einige Built-in Variablen

- $$... PID
- $0... Name des Shellscripts
- $n... n.ter übergebener Parameter
- $#... Anzahl der Positionsparameter
- $* ... alle Positionsparameter
- $?... letzter Exit Code (siehe unten)
- $!... letzte Background PID

Folie 114

Subshells

Aus einer Shell kann man eine weitere Shell starten, welche dann als Subshell der ursprünglichen Shell bezeichnet wird.

```
$ bash
```

Die im Script enthaltenen Kommandos werden in

- einer Subshell ausgeführt, wenn das Script mit
  `$ ./script [&]` oder
  `$ bash script [&]`
- in der aktuellen Shell augeführt, wenn das Script mit
  `$ . script` oder
  `$ source script`

gestartet wird, wobei das optionale `&` das Script im Hintergrund startet.

Folie 115

11.3 Spezielle Zeichen und Quoting

Leerzeichen <space> und Tabulatoren <tab> werden als Trennzeichen verwendet. So werden im folgenden Beispiel das Kommando, die Optionen und die Parameter eines Befehls durch Leerzeichen getrennt:

```
$ ls -l foo bar
```

Manchmal ist es erwünscht, einem Zeichen mit spezieller Bedeutung (einem sogenannten *Shell-Metacharacter*) diese zu nehmen. So kann ein Dateiname auch ein Leerzeichen enthalten. Seit Microsofts Betriebssysteme über die 8.3 Namenskonvention hinausgekommen sind, tritt dieses Phänomen leider gehäuft auf. Als Beispiel nehmen wir eine Datei mit dem Namen *Mein Lied.mp3* an. Versucht man diese in der Shell zu löschen und schreibt:

```
$ rm Mein Lied.mp3
```

so versucht die Shell zwei Dateien mit Namen *Mein* beziehungsweise *Lied.mp3* zu löschen. Um der Shell mitzuteilen, dass das Leerzeichen in diesem Fall keine spezielle Bedeutung hat verwendet man eine der drei Quoting Methoden. Diese seien im Folgenden anhand unseres Beispiels angeführt:

```
$ rm Mein\ Lied.mp3
$ rm 'Mein Lied.mp3'
$ rm "Mein Lied.mp3"
```

Der Backslash \ (escape character) hebt dabei die spezielle Bedeutung des unmittelbar folgenden Zeichens auf. Auch wenn dieses Zeichen ein „newline“, also das Resultat des Betätigens der Return Taste, ist. Sowohl einfache '' (Single Quotes) als auch doppelte Anführungszeichen "" (Double Quotes) heben die spezielle Bedeutung der Zeichen dazwischen auf, wobei dies bei den einfachen Anführungszeichen für alle Zeichen gilt. Bei doppelten Anführungszeichen bleibt die spezielle Bedeutung der Zeichen $, ' und \ erhalten. Vergleiche die Ausgaben folgender Kommandos:


```
$ TEST=rose
$ echo "In \$TEST steht \"$TEST\""
In $TEST steht "rose"
$ echo 'In \$TEST steht \"$TEST\"'
In \$TEST steht \"$TEST\"
```

Im weiteren werden wir noch des öfteren auf spezielle Zeichen stoßen.

Befehle zu Gruppen zusammenfassen

Befehle werden durch einen Zeilenumbruch <newline> oder ein Semikolon ; getrennt. Im Folgenden zwei Schreibweisen, die das gleiche liefern:

```
$ cd /usr/bin
$ ls
```

bzw.

```
$ cd /usr/bin; ls
```

Es gibt zwei Möglichkeiten Kommandos zu Gruppieren. Runde Klammern () (Parantheses) beziehungsweise geschwungene Klammern {} (Curly Braces). Befehle, die in runden Klammern gruppiert sind, werden in einer Subshell ausgeführt, während in geschwungenen Klammern gruppierte Befehle in der aktuellen Shell ausgeführt werden. Dazu folgende Beispiele:

```
$ { FOO=bar; echo "\\$FOO ist $FOO"; }; echo "\\$FOO ist $FOO"
$FOO ist bar
$FOO ist bar
$ ( FOO=bar; echo "\\$FOO ist $FOO" ); echo "$\\FOO ist $FOO"
$FOO ist bar
$FOO ist
```

Die runden und die geschwungenen Klammern zählen zu den speziellen Zeichen. Diese müssen also, so sie in Dateiname auftreten, mit Quotes versehen werden.

Quoting

Quoting wird dazu benutzt, um bestimmten Zeichen ihre spezielle Bedeutung zu nehmen. Es gibt drei Möglichkeiten zu quoten.

`\`	escape character
`''`	single quotes
`""`	double quotes

Hat ein geistreicher Benutzer eine Datei unter „Mein Lied * Napster.mp3“ abgespeichert, so kann man diese mit einer der folgenden Zeilen löschen.

```
$ rm Mein\ Lied\ \*\ Napster.mp3
$ rm "Mein Lied * Napster.mp3"
```

Der escape character nimmt dem folgenden Zeichen seine spezielle Bedeutung. Alle Zeichen zwischen single quotes sind von ihrer speziellen Bedeutung befreit. Double quotes lassen den Zeichen `$`, `'` und `\` ihre spezielle Bedeutung. Double quotes sind also schwächer als single quotes.

Folie 116

Kommandos Gruppieren

; Trennt verschiedene Kommandos, die in der gleichen Zeile geschrieben werden. Die Kommandos werden hintereinander ausgeführt

() Ein oder mehrere Kommandos innerhalb runder Klammern werden in einer Subshell ausgeführt.

{} Ein oder mehrere Kommandos innerhalb geschwungener Klammern werden als Block in der aktuellen Shell ausgeführt.

Folie 117

Wildcards und Pattern Matching

Gehen wir im Folgenden davon aus, dass im aktuellen Verzeichnis folgende Dateien existieren:

```
$ ls
glut gut hut mut mutter
```

`*` steht für beliebige Zeichenketten; auch leere.

```
$ ls mut*
mut mutter
```

`?` steht für genau ein beliebiges Zeichen.

```
$ ls ?ut
gut hut mut
```

Alle in eckigen Klammern angegebenen Zeichen dürfen an dieser stelle alternativ vorkommen.

```
$ ls [gh]ut
gut hut
```

Ein `!` oder `^` verneint diese Auswahl.

```
$ ls [!gh]ut
mut
```

Alle in geschwungenen Klammern angegebenen Zeichenketten, die durch Beistriche getrennt sind dürfen vorkommen,

```
$ ls {gl,m}ut
glut mut
```

Diese Konstrukte sind auch kombinierbar.

```
$ ls {gl,m}ut*
glut mut mutter
```


Wildcards und Pattern Matching

Folgende Zeichen haben in der `bash` spezielle Bedeutung

`*`	beliebige Zeichenkette
`?`	genau ein beliebiges Zeichen
`[ ]`	genau eines der genannten Zeichen
`[^ ]`	genau ein nicht genanntes Zeichen
oder `[! ]`	
`{ , }`	genau eine der Zeichenketten

Folie 118

11.4 Exit Status

Jedes Kommando liefert nach seiner Beendigung seinem Parentprozess einen *Exit Status* zurück. Der Exit Status ist ein Integerwert zwischen 0 und 255. 0 bezeichnet den Erfolg des Kommandos, alle anderen Werte bezeichnen verschiedene Ausmaße des Scheiterns. Der Exit Status des letzten Kommandos wird in der Variable `$?` gespeichert.

```
$ grep root /etc/passwd
root:x:0:0:root:/root:/bin/bash
$ echo $?
0
$ grep Administrator /etc/passwd
$ echo $?
1
$ true
$ echo $?
0
$ false
$ echo $?
1
```

Die Programme `true` beziehungsweise `false` dienen einzig und allein dazu Exit Status 0 beziehungsweise 1 zu liefern. Das scheint auf den ersten Blick sinnlos, aber das tut auch `/dev/null`.
Um den Exit Status eines Shell Scripts zu beeinflussen gibt es den built-in Befehl `exit`. Dieser beendet ein Script sofort und setzt einen anzugebenden Wert als Exit Status des Scripts. Das folgende Script namens *parameterexists* liefert Exit Status 0, wenn mindestens ein Parameter übergeben wurde. Andernfalls liefert es Exit Status 1.

```
#!/bin/bash
if [ $1 ]; then
   exit 0
else
   exit 1
fi
```


Exit Status

Jedes Programm liefert nach Beendigung seinem Parent einen Exit Status zurück.

0 steht für eine erfolgreiche Beendigung des Programms

1-255 bezeichnet verschiedene Ausmaße des Scheiterns.

Der Exit Status eines Shell Scripts kann über den `bash` built-in Befehl `exit` gesteuert werden.

Der Exit Status des letzten ausgeführten Kommandos steht in der Variable `$?`.

Folie 119

Man sollte dabei unbedingt die Konvention beachten, dass 0 für einen Erfolg steht, während andere Zahlen als Misserfolg interpretiert werden.

11.5 Flow Control

Unter Flow Control versteht man *Kontrollstrukturen* wie bedingtes Ausführen von Kommandos und Schleifen. Im Wesentlichen sind dies `if`, `case`, `for` und `while`. Wir werden diese im Weiteren nacheinander abhandeln, und nebenbei allerlei Nützliches „mitnehmen“.

Bedingungen (`if`)
Zuerst wenden wir uns dem `if` zu, von dem wir schon ein Beispiel gesehen haben; die Syntax der `if`-Anweisung ist auf Folie 120 angegeben: Bei zutreffen von *Bedingung1* die wird die *Anweisung1* ausgeführt. Trifft *Bedingung1* nicht, *Bedingung2* aber schon zu, so wird *Anweisung2* ausgeführt. Trifft keine der beiden Bedingungen zu, so wird *Anweisung3* ausgeführt.

Um ein `if` formulieren zu können, müssen wir also wissen, was eine Bedingung ist. Eine Bedingung ist nichts anderes als ein Kommando. Ist dessen Exit Status 0, so gilt die Bedingung als erfüllt. Andernfalls gilt sie als nicht erfüllt. Das erklärt auch, warum man den Konventionen des Exit Status in eigenen Scripts folgen sollte.
Ein in Bezug auf Bedingungen besonders wertvoller Befehl ist der built-in Befehl `test`. Will man zum Beispiel feststellen, ob der Inhalt der Variable `TEST` gleich „rose“ ist, so kann man das so überprüfen:

```
$ TEST=rose
$ test $TEST = rose
$ echo $?
0
$ TEST=eros
$ test $TEST = rose
$ echo $?
1
```

Als Synonym für `test` können auch eckige Klammern `[]` verwendet werden, wobei darauf zu achten ist, dass nach der

öffnenden und vor der schließenden Klammer Leerzeichen stehen.

```
$ TEST=rose
$ [ $TEST = rose ]
$ echo $?
0
```

Arithmetik
Neben der Möglichkeit ganze Zahlen gegeneinander zu testen, kann man in der Shell mit ganzen Zahlen auch Rechnen. Ausdrücke die mit `$[]` oder `$(())` umschlossen sind werden als ganzzahlige Rechenoperationen ausgelegt und auszuwerten versucht.

```
$ echo "1+1=$[1+1]"
1+1=2
$ echo "3*3=$((3*3))"
3*3=9
$ echo "11/4=$[11/4] mit Rest $[11%4]"
11/4=2 mit Rest 3
```

In der Programmierung ist es häufig gefragt, den Inhalt einer Variable zu inkrementieren, sprich um 1 zu erhöhen. Das sieht in C definitiv schöner aus, als in der `bash`:

```
$ N=1
$ echo $[$N+1]
2
```

Um in der Shell oder innerhalb von Scripts Gleitkommarechnungen oder allgemein kompliziertere Rechnungen durchzuführen sei dem Leser `bc` und `dc` and Herz gelegt.

Flow Control, `if`

- erlaubt bedingte Ausführung von Kommandos
- dem `if` in Programmiersprachen sehr ähnlich
- Syntax:

```
if Bedingung1
then
  Anweisung1
elif Bedingung2
then
  Anweisung2
else
  Anweisung3
fi
```

Der `elif` und der `else`-Block sind optional.

Die *Bedingung* ist ein Kommando, das 0 (true) oder $\neq 0$ (false) als Exit Status zurückgibt.

Folie 120

Bedingungen (Strings, Dateien)

Das ist ein unvollständige Liste von Tests mit Strings (Zeichenketten) und Dateien.

Im folgender Liste bezeichnen *S1* beziehungsweise *S2* Strings und *D1* beziehungsweise *D2* Dateinamen.

Test	**Wahr wenn**
`[` *S1* `=` *S2* `]`	Strings ident
`[` *S1* `!=` *S2* `]`	Strings nicht ident
...	
`[ -e` *D1* `]`	Datei *D1* existiert
`[ -d` *D1* `]`	*D1* ist ein Verzeichnis
`[ -x` *D1* `]`	*D1* ist ausführbar
`[` *D1* `-nt` *D2* `]`	*D1* neuer als *D2*
...	

Folie 121

Bedingungen (Integers)

Die folgenden Tests gehen davon aus, dass in den Variablen `A` und `B` ganze Zahlen stehen. Ist dies nicht so, gibt es eine Fehlermeldung.

Test	Wahr wenn
`[ $A -lt $B ]`	$A kleiner als $B
`[ $A -gt $B ]`	$A größer als $B
`[ $A -le $B ]`	$A kleiner gleich $B
`[ $A -ge $B ]`	$A größer gleich $B
`[ $A -eq $B ]`	$A gleich $B
`[ $A -ne $B ]`	$A ungleich $B

Folie 122

Arithmetik

Integerarithmetik wird innerhalb eckiger oder doppelter runder Klammern ausgewertet.

```
$ echo $[1+1]
$ echo $((1-1))
```

Eine unvollständige Liste von Operatoren:

Operator	Bedeutung
`+`	Plus
`-`	Minus
`*`	Multiplikation
`/`	Division
`%`	Modulo
`**`	Exponent

Das Inkrementieren einer Variable funktioniert folglich so:

```
$ N=1
$ N=$[$N+1]
$ echo $N
```

Folie 123

Bedingungen Verknüpfen
Neben dem `if` gibt es noch eine einfachere, eingeschränkte Möglichkeit des bedingten Ausführens von Kommandos. So wird im Folgenden der Befehl `ls` nur ausgeführt, wenn die Programmdatei `/bin/ls` existiert und ausführbar ist:

```
$ [ -x /bin/ls ] && ls
helloworld  parameterexists  parameters
```

Der Exit Status solch einer Kette von Kommandos ist der Exit Status des letzten ausgeführten Kommandos. Ein weiteres Beispiel legt eine Datei *foo* nur an, wenn diese noch nicht existiert:

```
$ touch foo
$ ls
foo
$ [ -e foo ] || touch foo
$ echo $?
0
$ [ ! -e foo ] && touch foo
$ echo $?
1
```


Bedingtes Ausführen

`$ Kommando1 && Kommando2`

Kommando2 wird ausgeführt, wenn Kommando1 Exit Status 0 hat.

`$ Kommando1 || Kommando2`

Kommando2 wird ausgeführt, wenn Kommando1 Exit Status $\neq 0$ hat.

- Der Exit Status dieser Zeilen ist der Exit Status des letzten ausgeführten Kommandos.
- Ein `!` vor einem Kommando verneint den Exit Status.

Operator	Bedeutung
`&&`	Und
`||`	Oder
`!`	Nicht

- Kann benutzt werden, um verknüpfte Bedingungen in einer `if`-Anweisung zu erstellen.

Folie 124

Flow Control, `case`

Eine spezielle und für manche Anwendungen sehr angenehme Variante der `if`-Anweisung ist die `case`-Anweisung, die nach folgender Syntax verlangt.

```
case Ausdruck in
  Pattern1)
    Anweisungen ;;
  Pattern2)
    Anweisungen ;;
  ...
esac
```

Das bietet sich zum Beispiel dazu an, um Switches zu realisieren. Wie bei Initscripts üblich erlaubt folgendes Script eine „start“ und „stop“ Option:

```
case $1 in
  start) ...;;
  stop) ...;;
  *) Usage: ...;;
esac
```

Folie 125

case-Anweisung
Die `case`-Anweisung wird oft in Initscripts verwendet. Diese Scripts dienen zum Starten und Stoppen von Systemdiensten. Üblicherweise liegt für jeden Systemdienst im Verzeichnis `/etc/init.d/` (manchmal auch `/etc/rc.d/init.d` oder `/etc/rc.d/`) ein Script, das die Parameter `start`, `stop` oder `restart` versteht (vgl. Teil 1, Abschnitt 9.2).

```
$ cat /etc/init.d/inetd
#!/bin/sh
#
# start/stop inetd super server.
[...]
case "$1" in
    start)
        echo -n "Starting internet superserver:"
        [...]
        ;;
    stop)
        echo -n "Stopping internet superserver:"
        [...]
        ;;
    restart)
        echo -n "Restarting internet superserver:"
        [...]
        ;;
    *)
        echo "Usage: /etc/init.d/inetd {start|stop|restart}"
        exit 1
        ;;
esac
```

Gibt man einen Parameter an, der nicht angeführt ist, so wird der Punkt unter `*)` ausgeführt. Dieser klärt über die richtige Benutzung des Scripts auf und beendet das Script mit Exit Status 1.

for-Anweisung
Die `for`-Schleife unterscheidet sich stark von `for`-Schleifen anderer Programmiersprachen. In ihr durchläuft ein Variable alle Werte einer Liste. Die Einträge dieser Liste sind durch Leerzeichen, Tabulatoren oder Zeilenumbruch getrennt. Alle Frauen sind herzlichst dazu eingeladen das Script *polygam* nach ihren Bedürfnissen zu modifizieren.

```
#!/bin/bash

LISTE="Liese Ingrid Stefanie Frauke"
for FRAU in $LISTE; do
   echo "$FRAU ist meine Frau."
done
```


Flow Control, `for`

Syntax der `bash` `for`-Schleife wesentlich anders als in vielen Programmiersprachen

`for` *Name* `in` *Liste*
`do`
Anweisungen
`done`

- Inhalt der Variable Name durchläuft alle Elemente der Liste
- folgender Code spiel alle mp3-Dateien im aktuellen Verzeichnis ab

```
for LIED in *.mp3
do
 mpg123 $LIED
done
```

`mpg123` ist ein mp3-Player.
`*.mp3` wird von der `bash` zu einer Liste aller Dateien mit der Endung `.mp3` expandiert.

Folie 126

while- und until-Anweisung
Oft will man an einer bestimmten Stelle in einem Script die Ausgabe eines Kommandos platzieren. Das nennt man Kommando-Substitution und lässt sich auf zwei Arten realisieren. Das Kommando wird entweder mit Backticks (Backquotes) ‘‘ oder mit `$()` umschlossen. Das Script *summerton* ist der Telefonzeitansage nachempfunden:

```
#!/bin/bash

# Zeitausgabe ala Zeitansage per Telefon

# Warten bis zu den naechsten vollen 10 Sekunden
while [ $[‘date +%S‘%10] -ne 0 ]; do
   sleep 1
done

# Alle 10 Sekunden Zeitansage
while true; do
   echo "Es wird mit dem Summerton ‘date +%k‘ Uhr, \
‘date +%M‘ Minuten und ‘date +%S‘ Sekunden."
   sleep 10
done
```

Die Frage ob man ‘‘ oder `$()` verwendet ist nicht ganz irrelevant. Die Verwendung von `$()` hat den Vorteil, dass man diese Konstruktion ineinander verschachteln kann. Der Nachteil ist, dass diese Konstruktion in der `bash`, nicht jedoch in der `sh` existiert. Versucht man ein Script, das `$()` verwendet auf einem System ohne einer `bash` zu verwenden, so wird dies scheitern.

Die `until`-Anweisung funktioniert völlig analog zu `while` natürlich mit dem Unterschied, dass der Aweisungsblock ausgeführt wird, wenn die Bedingung nicht erfüllt ist.

Das übliche For I
Um das in anderen Programmiersprachen übliche Verhalten einer `for`-Schleife zu erhalten kann folgender Code in *usualfor1* dienen:

```
#!/bin/bash

# Immitiert ein for wie in C, wobei dies einem
# for(int i=$START, i<=$STOP, i=i+$STEP) entspricht

START=1; STOP=10; STEP=3

for N in ‘seq $START $STEP $STOP‘
do
   echo $N
done
```

`$N` durchläuft alle Werte von `$START` bis `$STOP` in Abständen von `$STEP`.
Zur Kommando-Substitution werden hier Backticks (‘‘) verwendet, was die Portabilität des Codes erhöht. In den meisten Fällen kann auf eine einfachere Syntax von `seq` zurückgegriffen werden. Siehe dazu
`$ man seq`

Flow Control, `while, until`

`while`- bzw. `until`-Syntax entspricht der in anderen Programmiersprachen.
Anweisungsblock wird, solange eine Bedingung wahr bzw. nicht wahr ist, ausgeführt.

```
while Bedingung
do
  Anweisungen
done
```

Als Beispiel ein Codesegment, das alle 5 Sekunden prüft, ob eine Modemverbindung existiert und falls diese zusammengebrochen ist, eine Funktion namens `reconnect()` ausführt.

```
while ifconfig | grep ppp0
do
 sleep 5
done
reconnect()
```

Folie 127

Das übliche For II
Eine weitere Methode, das in anderen Programmiersprachen übliche `for` zu erhalten, ist die folgende Umschreibung in *usualfor2*, die natürlich nicht Shell spezifisch ist:

```
#!/bin/bash

# umschreibt ein for wie in C
# durch ein while

START=1; STOP=10; STEP=3

N=$START
while [ $N -le $STOP ]; do
   echo $N
   N=$[$N+$STEP]
done
```

Auch hier durchläuft `$N` alle Werte von `$START` bis `$STOP` in Abständen von `$STEP`.

Zum Abschluß geben wir noch einige Quellen für (weiterführende) Informationen zur Bashprogrammierung an.

Quellen

1. Manpage
   `$ man bash`
2. Bücher
   C. Newham, B. Rosenblatt, „Learning the Bash Shell"(2nd Edition, 'O' Reilly, 1998)
3. Webpages
   `www.gnu.org/manual/bash-2.02/`
   `/html_manual/bashref.html`
   `www.ldp.at/HOWTO/Adv-Bash-Scr-HOWTO/`
   `unixhelp.ed.ac.uk/scrpt/scrpt2.html`
   `www.beforever.com/bashtut.htm`
   `www.linuxgazette.com/issue25/dearman.html`
   `pegasus.rutgers.edu/~elford/`
   `/unix/bash-tute.html`
4. auf jedem System vorhandene Scripts
   `/etc/init.d/*`
   `~/.bashrc`

Folie 128

12 Grundlagen der Security und Logging

Dieses Kapitel dient der Besprechung grundlegender Sicherheitskonzepte und Sicherheitsmechanismen. Wir erklären SUID, SGID und Sticky-Bit Berechtigungen und die Grundlagen des Pluggable Authentication Module (PAM). Wir geben einen Überblick über das Logging auf Linuxsystemen – das nicht nur im Bereich der Sicherheit, sondern auch bei jeglicher Fehlersuche eine große Rolle spielt – und erklären die Konfiguration des Systemlogdaemons. Schließlich besprechen wir Varianten von Angriffen auf Computersysteme und diskutieren grundlegende Schutzmechanismen.

Bei der Entwicklung von Unix und Linux war und ist Sicherheit nicht das primäre Ziel; im Vordergrund stehen vielmehr Machbarkeit und Benutzerfreundlichkeit. Daher werden und wurden Unix/Linux-Systeme immer wieder Ziel von Attacken und Einbrüchen. Es ist eine der wesentlichen Aufgaben des Systemadministrators, die Sicherheit des Systems und seiner Daten zu überwachen und sicherzustellen.
In kaum einem Bereich der Systemadministration spielen Planung, Methode und „Politik" eine so große Rolle, wie im Bereich der Sicherheit. Bei größeren Systemen ist es unumgänglich, ein umfassendes Sicherheitskonzept zu erarbeiten, in dem genau festgelegt wird, was wie geschützt werden soll. (Man denke zB an den juristischen Aspekt.) Die „politischen Aspekte" (vgl. Kapitel 1) der Sicherheit von Computersystemen sind vor allem deshalb besonders zu beachten, weil die Sicherheit indirekt proportional zur Bequemlichkeit der User ist (siehe auch Folie 129). Vor der allgemeinen Diskussion warum und wovor Computersysteme geschützt werden müssen erklären wir in jeweils eigenen Abschnitten spezielle Dateiberechtigungen, das Pluggable Authentication Module (PAM) und das Logging auf Linuxsystemen.

Security

- Unix optimiert Benutzerfreundlichkeit, nicht Sicherheit
- $$\text{security} = \frac{1}{\text{convenience}}$$
- „politische Aspekte“
- rechtliche Aspekte
- umfassendes Sicherheitskonzept

Folie 129

12.1 Spezielle Dateiberechtigungen

Ein wichtiger Punkt der Unix-Sicherheitskonzeption ist das *SUID (Set UID)-Bit*. Dabei handelt es sich um eine spezielle Dateiberechtigung, die es erlaubt, ein Kommando nicht mit den Rechten des Benutzers, der es aufruft, sondern mit den Rechten des Besitzers der Programmdatei auszuführen. Dieses Konzept ermöglicht es, dass zB ein normaler Benutzer sein Passwort ändern kann. Dazu muss ja der Passworteintrag in `/etc/passwd` bzw. `/etc/shadow` geändert werden, also eine Datei geschrieben werden, für die nur root Schreibrecht besitzt. Daher ist für das Programm zur Passwortänderung (`/usr/bin/passwd`) das SUID-Bit gesetzt. SUID-Programme stellen immer ein potentielles Sicherheitsrisiko dar und sind oft Ziel von Hackern. Daher sollte die Zahl an SUID-Programmen am System möglichst gering gehalten werden und regelmäßig überprüft werden, ob nicht neue SUID-Programme aufgetaucht sind (Zeichen für Hackereinbruch!).
Analog dazu (aber in der Praxis weniger relevant) gibt es das Konzept des *SGID-Bits*, das es ermöglicht ein Programm mit den Gruppenrechten des Gruppenbesitzers des Programmfiles auszuführen. Ist auf einem Directory das SGID-Bit gesetzt, so erhält ein, in diesem Verzeichnis erstelltes File den Gruppenbesitz des Gruppenbesitzers des Directories.

Eine weitere spezielle Berechtigung ist das sogenannte *Sticky-Bit* für Verzeichnisse. Ähnlich wie das SGID-Bit für Verzeichnisse erfüllt es eine wichtige Funktion vor allem bei Directories, die von einer aus mehreren Benutzern bestehenden Gruppe verwendet wird. Ist für ein Verzeichnis das Sticky-Bit gesetzt, so kann ein Benutzer, selbst wenn er Schreibrechte in diesem Directory besitzt nur Dateien schreiben, in deren Besitz er sich befindet. (Sonst reicht ja die Schreibberechtigung im Directory aus, um *alle* Files darin (auch die, für die keine Schreibberechtigung besteht) zu löschen; das Sticky-Bit entspricht somit der Option „Ändern, Ersteller/Besitzer“ in der NT ACL. Typischerweise ist für das `/tmp`-Directory das Sticky-Bit gesetzt. Achtung es vererbt sich *nicht* automatisch auf Subdirectories!

Die speziellen Berechtigungen SUID, SGID und Sticky-Bit können (ganz genau wie die Basisberechtigungen „rwx“) mittels `ls -l` angezeigt und mittels `chmod` verändert werden. Im symbolischen Modus werden SUID, SGID und Sticky-Bit mit „s“, bzw. „t“ bezeichnet: `chmod u=s` bzw. `g=s` setzt also das SUID resp. das SGID Bit, das Sticky-Bit wird mit `chmod o=t` gesetzt. Die oktale Syntax hierfür wird auf den Folien 130 und 131 erklärt, die auch das Setzen der Basisberechtigungen sowie des Besitzers von Files und Directories aus Teil 1, Abschnitt 3.6 wiederholen.

Fileberechtigungen

Perm.	File	Directory
r=4	lesen	listen
w=2	schreiben	Files schreiben
x=1	ausführen	cd, PATH
SUID	runs with UID=owner	
SGID	runs with GID=owner	neue Files GID=Directory
Sticky-Bit		nur Besitzer von File oder Dir. kann schreiben

Folie 130

Besitz/Berechtigungen ändern

- Jedes File hat Besitzer und Gruppenbesitzer;
  ändern mit
  - `chown karli vielgeld.tex`
  - `chgrp finanz vielgeld.tex`
  - `chown karli.finanz vielgeld.tex`
- Berechtigungen rwx(s,t) oder numerisch;
  ändern mit
  - `chmod 1755 (o+t)...rwxr-xr-t`
  - `chmod 2755 (g+s)...rwxr-sr-x`
  - `chmod 4755 (u+s)...rwsr-xr-x`

Folie 131

12.2 PAM

In diesem kurzen Abschnitt besprechen wir die Grundlagen des Pluggable Authentication Module- System (PAM). Dabei handelt es sich um eine Sammlung gesharter Bibliotheken, die systemweite Authentifizierungsaufgaben übernimmt und dadurch vereinheitlicht. Es gibt eine Vielzahl von Prozessen, die eine Authentifizierung vornehmen müssen (zB `login, su, sshd, ftp, telnetd`, etc.).
Müssten diese Programme jeweils direkt auf die verschiedenen Authentifizierungsmechanismen zugreifen, so würde sich ein fast unüberschaubares Konfigurationschaos ergeben (siehe Folie 133). An diesem Punkt setzt das PAM-System ein. Muss irgendein Prozess eine Authentifizierung vornehmen (zB Login) so nimmt er dafür PAM in Anspruch. Das PAM-System erledigt gemäß seiner Konfiguration in `/etc/pam.d/` die Authentifizierung und meldet dem anfragenden Prozess, ob die entsprechende Authentifizierung positiv erledigt werden konnte.

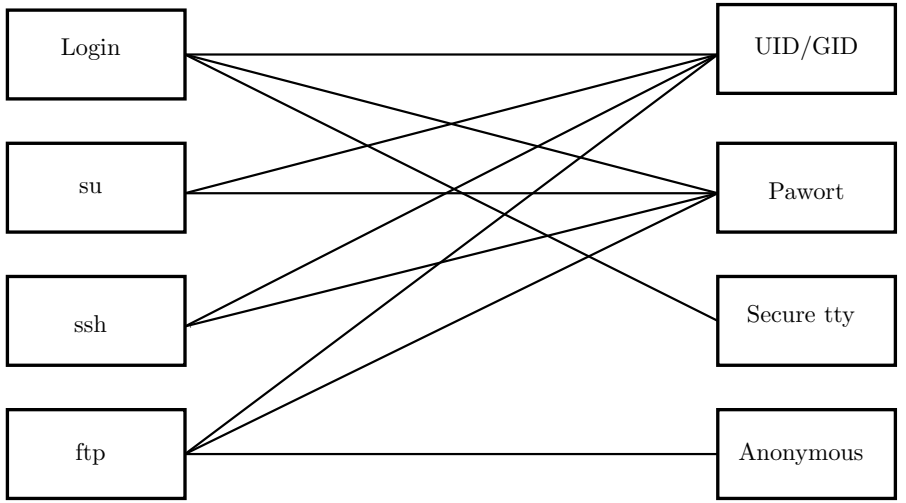
Die Konfiguration des PAM wird auf den Folien 135 und 136 erläutert. Darüber hinaus findet man Informationen über PAM auf der Manpage bzw. unter `http://www.kernel.org/pub/linux/libs/pam`.

Pluggable Authentication Modules (PAM)

- Sammlung gesharter Libraries
- übersichtliche Konfiguration, wie Anwendungen Benutzer authentifizieren
  `/etc/pam.d/`
- entwickelt von Sun Microsystems
- adaptiert für Linux

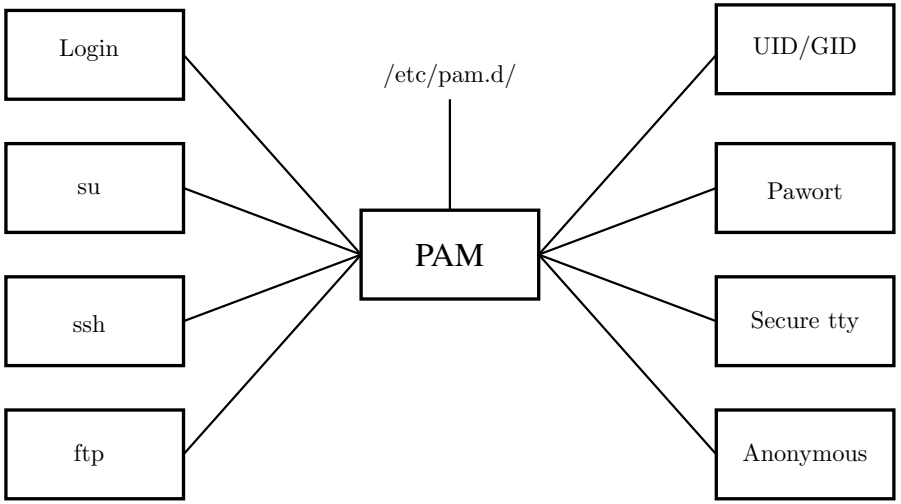
Folie 132

Authentifizierung ohne/vor PAM



Folie 133

Authentifizierung mit PAM



Folie 134

PAM Konfiguration (1)

```
[root@pablo /tmp]# cat /etc/pam.d/login
#%PAM-1.0
auth       required     /lib/security/pam_securetty.so
auth       required     /lib/security/pam_pwdb.so
                          shadow nullok
auth       required     /lib/security/pam_nologin.so
account    required     /lib/security/pam_pwdb.so
password   required     /lib/security/pam_cracklib.so
password   required     /lib/security/pam_pwdb.so
                          nullok use_authtok shadow
session    required     /lib/security/pam_pwdb.so
session    optional     /lib/security/pam_console.so
```

Folie 135

PAM Konfiguration (2)

```
[root@pablo /tmp]# cat /etc/pam.d/ssh
#%PAM-1.0
auth       required     /lib/security/pam_pwdb.so shadow
auth       required     /lib/security/pam_nologin.so
account    required     /lib/security/pam_pwdb.so
password   required     /lib/security/pam_cracklib.so
password   required     /lib/security/pam_pwdb.so shadow
                          nullok use_authtok
session    required     /lib/security/pam_pwdb.so
```

Folie 136

12.3 Logging

Wir besprechen zunächst die wichtigsten *Logfiles* auf einem Unix/Linux-System, in denen (je nach Konfiguration) alle relevanten Ereignisse am System protokolliert werden. Diese Dateien sind neben ihrer Sicherheitsrelevanz natürlich auch für viele weitere Aufgaben des Systemadministrators wichtig (Monitoring, Fehlersuche und Behebung,...).
Auf fast allen Linux-Systemen befinden sich diese Dateien in `/var/log/`, auf anderen Unix-Systemen aber auch oft in `/var/adm/` oder `/usr/adm/`.
Das wichtigste Logfile ist `/var/log/messages`, in dem die meisten relevanten Informationen gespeichert werden; es ist eine ASCII Datei, die zB mit `less` angesehen werden kann. Weitere wichtige Logdateien sind auf Folie 137 zusammengestellt. Die Dateien `lastlog, wtmp` und `utmp` sind binär und können mittels der entsprechenden Kommandos auf Folie 138 ausgewertet werden.

Das Logging in Unix-Systemen wird mittels des Syslog Daemons `syslogd` (und des Kernel-Log Daemons `klogd`) durchgeführt. Der Syslog Daemon wird in `/etc/syslog.conf` konfiguriert und nimmt von verschiedenen anderen Prozessen bzw. dem Kernel geordnet nach sog. Facilities: (auth(=security), authpriv, cron, daemon, kern, lpr, mail, mark, news, syslog, user, uucp und local0–local7) Meldungen verschiedener Priorität (debug, info, notice, warning(=warn), error(=err), crit, alert, emerg(=panic)) entgegen und schreibt sie gemäß seiner Konfiguration in verschiedene Dateien bzw. leitet sie weiter. Mehr Information über den Syslog Daemon bzw. seine Konfiguration ist den entsprechenden Manpages mittels `man syslog` bzw. `syslog.conf` zu entnehmen.

Logfiles

- `/var/log/messages`... Masterlogfile (ASCII)
- `/var/log/lastlog`... letzter erfolgreicher Login
- `/var/log/secure`... erfolglose Logins (ASCII)
- `/var/log/wtmp`... erfolgreiche Logins
- `/var/run/utmp`... derzeit eingeloggte User
- `/var/log/{maillog, http, cups, rpmpkgs, XFree86, samba}`, etc. ... Logfiles einzelner Programme

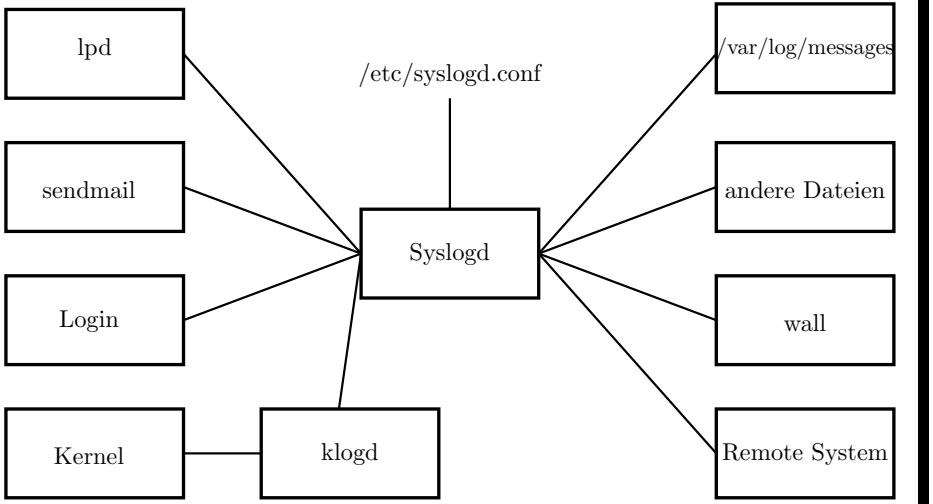
Folie 137

Nützliche Kommandos

- `w`... Wer ist eingeloggt und tut was?
- `who`... Wer ist eingeloggt und weitere Information aus `/var/log/utmp, wtmp`
- `last`... Wer war wann das letzte Mal eingeloggt
- `lastlog`... Letztes login aller User
- `tail -f file`... zeige die letzten 10 Zeilen des Files und neuen Input

Folie 138

Das Logging-Konzept



Folie 139

Der Syslog-Daemon

- Konfiguration `/etc/syslog.conf`
- Facilities
  - auth(=security)
  - cron
  - daemon
  - kern
  - mail, ...
- Priorities
  - debug
  - info
  - warning(=warn)
  - crit
  - emerg(=panic), ...

Folie 140

/etc/syslog.conf

```
# Log anything (except mail) of level info or higher.
# Don't log private authentication messages!
*.info;mail.none;authpriv.none  /var/log/messages
# The authpriv file has restricted access.
authpriv.*                      /var/log/secure
# Log all the mail messages in one place.
mail.*                          /var/log/maillog
# Everybody gets emergency messages, plus log them on another
# machine.
*.emerg                         *
# Save mail and news errors of level err and higher in a
# special file.
:uucp,news.crit                 /var/log/spooler
```

Folie 141

/var/log/messages

```
Apr 30 21:08:04 phobos rpc.mountd: authenticated mount request
from radon.mat.univie.ac.at:1000 for /users/gerald (/users)
Apr 30 21:13:43 phobos rpc.mountd: authenticated unmount request
from radon.mat.univie.ac.at:1012 for /users/gerald (/users)
Apr 30 21:23:20 phobos sshd2[1143]: connection from "131.130.145.151"
Apr 30 21:23:21 phobos sshd2[13747]: Remote host disconnected:
Connection closed.
Apr 30 21:23:21 phobos sshd2[13747]: connection lost:
'Connection closed.'
Apr 30 21:23:52 phobos sshd2[1143]: connection from "131.130.145.151"
Apr 30 21:24:06 phobos rpc.mountd: authenticated mount request
from radon.mat.univie.ac.at:602 for /users/gerald (/users)
Apr 30 21:24:13 phobos sshd2[13750]: User root's local password accepted.
Apr 30 21:24:13 phobos sshd2[13750]: Password authentication for user
root accepted.
Apr 30 21:24:13 phobos sshd2[13750]: User root, coming
from hektor.mat.univie.ac.at, authenticated.
```

Folie 142

12.4 Sicherheit – Allgemeine Diskussion

Warum sollte ein System geschützt werden?
Diese Frage umfasst zwei wesentliche Themengebiete. Einerseits muss man sensible Benutzerdaten schützen, andererseits den Rechner selbst, damit das System verfügbar bleibt und nicht mißbräuchlich verwendet wird.
Attacken gegen die *Verfügbarkeit des Systems* werden DoS (Denial of Service) Attacken genannt. Dabei bzw. bei der (unter bösartigen Hackern besonders beliebten) „erweiterten Variante“ der Distributed DoS Attacken (DDoS) beanspruchen mehrere Rechner (in der Größenordnung von einigen 100, in seltenen berühmten Fällen (yahoo) noch mehr) gleichzeitig ein Service (etwa einen Webserver) des angegriffenen Systems, bis dieses unter der hohen Systemlast zusammenbricht und jeden weiteren Zugriff verbietet.
Der Schutz vor *missbräuchlicher Verwendung* ist deshalb besonders wichtig, weil der Administrator dafür verantwortlich ist, dass zB von seinem System keine Angriffe auf andere Rechner erfolgen. Viele Hacker verwenden mehrere Rechner als „Zwischenstationen“, um ihre Spuren möglichst zu verwischen; es ist nur schwer möglich, über 5 und mehr Stationen hinweg Hinweise zurückzuverfolgen (besonders wenn die Rechner nicht im eigenen Netz, sondern über die ganze Welt verstreut sind).

Nicht überall wiegen die zwei genannten Bereiche – Schutz der Daten und des Systems – gleich schwer, denn zB in einem Netz mit langsamen Übertragungsraten (ev. über Modems) lässt sich ein DDoS kaum durchführen, andererseits bietet zB ein Universitätsinstitut kaum sensible Daten; allerdings ist eine Universität meistens über besonders schnelle Datenleitungen angebunden, was wiederum DDoS Angreifer anlockt. Andererseits ist es unter Umständen ein „prestigeträchtiges“ Unterfangen den Webserver einer Universität lahmzulegen. Bei Banken, Technologiekonzernen und öffentlichen Einrichtungen (zB Polizei) ist dagegen der Schutz der geheimen Daten oberstes Gebot. Eine Vernachlässigung des Datenschutzes ist hier sogar strafbar. Auf jeden Fall wird das Vertrauen des Kunden in die jeweilige Organisation dauerhaft geschädigt und den Administrator kostet es vermutlich den Job.

Wer greift an?
Die Antwort ist so einfach, wie beunruhigend: Prinzipiell **jeder** ist ein potentieller Angreifer. Obwohl Paranoia im Allgemeinen ein gewisses soziales Problem darstellt, sollte sie bei einem Systemadministrator in höherem Masse ausgeprägt sein; egal ob der Kollege von nebenan, der noch eine alte „Rechnung“ zu begleichen hat, oder ein „Nachwuchshacker“ (neudeutsch „Script-Kiddie“), der gewöhnlich ein vorgefertigtes Paket verwendet, das eine bestimmte Sicherheitslücke ausnützt, bis zum Profi-Hacker, der die Bugs in den Diensten selbst entdeckt und ein Programm („Exploit“) schreibt, das diese Bugs ausnützt. Diesem Profi-Hacker kann vermutlich kaum ein Rechner standhalten, der nur irgendeinen Dienst im Internet anbietet. Das einzige Glück, wenn man es so nennen will, ist, dass sich solche Hacker wohl kaum mit kleineren Systemen abgeben, sondern gleich die „großen Kaliber“ und „lohnende Ziele“ in Angriff nehmen.

Wie wird angegriffen?
Hier unterscheidet man (hauptsächlich) zwischen drei Möglichkeiten:

1. Physischer Angriff
Dies ist der Weg, wie man am einfachsten unauthorisierten Zugriff auf einen Rechner erlangt, denn die Hardware an sich bietet kaum Schutz. Man hat hier mannigfaltige Möglichkeiten: Ausbau der Festplatte und Einbau in einen anderen Rechner; falls ein BIOS-Passwort gesetzt ist, Abklemmen bzw. Kurzschließen der BIOS-Batterie, wodurch alle BIOS-Einstellungen gelöscht werden; Starten von Linux in den Singleuser Modus oder als Init-Prozess die Shell angeben (am LILO-Prompt `linux init=/bin/sh` eintippen), danach kann man problemlos das `root` Passwort ändern bzw. die `/etc/shadow` auf eine Diskette kopieren und auf einem schnellen Rechner Benutzerpasswörter cracken (es erregt weit weniger Aufsehen, wenn man sich als normaler Benutzer einloggt, als wenn man das root-Passwort ändert).

Vorüberlegungen

- Was soll am System geschützt werden? (Daten/Verfügbarkeit)
- Vor wem schütze ich das System?
- Gibt es sensible Daten am System?
- Zugang von außen notwendig?
- (Wie viel) Internetzugang notwendig?
- Ausreichender Schutz durch Passwörter/Verschlüsselung?

Folie 143

Auch wenn der LILO-Prompt durch ein Passwort geschützt ist, könnte man immer noch von einer eigenen Bootdiskette starten (sofern die Boot-Reihenfolge im BIOS auf `A: C:` gestellt ist); wenn ein zweites Betriebssystem auf der Festplatte ist, für das man entweder einen Account hat bzw. das keine Accounts benötigt (zB Windows 98), kann man dort ein Programm installieren, welches das Dateisystem von Linux lesen kann und sich wiederum die `/etc/shadow` (oder beliebige andere Daten) auf eine Diskette kopieren.
Der größte Nachteil für den Hacker ist, dass er tatsächlich vor Ort sein muss, um den Rechner anzugreifen. Das sollte sich durch mechanische Barrieren lösen lassen (Zugang zu den Räumen kontrollieren, Server in eigene Räume sperren, Zugangskontrolle durch Fingerabdruck, Abbild der Regenbogenhaut, ...). Bei Workstations in zB einem PC Labor wird das kaum eine komfortable Möglichkeit darstellen, sodass man hier darauf angewiesen ist, einen gewissen Überblick über die Räumlichkeiten und die Hardware darin zu halten (Aufsicht, ...).

2. Lokaler Angriff
Darunter versteht man die potentiellen Attacken eines Benutzers, der einen Account am (ev. nicht im Netz befindlichen) System hat. Da man dem Benutzer im Allgemeinen vertraut, hat er vermutlich auch physischen Zugang zum Rechner, was auch das weite Feld der oben genannten Hacks offen lässt. Zusätzlich besteht hier die Gefahr, dass der User alle Dateien im System lesen kann, denen nicht explizit die Rechte entzogen wurden. Das ermöglicht auch das Ansehen von `/etc/passwd`, in der gewöhnlich alle vorhandenen Benutzer eingetragen sind. Damit hat man zumindest schon einen Überblick über die Benutzernamen und damit eventuell schon halb gewonnen, da viele User schlechte Passwörter wählen und das Durchprobieren von Namen etc. oft zum Erfolg führt.
Eine weitere große Gefahr stellen Bugs in Systemdiensten dar, die dem User mittels Exploits oft zu root Rechten verhelfen können; ein häufig gewählter Weg ist der „Buffer Overflow“. Wenn ein Programm/Dienst Benutzereingaben akzeptiert, dürfen diese meistens eine maximale Länge von 255 Zeichen aufweisen. Ist der eingegebene String länger als diese 255 Zeichen, wird dem normalerweise vom Programm mit einer

Fehlermeldung begegnet. Unterlässt der Programmierer allerdings einen Check der Stringlänge, überschreibt das, was nach dem 255. Zeichen steht, den Hauptspeicher, der sich nach dem String befindet. Dadurch kann es vorkommen, dass alles ab dem 256. Zeichen als Kommando interpretiert und ausgeführt wird; viele Daemonen/Dienste laufen aber mit dem SUID-Bit (siehe Abschnitt 12.1), d.h. mit root-Rechten. Wenn also ab dem 256. Zeichen etwa `/bin/sh` im Speicher steht, hat man Zugang zu einer root-Shell!

3. Angriffe aus dem Netz
Neben den oben erwähnten DDoS Attacken, für die der Angreifer keinerlei Rechte auf dem Zielsystem benötigt, gibt es noch zahlreiche andere Angriffe, die ebenso wie beim lokalen Angriff einen „Buffer Overflow“ ausnutzen. Häufig betroffen sind hier hochkomplexe Internet Dienste. Wir widmen dem weiten Feld der Netzwerksicherheit das gesamte Kapitel 18.

Schutz des Systems

Es sind in der Regel drei Sicherheitsformen zu gewährleisten:

- **Physische Sicherheit**: Schutz vor Angreifern, die direkten Zugriff auf die Hardware haben.
- **Lokale Sicherheit**: Schutz vor Angreifern, die einen lokalen Account besitzen.
- **Netzwerk Sicherheit**: Schutz vor Angreifern, die keinen lokalen Account besitzen, aber über ein Netzwerk Zugriff auf den Rechner haben.

Folie 144

12.5 Sicherheit – Lösungsansätze

Natürlich können hier keine vollständigen Lösungen für alle oben genannten Probleme genannt werden, dafür ist die Materie viel zu komplex. Vielmehr geben wir einen groben Überblick; jeder Administrator entwickelt mit der Zeit ein Gespür dafür, welche Dienste/Systeme er besonders schützen muss.
Von fundamentalster Wichtigkeit für jede Art von Sicherheit ist ein regelmäßiges Einspielen der vom Distributor herausgegebenen bugbereinigten Softwarepakete (Updates). Diese Aufgabe sollte möglichst automatisiert erfolgen (siehe Abschnitt 4.3).
Außerdem wird der sicheheitsbewusste Administrator relevante Mailinglisten der Distribution und/oder allgemeine Sicherheistmailinglisten (zB Bugtraq auf `http://online.securityfocus.com` oder CERT (`http://www.cert.org`)) verfolgen.

Physische Attacken
auf die Hardware frei zugänglicher Rechner kann man wie erwähnt kaum abwehren. Daher sollte man öffentlich aufgestellte Rechner (PC-Labor) nicht lange unbeaufsichtigt lassen und private Rechner immer dem Zugriff außen Stehender entziehen.
Geht man zur Software über, eröffnet sich ein weiteres Feld an Möglichkeiten: Auf jeden Fall muss man ein BIOS-Passwort setzen und die Bootreihenfolge so ändern, dass nur mehr von der Festplatte gebootet werden darf („C only“ oder „C:“). Hacken über Diskettenzugriff ist nun weitgehend beseitigt. Sodann geht man unter Linux daran, ein LILO-Passwort zu setzen (das erfolgt in der Datei `/etc/lilo.conf`, deren Rechte daher unbedingt `600` sein sollten), damit kann man nur mehr mit den voreingestellten Kernel-Parametern booten und keinen Init-Mode manuell einstellen, wenn man das Passwort nicht kennt.
Da Linux-Systeme im Normalfall wochen- bis monatelang ohne Reboot laufen, ist eine zusätzliche Option das Neustarten mittels Menü auf dem GUI oder CTRL+ALT+DEL zu unterbinden (keine Garantie gegen das Stromabschalten). Ersters erfolgt übder die Konfiguration des Desktopsystems (Loginmanager), letzteres in `/etc/inittab` durch Auskommentieren der entsprechenden Zeile, danach muss man noch `init q` ausführen, damit die Änderungen aktiviert werden.

Physische Sicherheit

Zugang zu Hardware erschweren:

- kein Zugang zur Hardware (Server)
- kein Zugang zu BIOS-Setup (kein Booten von Floppy!)
- Software Reboot disablen
  - Loginmanager des GUI
  - CTRL+ALT+DEL in `/etc/inittab`
    `#ca::ctrlaltdel:/sbin/shutdown -t3 -r now`
    mit `/sbin/init q` aktivieren

Folie 145

Lilo Passwort

Für die Übergabe von Bootparametern an den Kernel Authentifizierung verlangen.

In `/etc/lilo.conf` die Zeilen:

```
restricted
password=<password>
```

einfügen.
Danach Rechte für `/etc/lilo.conf` auf `600` setzen und

`lilo` ausführen.

Folie 146

Um **lokalen Attacken** möglichst entgegenzuwirken, sollte der Administrator sicherstellen, dass alle User ein gutes und kaum zu erratendes Passwort gesetzt haben, das auch eine höhere Verschlüsselung als normale Unix-Passwörter hat (durch Einsatz von md5-Verschlüsselung). Die Verwendung von `/etc/shadow` ist zum Glück unter beinahe allen Linux/Unix-Varianten inzwischen Standard, sodass unter Normalbedingungen kein User an ein Passwort geraten kann, das nicht für ihn bestimmt ist (vgl. Abschnitt 3.1).
Als Administrator selbst sollte man unbedingt den `su` bzw. `sudo` Befehl verwenden, statt sich als root einzuloggen (vgl. auch Abschnitt 1.3). Außerdem ist es beinahe tödlich, eine root Shell unbeabsichtigt offen zu lassen. Ein fortgeschrittener Anwender vorausgesetzt, der einige Minuten Zeit hat, kann sich im System einnisten. Einem „gehackten“ Rechner sollte man niemals wieder vertrauen und nach Möglichkeit sofort neu installieren und alle Passwörter ändern. Die Folgen der Nachlässigkeit von root lassen sich zwar durch ein Timeout der Shell, wenn eine bestimmte Zeit lang keine Tasten gedrückt werden, mindern (durch die Shell-Variable `TMOUT`, deren Wert man in Sekunden setzt), aber generell muss man natürlich trotzdem äußerst wachsam sein.
Durch die entsprechenden Dateien in `/etc/` lassen sich die Benutzer von `cron`, `at` etc. einschränken (vgl. 6.2). Speziell privilegierte Pseudobenutzer sollten niemals Cronjobs ausführen dürfen; tritt dies auf, so ist das ein relativ sicheres Zeichen, dass mit dem System etwas nicht stimmt.
Besonders gefährlich (zB bei den genannten „Buffer Overflows“) sind SUID-Programme, die von Administratoren mitunter auch als „Suizid“-Programme bezeichnet werden und das nicht ohne Grund. Nicht benötigte SUID-Dateien sind unbedingt zu deinstallieren und bei benötigten muss man das Augenmerk darauf legen, ob diese Dateien seit der Installation jemals verändert wurden (zB mittels `rpm`).

Was die **Netzwerksicherheit** betrifft, gilt hier allgemein, dass man auf jeden Fall alle nicht benötigte Dienste stoppen (zB `service httpd stop`) und per `chkconfig` aus der Liste der Dienste, die beim Hochfahren des Rechners gestartet werden, entfernen muss. Viele weitere Aspekte der Netzwerksicherheit besprechen wir im Kapitel 18.

Lokale Sicherheit (1)

- **Passwörter:**
  - sinnvolle Mindestlänge von 8 Zeichen
    mit: `# vi /etc/login.defs`
    Zeile ändern auf: `PASS_MIN_LEN 8`
  - **md5** und **shadow** verwenden
    (Default in vielen Disributionen)
    Konfig unter RedHat mit `authconfig`
- `su [-]` statt root login verwenden!
- Keine unbeaufsichtigte root Shell hinterlassen
  Umgebungsvariable `TMOUT=600` für `root` setzen

Folie 147

Lokale Sicherheit (2)

- Cronjobs nur für bestimmte Benutzer erlauben (`/etc/cron.allow`).
- Nicht benötigte SUID-Programme deinstallieren.
  Auflisten mit `find / -perm -4000`
- `su`-Befehl nur für Mitglieder der Gruppe `wheel` erlauben
  In `/etc/pam.d/su` folgende Zeile eintragen:
  `auth required /lib/security/pam_wheel.so group=wheel use_uid`
- ...

Folie 148

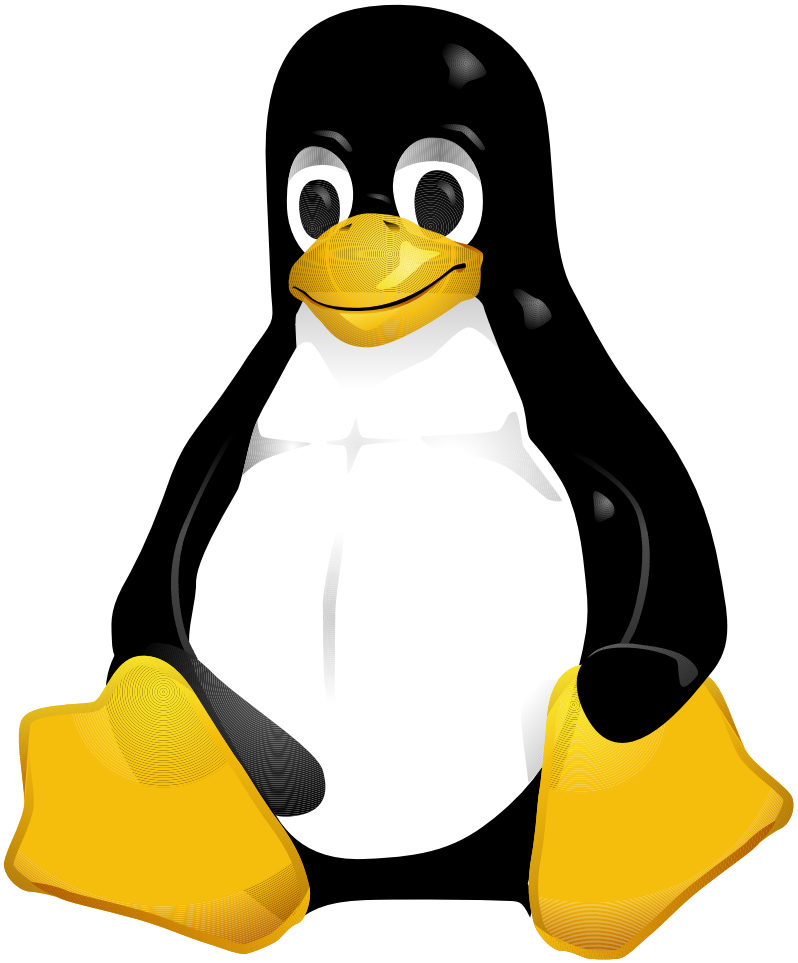
Technische Praxis der Computersysteme

Teil 2-2

Netzwerkadministration
unter Linux/Unix

Roland Steinbauer, Andreas Nemeth, Martin Piskernig,
Gerald Teschl, Florian Wisser

Version 1.00, Mai 2001



Inhaltsverzeichnis

Literatur

[9] Charles Aulds. *Linux Apache Web Server Administration.* Sybex Inc. 2000.

[10] Bryan Costales, Eric Allman. *Sendmail.* 2nd Edition. O'Reilly & Associates Inc. Sebastopol, CA. 1997.

[11] Robert Eckstein, David Collier-Brown. *Using Samba.* O'Reilly & Associates Inc. Sebastopol, CA. 1999.

[12] Craig Hunt. *TCP/IP Netzwerk Administration.* 2nd Edition. O'Reilly & Associates Inc. Sebastopol, CA. 1997.

[13] Craig Hunt. *Linux Sendmail Administration.* Sybex Inc. 2001.

[14] Mohamet J. Kabir. *Apache Server Administrator's Handbook.* Hungry Minds. 1999.

[15] W. R. Stevens. *TCP/IP Illustrated, Vol. 1: The Protocols.* Addison Wesley Longman Publishing. 1994.

13 TCP/IP-Grundlagen

Dieses Kapitel ist eine komprimierte Einführung in die Terminologie und die grundlegende Funktionsweise der TCP/IP-Protokollfamilie. Aus diesem großen Gebiet erklären wir gerade die Begriffe und Konzepte, die in den weiteren Kapiteln verwendet werden und deren Verständnis unbedingte Voraussetzung ist. Darüberhinaus verweisen wir auf die vielen guten Bücher zum Thema und insbesondere auf [12] und [15].

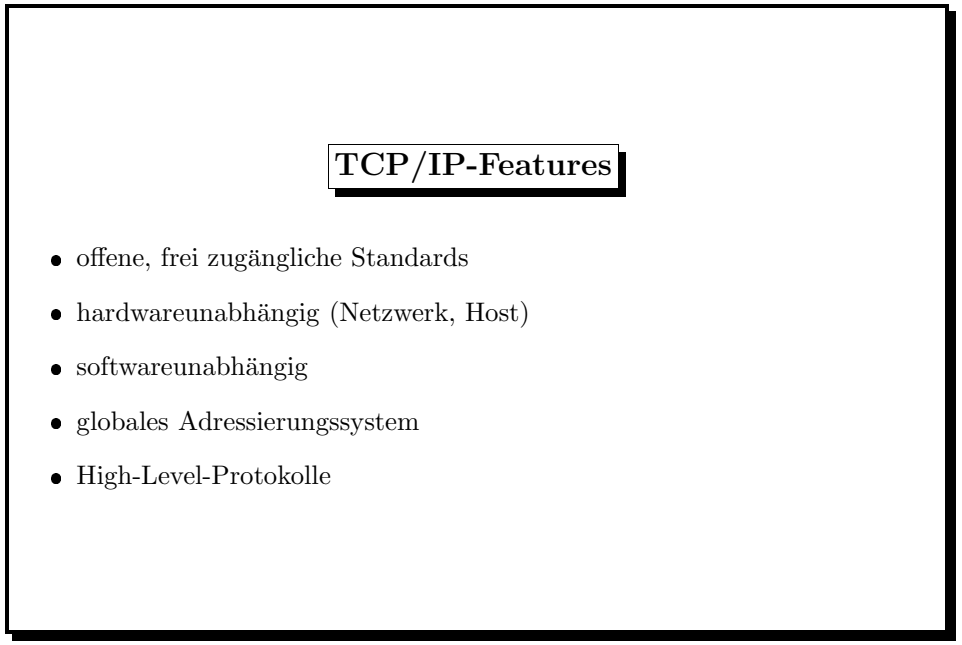
Eines der Zeichen, das den großen Erfolg von Computernetzwerken (diese sind mit großer Geschwindigkeit weit über ihre ursprünglich geplanten Dimensionen hinausgewachsen) im letzten Jahrzehnt begleitet, ist die Verwirrung, die sich um den Begriff „*Internet*“ rankt. Ursprünglich war damit ein Netzwerk gemeint, das auf dem sog. Internet Protokoll aufbaut. Mittlerweile bezeichnet dieser Ausdruck entweder eine Kollektion von verschiedenen physikalischen Netzwerken, die durch ein gemeinsames Protokoll verbunden werden, oder gleich das (ganze) weltweite Computernetzwerk.

Wir besprechen hier die Grundlagen des Internet Protokolls, eigentlich *Transmission Control Protocol/Internet Protocol (TCP/IP)*. In der Netzwerkterminologie bezeichnet „Protokoll“ einen Satz von Regeln, Standards und Vorschriften für die Kommunikation im Netzwerk. (Für eine kleine Begriffserklärung siehe Folie 149.)
Genaugenommen ist TCP/IP nicht nur ein einziges Protokoll, sondern eine ganze Familie von aufeinander abgestimmten und miteinander verbundenen Protokollen. TCP/IP zeichnet sich vor allem durch folgenden Merkmale aus, die auch ein Grund für seine weite Verbreitung sind: *Offene Protokoll Standards*, die unabhängig von Rechner- und Netzwerk-Hardware und Betriebssystem festgelegt und frei zugänglich sind, ein *globales Adressierungssystem*, das eine eindeutige Adressierung aller Hosts (selbst im weltweiten Internet) ermöglicht und die *Standardisierten High-Level-Protokolle* für bequeme, konsistente und verlässliche Anwendungen (siehe auch Folie 150).

Netzwerkterminologie

- Protokoll: Satz von Regeln und Kommunikationsstandards
- TCP/IP: Transport Control Protocol/Internet Protocol Protokollfamilie
- Host: Rechner in einem TCP/IP-basierten Netzwerk
- Internet: Netzwerk von TCP/IP basierten Netzwerken
- Gateway/Router: physikalisch an mehrere Netzwerke angebundener Host

Folie 149



Folie 150

Die TCP/IP-Standards werden von verschiedenen Organisationen (siehe Folie 151) weiterentwickelt und in frei zugänglichen Dokumenten, den sogenannten *RFC's (Requests for Comment)* veröffentlicht. Diese Organisationen übernehmen auch wesentliche Verwaltungsaufgaben für das weltweite Netz, vor allem im Bereich der Adressierung und Namensvergabe.
Jeder Softwarehersteller oder Programmierer kann nach eigenem Belieben TCP/IP-Protokolle in sein Produkt/Betriebssystem implementieren; die erste Implementation von TCP/IP in ein Betriebssystem erfolgte 1983 in BSD-Unix.

13.1 Die TCP/IP-Protokollfamilie

Wir geben nun einen schematischen, kurzen Überblick über die interne Strukturierung der TCP/IP- Protokollfamilie. Unser Ziel ist es, ein grundlegendes Verständnis für die Kommunikationsprozesse zu vermitteln, ohne zu sehr auf Details einzugehen.

Um die Kommunikation nicht nur von Host zu Host, sondern von einer spezifischen Anwendung, die ein bestimmter Benutzer auf einen Host ausführt mit einer anderen Anwendung, die ein anderer Benutzer auf einem anderen Host ausführt (inklusive verlässlicher Datenübertragung) zu ermöglichen, ist ein komplexes Bündel von Kommunikationsstrukturen nötig. Üblicherweise wird ein Schichtenmodell zu Grunde gelegt, wobei die verschiedene Aufgaben jeweils verschiedenen Schichten (Layer) zugewiesen sind. Das sogenannte *OSI-Referenzmodell*, das grundsätzlich den Standard für eine derartige Kommunikationsarchitektur festschreibt, ist in 7 Schichten organisiert.

Die TCP/IP-Protokollfamilie ist nicht in allen Punkten OSI-konform und wird meist vereinfacht in einem 4-Schichten-Modell beschrieben. Die Daten einer Anwendung, die über das Netzwerk transportiert werden sollen, werden beginnend von der höchsten Schicht (*Application Layer*) mit Kontrollinformation (in einem *Header*) versehen an die darunterliegende Schicht weitergegeben. In dieser werden den Datenpaketen gemäß den in der Schicht beheimateten Protokollen weitere Kontrolldaten (in einem weiteren Header) vorangestellt und wiederum an die nächst tiefere Schicht weitergegeben; man spricht von *Encapsulation*: Am unteren Ende des *Stacks* (Stapels) befindet sich der

Network Access Layer, von dem aus die Daten auf das physikalische Netz weitergeleitet werden.
Die Datenpakete werden dann über das Netzwerk bis zum Empfängerhost geleitet und dort zunächst vom Network Access Layer empfangen. Dann werden sie „entpackt“ und an den darüberliegenden Layer weitergegeben, bis sie schließlich im Application Layer angekommen sind und an die entsprechende Anwendung weitergeleitet werden. Die vier Schichten des TCP/IP-Stacks sind auf Folie 152 dargestellt.

Organisationen und Standards

- IANA (Internet Assigned Number Authority): IP-Adr., Portnr.
- InterNIC: Registrierung von Domainnamen
- IAB (Internet Advisory Board): policy
- IETF (Internet Engineering Task Force)
- IRTF (Internet Research Task Force)
- RFCs (Requests for Comment): Festlegung der Standards, Dokumentation

Folie 151

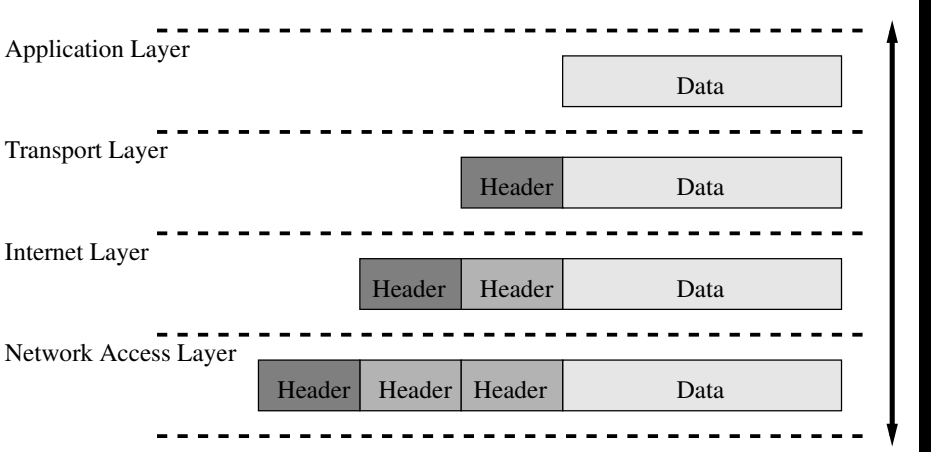
TCP/IP-Layer

Layer	Aufgabe	Protokolle
4. Application Layer	End-User Anw.	FTP, TELNET,...
3. Transport Layer	Host-to-Host Komm.	TCP, UDP,...
2. Internet Layer	Adressierung, Routing	IP, ICMP,...
1. Network Access L.	Zugang zum Netz	ETHERNET, ARP,...

OSI-Referenzmodell: 7 Schichten; TCP/IP: 4 Schichten

Folie 152

Encapsulation



Folie 153

13.2 TCP/IP-Layer

Wir besprechen nun die einzelnen Layer und die wichtigsten damit assoziierten Protokolle. Der **Network Access Layer** (NAL) ist als unterste Schicht im TCP/IP-Stack für den Zugriff auf das physikalische Netzwerk verantwortlich. Es ist der einzige Layer, der Informationen über die Details der Netzwerkhardware und die Art des Netzwerks (Ethernet, Token Ring, Serielle/Telefon-Leitung, etc.) benötigt. In der Unix-Implementation ist der NAL meist eine Kombination aus (Netzwerkkarten-) Treibersoftware und Software, die zB IP-Adressen auf Ethernet-Adressen umschreibt (ARP Protokoll, siehe Abschnitt 13.4). Die Datenpakete, die vom NAL auf das Netzwerk ausgehen, heißen *Fragments*.

Der **Internet Layer** (IL) bewerkstelligt die grundlegende Datenpaketzustellung. Das wichtigste Protokoll im IL, das Internet Protocol (IP), ist gleichzeitig das Herzstück des TCP/IP-Stacks. Alle Protokolle der anderen Schichten benutzten das IP zum Datentransport; alle ein- und ausgehenden Daten fließen durch das IP, unabhängig von ihrem Quell- bzw. Bestimmungsort.
Einige Aufgaben des IP sind die Definition des *Datagrams*, der Basisdatenübertragungseinheit im Internet sowie des Adressierungsschemas und das *Routen* der Datagrams. Auf den Folien 156 und 157 ist das IP Datagram Format und das Routen von Datagrams dargestellt.
Die ersten 5 (oder 6 je nach Festlegung im Internet Header Field (IHL)) 32-Bit Worte des *Datagrams* bilden den Header, danach folgen die Daten. Der Header enthält alle Informationen, um die Daten richtig transportieren zu können. Die *Destination Address* im 5. Wort ist eine 32-Bit-Nummer, die eindeutig Zielnetzwerk und Zielhost festlegt (zB 131.130.145.110, siehe 13.4). Befindet sich der Zielhost im lokalen Netzwerk (also im selben physikalischen Netzwerk wie der Source Host), so können die Daten direkt übertragen werden (mittels NAL und der Auflösung der IP-Adressen in Hardwareadressen). Befindet sich der Zielhost in einem anderen Netzwerk, so muss das entsprechende Datenpaket über ein oder mehrere Gateways/Router geleitet werden. (Gatway vs Router; die Terminologie ist hier nicht einheitlich. Manchmal wird Gateway als Bezeichnung für einen Host verwendet, der Daten zwischen verschiedenen Protokollen vermittelt; dann bezeichnet nur Router das, was wir hier Gateway nennen. Wir verwenden aber beide Begriffe synonym.)

Jeder Host „kennt“ (per Konfiguration) sein Gateway, das die Verbindung vom lokalen Netzwerk (Local Area Network, LAN) zum übergeordneten Netzwerk herstellt. Im Beispiel auf Folie 157 sollen Daten von Host 1 zum Host 2 übertragen werden. Host 1 sendet die Daten als Fragment über das lokale Token-Ring-Netzwerk an Gateway 1. Dessen NAL übernimmt das Fragment und leitet die Daten entpackt zum Datagram an den IL weiter. Dieser entscheidet dann (aufgrund seiner Konfiguration), wie das Paket weiter zu routen ist und sendet es an das entsprechende Gateway. Dieses kann entweder schon das für den Host 2 zuständige Gateway 2 sein (falls im selben physikalischen Netzwerk) oder ein dem Gateway 1 übergeordnetes Gateway. Nach möglicherweise vielen Zwischenschritten gelangt das Fragment schließlich zu Gateway 2. Dessen IL stellt dann (nach Entpacken des Fragments zum Datagram) fest, dass die Daten an Host 2 zu senden sind und schickt das entsprechende Frame über das lokale Ethernet an Host 2. Wichtige Tatsache ist, dass weder Host 1 noch Host 2 irgendeine Information über die Netzwerke jenseits ihrer Gateways benötigen (und auch nicht darüber verfügen).
In der Unix-Implementierung kann man mittels des Kommandos `traceroute host` die Route zum entsprechenden Host abfragen; es wird eine Liste der dabei verwendeten Gateways und der Laufzeit zwischen ihnen ausgegeben.

Wenn der IL ein Datagram erhält, das für den lokalen Host bestimmt ist, so wird dieses an den darüberliegenden Transport Layer weitergereicht, wobei es direkt an das entsprechende Protokoll im TL überstellt wird, das im 3. Wort des IP-Datagrams eingetragen ist.

Network Access Layer

- unterste Schicht im TCP/IP-Stack
- physikalischer Zugriff auf Netzwerk
- Kombination
  - Netzwerktreiber-Software
  - IP-MAC-Adressenauflösung (ARP-Protokoll)
- Daten aufs Netz als Fragments

Folie 154

Internet Layer

- grundlegende Datenzustellung
- wichtigstes Protokoll: Internet Protocol (IP)
  - definiert Datagram als Standard-Übertragsungseinheit
  - IP-Adressierungsschemas
  - Routen von Datagrams
- Internet Control Message Protocol (ICMP)

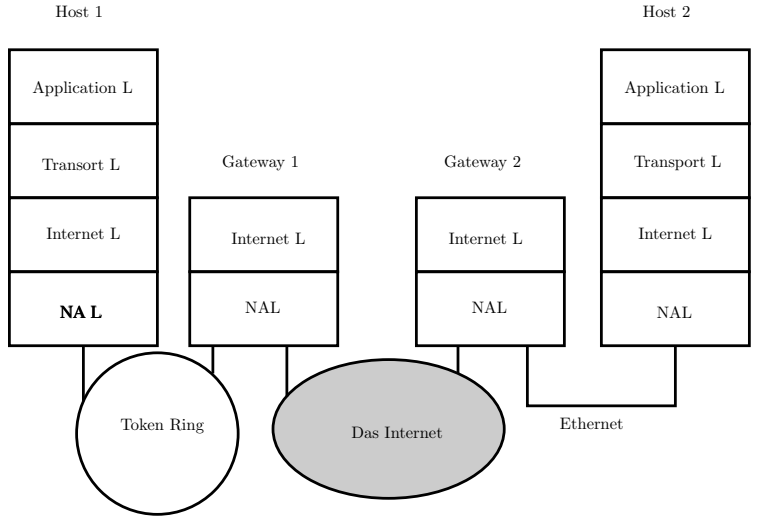
Folie 155

IP-Datagram

Wort	Bit 0	4	8	12	16	20	24	28 31	
1	Version	Header Length	TOS		Total Len.				Header
2	Identification				Flags	Fragment Offset			
3	TTL		Protocol		Header Checksum				
4	Source IP Address								
5	Destination IP Address								
(6)	(Possible Options)								
	Data ...								Data

Folie 156

Routing



Folie 157

Ein weiteres Protokoll innerhalb des IL ist das *Internet Control Message Protocol (ICMP)*. Es definiert die Standards für Flusskontrolle, Fehlermeldungen und wichtige Informationsfunktionen von TCP/IP. Ein wichtiger Teil von ICMP ist das Überprüfen der Erreichbarkeit von Hosts mittels einer *Echo Message*; dies wird zB vom `ping`-Kommando benutzt.

Der **(Host-to-Host) Transport Layer** (TL) liegt im TCP/IP-Stack über dem IL. Seine beiden wichtigsten Protokolle sind das *Transmission Control Protocol (TCP)* und das *User Datagram Protocol (UDP)*. TCP stellt eine verlässliche Datenübertragung mit Fehlererkennung und Korrektur zu Verfügung; UDP bietet eine einfache, nicht verbindungsorientierte, nicht verlässliche Paketübertragung mit wenig Overhead. Der Programmierer einer Anwendung kann – je nach Anforderungen – entscheiden, welches der Protokolle er verwendet. Sollen zB viele kleine Datenpakete übertragen werden, so ist der Aufwand mittels TCP mit seinem Kontroll-Overhead eine verlässliche Verbindung herzustellen größer, als einfach ein verlorenes Paket neu zu übermitteln, wie bei Übertragung mittles UDP-Protokolls vorgesehen.

UDP übernimmt vom Application Layer Daten in Form einer *Message* und verpackt sie zu einem *Packet*. Im ersten Wort des Headers stehen *Source* und *Destination Port*, die jeweils das Protokoll (resp. die Anwendung) im Application Layer definieren, dem die Message übergeben werden soll bzw. von dem sie herrührt. Das UDP Packet Format ist auf Folie 160 dargestellt. Generell können nur solche Anwendungen/Protokolle im AL UDP verwenden, die selbst für einen verlässlichen Datentransfer sorgen und nicht darauf angewiesen sind, die Verlässlichkeit mittels TL-Protokolls zu erzielen. Beispiele dafür ist das sogenannte *Query-Response*-Modell. Das Einlangen einer Antwort (Response) wird als Zeichen dafür gewertet, dass die Anfrage (Query) richtig übertragen wurde. Wird nach einer Timeout-Periode keine Antwort verzeichnet, so wird einfach die Anfrage erneut übertragen.

Im Unterschied zu UDP ist TCP ein *verlässliches, verbindungsorientiertes Byte-Stream-Protokoll*. Es übernimmt Daten aus dem AL in Form eines *Streams* und gibt diese als *Segment* an den IL weiter. Das TCP-Segment-Format ist schematisch auf Folie 161 dargestellt. Die Verlässlichkeit der Datenübertragung wird mittels eines *Positive Acknowledgement with Re-Transmission (PAR)* genannten Mechanismus hergestellt. Der Segment Header enthält eine Prüfsumme, die es dem Empfänger ermöglicht festzustellen, ob die Übertragung korrekt verlaufen ist. In diesem Falle schickt er ein *positives Acknowledgement* zurück an den Sender. Bleibt dieses nach einem Timeout aus, so überträgt der Sender das Segment erneut.
Die Verbindungsorientiertheit von TCP besteht darin, dass zu jeder Datenübertragung eine logische *End-to-End*-Verbindung aufgebaut wird. Diese wird durch einen sogenannten *Three-Way-Handshake* initialisiert, bei dem Sender und Empfänger Details des Kommunikationsablaufs festlegen (Synchronize Sequence Numbers (SYN-Flag gesetzt) und Acknowledgement (ACK-Flag gesetzt)). Jede Verbindung wird ebenfalls durch einen Three-Way-Handshake beendet (FIN). Im TCP werden die Daten innerhalb einer Verbindung nicht als individuelle Pakete angesehen, sondern als Datenstrom (Byte-Stream); dieser wird mittels *Sequence* und *Acknowledgement Number* kontrolliert. Mittels des *Acknowledgement Segments (ACK)* wird neben dem positiven Acknowledgement auch die Flusskontrolle durchgeführt. Die Kommunikationspartner teilen sich so mit, wie viel Daten sie im Moment noch aufnehmen können (Window Size). Analog zu UDP definieren Destination- und Source Portnummern im 1. Wort des TCP-Segments die jeweiligen Protokolle im AL für die Daten (Stream) übermittelt werden.

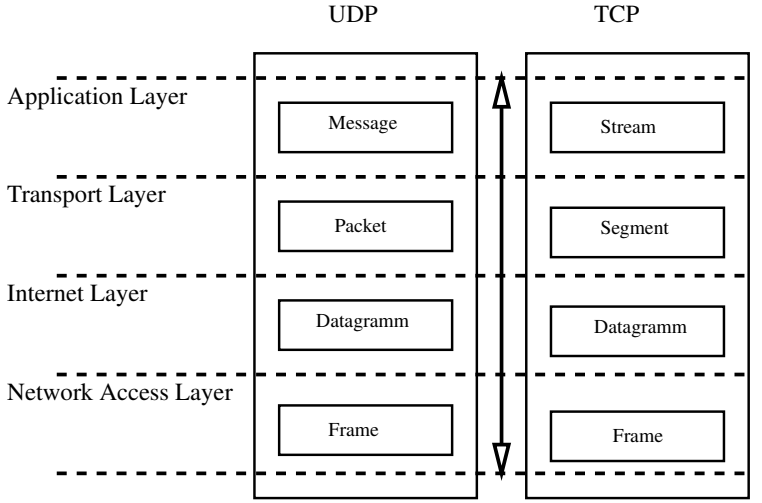
Der TL verfügt über weitere Protokolle, die in der Unix-Implementation von TCP/IP in der Datei `/etc/protocols` definiert sind. Eine Beispieldatei befindet sich auf Folie 162.

(Host-to-Host) Transport Layer

- Host-to-Host Kommunikation
- Transmission Control Protocol (TCP)
  - verbindungsorientiert, verlässlich
  - Fehlerkontrolle und -korrektur
  - Flusskontrolle
  - Format: Segment
- User Datagram Protocol (UDP)
  - nicht verbindungsorientiert
  - keine Fehlerkontrolle
  - wenig Overhead
  - Format: Packet
- Protokollnummern in `/etc/protocols` (TCP=6, UDP=17, ...)

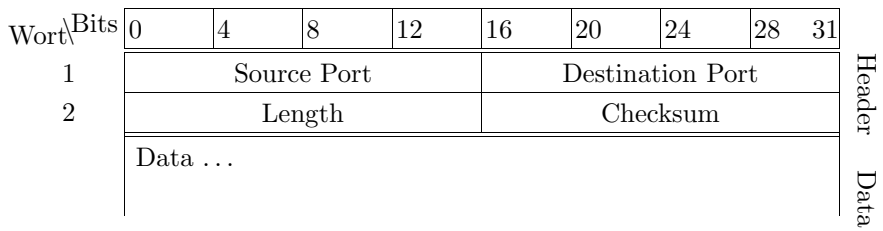
Folie 158

Datenformate



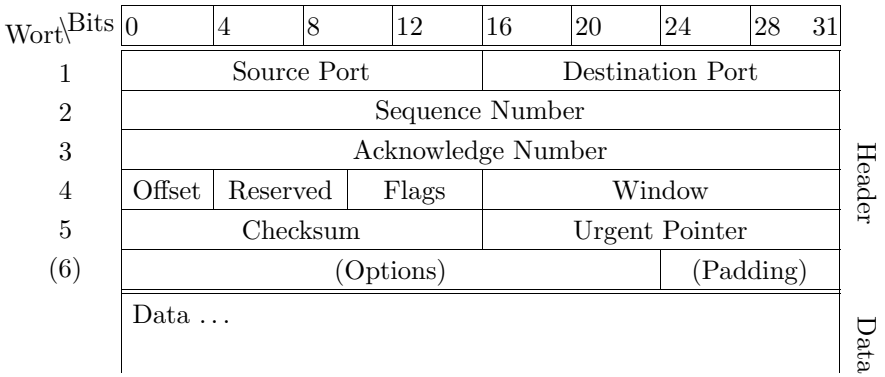
Folie 159

UDP-Packet



Folie 160

TCP-Segment



Folie 161

Protokolle im Transport Layer

```
bash# cat /etc/protocols
# /etc/protocols:
# Internet (IP) protocols
# from: @(#)protocols 5.1 (Berkeley) 4/17/89
ip   0  IP   # internet protocol, pseudo protocol nmb
icmp 1  ICMP # internet control message protocol
igmp 2  IGMP # Internet Group Management
tcp  6  TCP  # transmission control protocol
pup  12 PUP  # PARC universal packet protocol
udp  17 UDP  # user datagram protocol
hmp  20 HMP  # host monitoring protocol
ipip 94 IPIP # Yet Another IP encapsulation
ipip 94 IPIP # Yet Another IP encapsulation
```

Folie 162

Der **Application Layer** (AL) ist die oberste Schicht in unserem Modell und besteht aus einer Vielzahl verschiedener Protokolle, von denen die meisten bereits direkt User-Services, also Anwendungen sind. Neue Services werden laufend zum AL hinzugefügt. Wir bringen eine kurze Aufzählung der wichtigsten AL-Protokolle.

- TELNET (Network Terminal Protocol) Remote Login über ein Netzwerk, siehe Abschnitt 15.3
- FTP (File Transfer Protocol) Interaktiver Filetransfer, siehe Abschnitte 15.3 und 17.1
- SMTP (Simple Mail Transfer Protocol) E-Mail senden und empfangen, siehe Abschnitt 17.3
- SSH (Secure Shell) Sicherer Remote Login und Filetransfer, siehe Abschnitt 15.3
- POP3 (Post Office Protocol) E-Mail abholen
- IMAP2 (Interim Mail Access Protocol) E-Mail abholen
- PRINTER Netzwerkdrucker (lpd), vgl. Kapitel 7
- HTTP (Hyper Text Transfer Protocol), www, siehe Abschnitt 17.2
- NFS (Network File System), siehe Abschnitt 16.2
- NIS (Network Information System), siehe Abschnitt 16.3
- SUNRPC (Portmapper, Remote Procedure Call), siehe Abschnitt 16.1
- NETBIOS Windows Netzwerk Protokoll, siehe Kapitel 19
- DNS (Domain Name Service) Auflösen von IP-Adressen bzw. Hostnamen, siehe Abschnitt 13.4
- ...

Die Protokolle in AL werden vom TCP/IP-Stack aus über die *Portnummern* angesprochen. In der Unix-Implementation werden diese in der Datei `/etc/services` definiert. Diese Datei enthält neben den Portnummern auch Information darüber, welche TL-Protokolle von den entsprechenden Services verwendet werden. Eine Beispieldatei befindet sich auf Folie 164.

Application Layer

- oberste Schicht im TCP/IP-Stack
- End-User Applikationen
- Portnummern in `/etc/services`
  - 1-255: „well-known services“
    - TELNET
    - FTP
    - SMTP
    - POP
    - HTTP,...
  - 256-1024: „Unix specific services“
    - NFS
    - PRINTER
    - TALK, ...
  - 1024–: unprivilegierte Ports (dynamically allocated)

Folie 163

Ports und Services

```
bash# cat /etc/services:
tcpmux       1/tcp       # TCP port service multiplexer
echo         7/tcp
echo         7/udp
ftp-data    20/tcp
ftp         21/tcp
ssh         22/tcp       # SSH Remote Login Protocol
ssh         22/udp       # SSH Remote Login Protocol
telnet      23/tcp
# 24 - private
smtp        25/tcp  mail
# 26 - unassigned
time        37/tcp  timserver
```

Folie 164


```
www         80/tcp  http # WorldWideWeb HTTP
www         80/udp       # HyperText Transfer Protocol
# 100 - reserved
pop-3      110/tcp       # POP version 3
pop-3      110/udp
sunrpc     111/tcp portmapper # RPC 4.0 portmapper TCP
sunrpc     111/udp portmapper # RPC 4.0 portmapper UDP
netbios-ns 137/tcp            # NETBIOS Name Service
netbios-ns 137/udp
imap2      143/tcp imap  # Interim Mail Access Proto v2
imap2      143/udp imap
# UNIX specific services
syslog     514/udp
printer    515/tcp spooler# lpr spooler
talk       517/udp
```

Folie 165

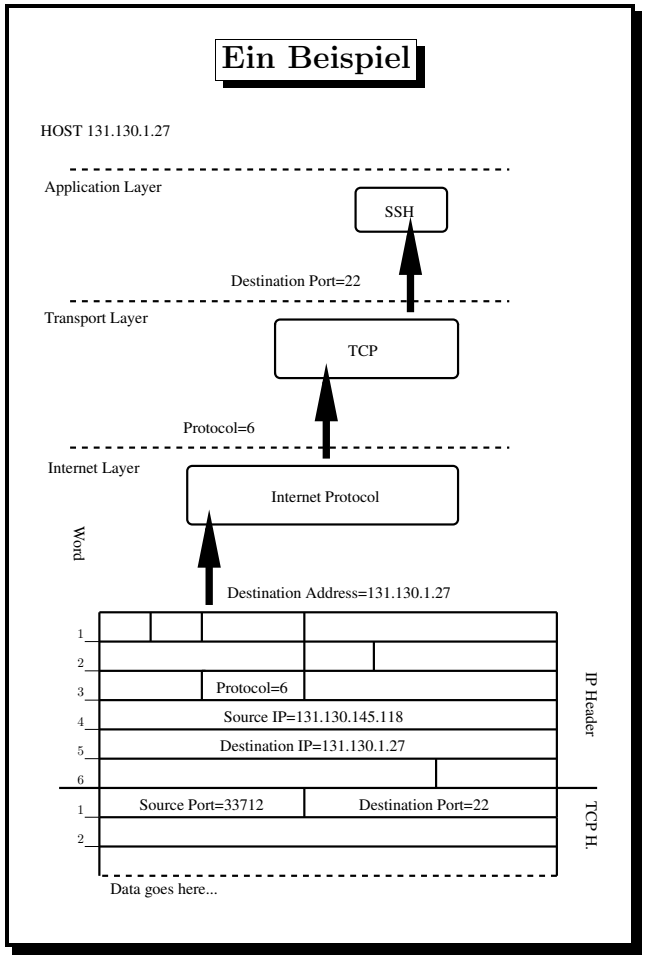
Die Ports 1–255 sind für „well-known services“ reserviert, die Ports von 256–1023 für „Unix specific services“. Der Name ist historisch; diese Services sind längst nicht mehr alle Unix-eigen und auch auf anderen Systemen implementiert. Die sogenannten unprivilegierten Ports ab 1024 werden als *„dynamically assigned ports“* (siehe Abschnitt 13.3) verwendet.

13.3 Protokolle, Ports und Sockets

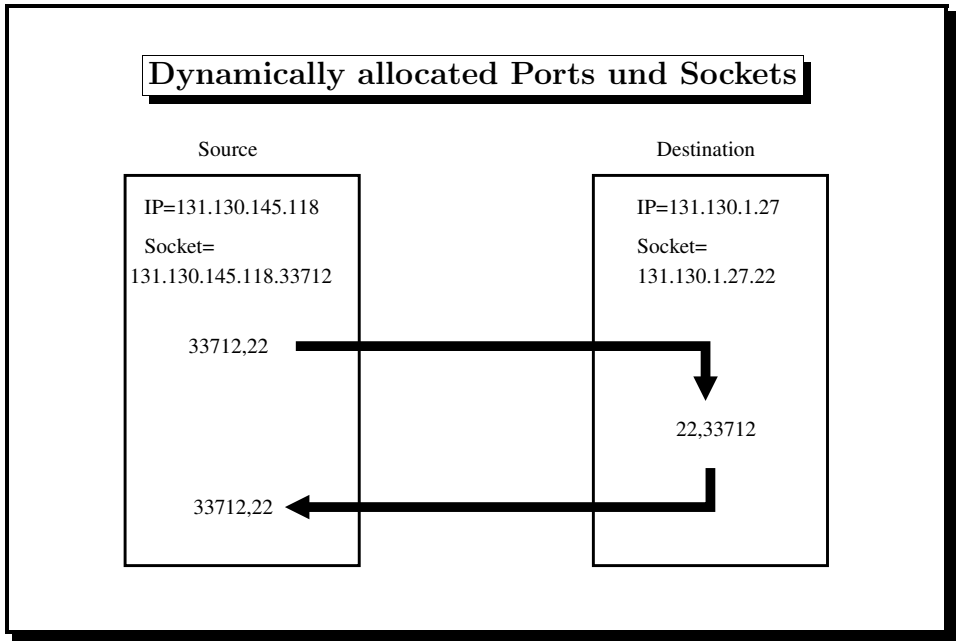
Nachdem wir nun im Überblick gesehen haben, wie der Transport von Daten im TCP/IP-Stack nicht nur zwischen Hosts, sondern auch zwischen den spezifischen Anwendungen auf den jeweiligen Hosts erfolgt, diskutieren wir als einfaches Beispiel eine Secure-Shell-Verbindung.

Angenommen ein Ethernet-Frame erreicht einen Host mit IP-Adresse 131.130.1.27, so wird es in dessen NAL in ein IP-Datagram verwandelt. Ist die Zieladresse (im 5. Wort des IP Headers, siehe Folie 156) tatsächlich 131.130.1.27, so wird das Datagram im IL weiter entpackt (sonst wird es geroutet, siehe oben). Anhand des Protokolleintrags (im 3. Wort des IP Headers) entscheidet der IL an welches Protokoll im TL die Daten zu überstellen sind. In unserem Beispiel (SSH, siehe Folie 166) wird das TCP-Protokoll (Protokollnummer 6, siehe `/etc/protocols`) verwendet (Es gibt zwar SSH-Varianten, die über UDP laufen; diese werden aber selten verwendet.) Daher leitet der IL die Daten als TCP-Segment entpackt an den TL weiter. Das TCP-Protokoll im TL liest die Destination Port Number (im 1. Wort des TCP Headers, siehe Folie) und stellt die Daten an das SSH-Service (Portnummer 22, siehe `/etc/services`) im AL zu.

Jetzt müssen wir allerdings noch den Mechanismus erklären, wie der Transport zwischen spezifischen Prozessen erfolgt. Das ist notwendig, um mehreren Benutzern die gleichzeitige Verwendung einer Anwendung (hier `ssh`) zu ermöglichen. Dazu konkretisieren wir unser Beispiel: Angenommen ein Benutzer 1 am Host 1 mit der IP-Adresse 131.130.145.118 möchte eine Secure Shell Session zum Benutzeraccount 2 am Host 2 mit der IP-Adresse 131.130.1.27 aufbauen. Nun kann es klarerweise nicht sein, dass die Datenübertragung zwischen den Hosts mit Source-Portnummer = Destination-Portnummer = 22 funktioniert, da sonst nicht zwischen einzelnen Prozessen resp. Benutzern unterschieden werden könnte. Daher wird dem `ssh`-Client des Benutzers 1 am Source Host (131.130.145.118) eine *„dynamically allocated Portnumber“* im nichtprivilegierten Bereich (größer 1024) zugewiesen, die für die gesamte folgende Kommunikation als Source Port Number verwendet wird; in unserem Beispiel 33712 (siehe Folie 166). Für die Kommunikation wird am Source Host also der Source Port 33712 und der Destination Port 22 verwendet. Umgekehrt verwendet der Destination Host 131.130.1.27 als Source Port 22 und als Destination Port 33712. Es ist dieser aus IP-Adresse und Portnummer gebildete *Socket*, der die Verbindung auf den beiden Seiten eindeutig definiert; auf Seite des Source Hosts wird der Socket 131.130.145.118.33712 verwendet, Destination-seitig 131.130.1.27.22. Beide Kommunikationspartner kennen die Portnummer des Destination Sockets (22), weil er für das „well-known Service“ SSH festgelegt ist (unter Unix in `/etc/services`). Ebenso kennen beide Hosts die Portnummer des Source Sockets (33712), da sie am Source Host dynamisch zugewiesen und im TCP-Segment dem Destination Host mitgeteilt wurde.



Folie 166



Folie 167

13.4 Adressierung

Zum Abschluss dieses Kapitels besprechen wir noch *IP-Adressen* und *Adressauflösung* in der TCP/IP-Protokollfamilie.
Im Internet Protokoll (IP) werden die Daten in Form von Datagrams bearbeitet. Jedes Datagram trägt im Header eine Source- (Wort 4) und eine Destination-IP-Adresse (Wort 5). Beide sind 32-Bit Wörter und identifizieren sowohl Netzwerk als auch Host von Source bzw. Destination.
Welcher Teil des 32-Bit-Worts das Netzwerk resp. den Host spezifiziert, ist von der *(Sub)Netzmaske* abhängig (vgl. Folien 169 und 170). In sogenannten *Klasse-A*-Netzwerken ist das erste Bit auf 0 gesetzt; die nächsten 7 Bits bilden den Netzwerkteil, die restlichen 24 den Hostteil. In *Klasse-B*-Netzwerken sind die ersten beiden Bits 1 0, die nächsten 14 Bits für Netzwerk- und die letzten 16 für den Hostteil reserviert. *Klasse-C*-Netzwerke werden durch die ersten Bits 1 1 0 bezeichnet; dann folgen 21 plus 4 Bits für Netzwerk- und Hostteil.
Schreibt man IP-Adressen in Dezimalzahlen an, so ergeben sich 4 Blöcke (jeweils 8 Byte) mit Einträgen zwischen 0 und 255. In dieser Schreibweise haben Klasse-A-Adressen den ersten Eintrag unter 128; es gibt also weniger als 128 Klasse-A-Netze, dafür können in jedem Millionen Hosts adressiert werden. Liegt der erste Eintrag zwischen 128 und 191, so handelt es sich um ein Klasse-B-Netz. Das erste und zweite Byte adressieren das Netzwerk, die letzten beiden Bytes den Host. Klasse-C-Netz haben den ersten Blockeintrag zwischen 192 und 223 (die Adressen darüber sind reserviert); die ersten drei Blocks bezeichnen das Netzwerk, der letzte den Host. In einem Klasse-C-Netzwerk können also nur 256 Hosts adressiert werden, dafür gibt es Millionen von Klasse-C-Netzwerken. Die Netzmasken für Klasse A, B bzw. C-Netzwerke sind respektive 255.0.0.0, 255.255.0.0, 255.255.255.0 (siehe auch Folie 170).

Da IP-Adressen eindeutig sein müssen, werden sie von der Organisation IANA (Internet Assigned Number Authority) bzw. für Subnetze von den jeweiligen Netzwerkadministratoren vergeben. In allen Netzwerkklassen sind die Hostadressen 0 und 255 reserviert. Eine IP-Adresse mit allen Hostnummern gleich 0 bezeichnet das gesamte Netzwerk (zB 26.0.0.0, das Klasse-A-Netz mit der Netzwerkadresse 26). Eine IP-Adresse mit allen Hostnummern auf 255 bezeichnet alle Hosts im Netzwerk und wird *Broadcastadresse* genannt (zB 131.130.145.255 ist die Broadcast-Adresse im Klasse-C-Netz 131.130.145.0). Gewisse IP-Adressen sind für private Netzwerke reserviert (die dann mittels Gatway an das Internet angeschlossen sind) und im Internet *nicht routbar* (zB 192.168.0.0 für private Klasse-B-Netze und 10.0.0.0 für private Klasse-A-Netzwerke).

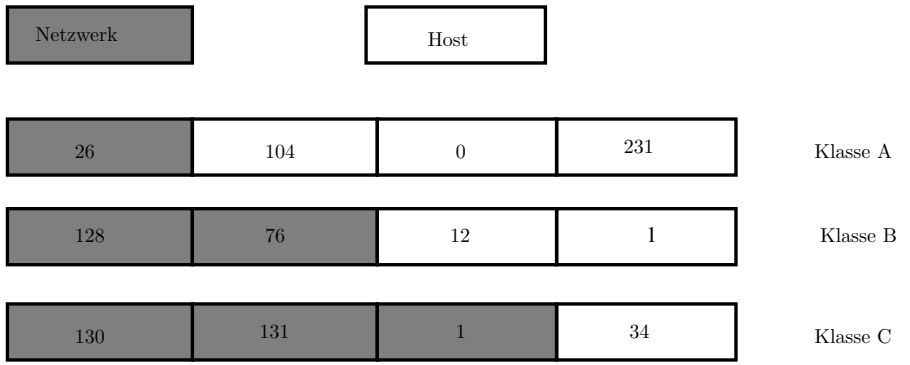
Am User-Ende der Kommunikation ist es natürlich unpraktisch, Hosts mit 32-Bit-Wörtern zu bezeichnen. Daher können Hosts auch mit sog. *Fully Qualified Domainnames (FQDN)* referenziert werden. Diese tragen dem Domänenkonzept im Internet Rechnung, das baumartig (ähnlich dem Unix-Verzeichnisbaum) organisiert ist. Die Organisation InterNIC (Network Information Center) vergibt Domainnamen an Organisationen, die dann berechtigt sind, Subdomänen zu vergeben (siehe `http://www.nic.at` oder `http://www.internic.at`).
FQDN wie zB `pablo.mat.univie.ac.at` beginnen mit dem spezifischen Teil, dem Hostnamen, hier `pablo`. Diesem folgen die Subdomänen `mat` (bezeichnet das Institut für Mathematik), `univie` (Universität Wien), `ac` (Academic) und schließlich die Top Level Domäne `at` (Austria). FQDN werden vom Domain Nameservice (DNS) in IP-Adressen aufgelöst bzw. umgekehrt. Jeder Host benötigt zur Auflösung von FQDN in IP-Adressen entweder Zugang zu einem Nameserver (der in der Konfiguration festgelegt ist; unter Unix in `/etc/resolv.conf`) und mittels DNS-Protokolls die Namensauflösung vermittelt oder eine lokale Referenztabelle (unter Unix `/etc/hosts`). Da die Verfügbarkeit des Nameservices ein kritischer Faktor für den gesamten Netzwerkverkehr ist (ohne dieses sind die Hosts am Netzwerk nur unter ihren IP-Adressen erreichbar, die natürlich die wenigsten Benutzer auswendig wissen), sind in `/etc/resolv.conf` mehrere Nameserver angegeben. Außerdem werden in dieser Datei Domänen definiert, in denen Hosts nur mit Hostnamen (ohne Domainnamen) angesprochen werden. Für den Fall, dass zB durch einen Fehler im übergeordneten Netzwerk kein Nameserver erreichbar ist, findet die Datei `/etc/hosts` Verwendung, die Namen und IP-Adressen der wichtigsten Hosts im LAN enthalten sollte (siehe auch Kapitel 14).

Adressen, Name Service

- Host-to-Host Kommunikation
  - User-End: FQDN, zB milkwood.mat.univie.ac.at
  - IL: IP-Adresse, zB 131.130.145.51
  - NAL: MAC-Adresse, zB 00:00:19:CE:C5:FB
- DNS, Nameserver, `/etc/hosts`: FQDN ↔ IP-Adresse
- ARP, RARP: IP-Adresse ↔ MAC Adresse

Folie 168

Klasse A B C Netzwerke (1)



Folie 169

Klasse A B C Netzwerke (2)

Klasse	(Sub)Netzmaske	Adressen
A	255.0.0.0	0.0.0.0–127.255.255.255
B	255.255.0.0	128.0.0.0–191.255.255.255
C	255.255.255.0	192.0.0.0–223.255.255.255
Multicast.	240.0.0.0	224.0.0.0–239.255.255.255

Folie 170

IP-Adressen

- 32-Bit-Wort
- dezimal vier 3er-Blöcke mit Eintragungen von 0 bis 255
- eindeutig vergeben von IANA
- Klasse A, B, C
- reservierte Adressen
  - Netzwerk = alle Hostbits 0: 193.130.145.0, 26.0.0.0
  - Broadcast = alle Hostbits 255: 193.130.145.255, 26.255.255.255
  - Private Netze: 10.0.0.0, 192.168.7.0

Folie 171

FQDN

- eindeutig vergeben von InterNIC
- Baumstruktur
- Subdomänenkonzept
- Format: hostname.subsub···subdomain.···.subdomain.domain
- Beispiel: durruti.mat.univie.ac.at

Folie 172

Am anderen Ende des TCP/IP-Stacks – im NAL – werden die IP-Adressen in Hardwareadressen umgewandelt (ARP, RARP). Jedes Netzwerkdevice (zB Ethernetkarte) verfügt über eine eindeutige, in der Hardware kodierte MAC-Adresse, zB 00:00:19:CE:C5:FB (12-stellige HEX-Nummer). Dem Host sind mittels ARP-Protokoll alle Hardwareadressen im LAN bekannt (`arp`-Kommando) und so können Frames direkt zugestellt werden. Soll ein IP-Datagram an einen Host gesendet werden, der sich nicht im lokalen Netz befindet, so wird es vom NAL in einen Frame an das Gateway verpackt und dort geroutet (siehe Folie 157). Jeder Host muss (mittels Konfiguration) alle *Routen* kennen. Typischerweise ist das die direkte Route zum lokalen Netz sowie die Gateway Route zu allen anderen Netzen. Die Routen können unter Unix mittels `route`-Kommandos angesehen bzw. modifiziert werden.

route, arp

```
bash-2.04$ /sbin/arp
Address                  HWtype  HWaddress           Iface
pan.cc.univie.ac.at      ether   00:50:53:87:B8:00   eth0
phobos.mat.univie.ac.at  ether   00:50:BF:10:F7:D8   eth0
golch.mat.univie.ac.at   ether   00:A0:24:59:35:D3   eth0
sirk.mat.univie.ac.at    ether   00:02:44:04:2B:9A   eth0

bash-2.04$ /sbin/route
Kernel IP routing table
Destination     Gateway         Genmask         Iface
127.0.0.0       *               255.0.0.0       lo
193.130.145.0   *               255.255.255.0   eth0
default         pan.cc.univie.a 0.0.0.0         eth0
```

Folie 173

14 Netzwerkkonfiguration

In diesem Kapitel erklären wir, wie unter Linux/Unix das TCP/IP-Protokoll, das Nameservice und Netzwerkinterfaces konfiguriert werden.

Bevor man überhaupt Internetanwendungen wie einen Browser oder ein Email-Programm verwenden kann, müssen die darunterliegenden Netzwerkeinstellungen vorgenommen werden. Leider ist viel dieser Konfigurationsarbeit je nach Linux-Distribution und Unix-Variante stark unterschiedlich, weshalb sich der Einsatz von graphischen Tools (zB `YaST` bei SuSE) besonders für Anfänger anbietet. Im Folgenden beschränken wir uns hauptsächlich auf die Netzwerkkonfiguration, wie sie sich unter RedHat-Linux darstellt und besprechen die einzelnen RedHat-spezifischen Konfigurationsdateien.
Grundsätzlich und auf jedem System gliedert sich die Netzwerkkonfiguration in einen Bereich, in dem Parameter für das TCP/IP-Protokoll gesetzt werden und in einen Bereich für jedes Netzwerkdevice, in dem nur die Parameter für das jeweilige Device gesetzt werden. Zum ersten Bereich gehören das Definieren des Hostnamens, des Domainnamens, des Gateways und das Konfigurieren des Nameservices (meist die Angabe eines oder mehrerer Nameserver). Der zweiten Bereich umfasst das Konfigurieren der IP-Adresse des Interfaces, sowie das Festlegen seiner Netzmaske, des Netzwerks, der Broadcastadresse und gewisser Steuerungsparameter (wer das Interface (de)aktivieren darf, wann es aktiviert wird etc.).

Es sei auch darauf hingewiesen, dass die Erläuterungen dieses Kapitel nicht komplett auf Modem-, ISDN- oder ähnliche Verbindungen zutreffen, wobei hier ebenfalls moderne (graphische) Konfigurationstools wie `kppp` einen Großteil der (distributionsspezifischen) Arbeit abnehmen. Für Details sei auf das Modem-HOWTO bzw. das DE-ISDN-HOWTO verwiesen. Auch ADSL- oder Telekabel-Verbindungen sind unter Linux gut unterstützt; es gibt dazu einige informelle HOWTOs im Internet, siehe zB das „Austrian Highspeed Internetconnection & Linux HOWTO“ unter `http://howto.htlw16.ac.at/at-highspeed-howto.html` oder die Webpage der „Telekabel Linux User Group (TKLUG)“

auf der Homepage der „Linux User Group Austria (LUGA)“ `http://www.luga.at`.

Ein besonderer Fall eines Netzwerkinterfaces ist das Loopback (`lo`)-Interface. Es wirkt wie eine virtuelle Netzwerkkarte mit der IP-Adresse `127.0.0.1` und (meistens) dem Hostnamen `localhost`. Alle Pakete, die vom lokalen Rechner an ihn selbst gehen, werden über das Loopback Device geschickt.

14.1 TCP/IP-Konfiguration

Der Großteil der TCP/IP-Konfiguration unter RedHat ist in der Datei `/etc/sysconfig/network` festgelegt. In diesem File definiert man ob überhaupt die Netzwerkfunktionen aktiviert werden sollen (was natürlich geschehen sollte (X Window System!) und daher defaultmäßig auf `YES` gesetzt ist). Weiters wird hier der Hostname (zB `auto.mat.univie.ac.at`) und das Standardgateway (das meist die IP-Adresse `a.b.c.1` oder `a.b.c.254` hat) für die Routingtabelle konfiguriert. Letztere wird beim Netzwerkstart automatisch aus den Informationen in den Konfigurationsdateien erstellt. Verfügt das System über mehr als ein Netzwerkgerät (das Loopbackinterface nicht mitgezählt), so muss das Gatewaydevice angegeben werden, also jenes Device, über das das Gateway erreichbar ist. Eine Beispieldatei befindet sich auf Folie 175.

Ein weiterer wichtige Punkt ist die Konfiguration des *Domain Name Services (DNS)*. Ist dieses nicht verfügbar, können Hostnamen nicht in IP-Adressen aufgelöst werden, was dem Administrator meist viele Useranfragen beschert, da dann nur mehr derjenige auf Netzwerkdienste bestimmter Hosts zugreifen kann, der ihre IP-Adresse kennt.

Netzwerkkonfiguration

- TCP/IP-Konfiguration: Hostname, Domainname, Gateway, Gatewaydevice, ...
  `/etc/sysconfig/network`
- DNS Konfiguration: Nameserver, Searchdomains, ...
  `/etc/resolv.conf, /etc/nsswitch.conf`
- Interfacekonfiguration: IP-Adresse, Netzwerk, Netzmaske, Broadcast, Funktionssteuerung, ...
  `/etc/sysconfig/network-scripts/ifcfg-device`

Folie 174

Es gibt einige Dateien und Dienste, die in einer bestimmten Reihenfolge durchsucht bzw. befragt werden, mit welcher IP-Adresse ein Hostname assoziiert ist. Je nach Einstellung der `hosts` Direktive in `/etc/nsswitch.conf` (bei früheren Linux-Distributionen und anderen Unix-Dialekten die `order` Direktive in `/etc/host.conf`) wird einerseits ein IP-Host(s)-Paar aus der Datei `/etc/hosts` ausgelesen, andererseits – was bei weitem die häufigere Methode darstellt Hostnamen aufzulösen – ein DNS-Server befragt. Welchen DNS-Server der Rechner kontaktieren soll, kann man in der Datei `/etc/resolv.conf` eintragen. Nach Möglichkeit sollte hier mehr als ein Server zu finden sein, damit bei einem Ausfall des ersten Servers der ungestörte Betrieb des Rechners gewährleistet bleibt. Eine komfortable Möglichkeit, Schreibarbeit zu sparen, stellt die `search` Direktive dar. Steht in `/etc/resolv.conf` etwa `search mat.univie.ac.at`, kann man einen beliebigen Rechner unter diesem Domainnamen erreichen, ohne die gesamte Domain mitanzugeben. Also statt `ssh sirk.mat.univie.ac.at` in diesem Fall nur `ssh sirk`. Auch mehrere `search` Direktiven sind zulässig.
Eine gute `/etc/hosts` sollte die wichtigsten IP-Adressen (zB `127.0. 0.1` für localhost, die eigene IP-Adresse, Adressen häufig benötigter Server, ...) enthalten, hauptsächlich aus Geschwindigkeitsgründen (Anfrage an den Server dauert länger als Auswerten einer Datei), aber auch, um im Falle eines totalen DNS-Ausfalls den Betrieb des Rechners möglichst weitgehend aufrecht zu erhalten.
Schließlich kann das DNS Service auch über das NIS Service bereitgestellt werden (siehe Kapitel 16).

TCP/IP-Konfiguration

```
$ cat /etc/sysconfig/network
 NETWORKING=yes
 FORWARD_IPV4=false
 HOSTNAME=milkwood.mat.univie.ac.at
 DOMAINNAME=mat.univie.ac.at
 GATEWAY=131.130.145.1
 GATEWAYDEV=eth0

$ grep hosts /etc/nsswitch.conf
 hosts:      files dns nis
```

Folie 175

/etc/hosts, /etc/resolv.conf

```
bash-2.04$ cat /etc/hosts
127.0.0.1       localhost.localdomain   localhost
131.130.145.118 soweto.mat.univie.ac.at soweto
131.130.145.101 phobos.mat.univie.ac.at phobos
131.130.14.151  erebus.mat.univie.ac.at erebus
131.130.87.22   banach.mat.univie.ac.at banach
131.130.14.152  radon.mat.univie.ac.at  radon

bash-2.04$ cat /etc/resolv.conf
search mat.univie.ac.at ap.univie.ac.at univie.ac.at
nameserver 131.130.1.11
nameserver 131.130.1.12
nameserver 131.130.11.3
```

Folie 176

14.2 Konfiguration der Netzwerkinterfaces

Gängige Netzwerkinterfaces für den LAN Betrieb sind Ethernetdevices (Bezeichnung `eth0, eth1,...`), oder (seltener) Token Ring Devices (`tr0,...`), für serielle Leitungen über Modems PPP-Interfaces (Point-to-Point Protokoll, `ppp0,...`), für parallele Verbindungen (heute sehr selten verwendet) gibt es PLIP-Interfaces.
Bevor ein Netzwerkinterface konfiguriert werden kann, muss sichergestellt sein, dass die Netzwerkhardware bzw. die Treiber richtig funktionieren. Meist werden modulare Treiber verwendet (siehe Kapitel 8). Wenn die Karte nicht bzw. nur durch einen Patch aktiviert werden kann, bietet es sich an, eventuell selbst einen Kernel zu compilieren.
Selbstverständlich können unter Unix mehrere Netzwerkdevices auf einem System betrieben werden zB ein Gateway (mit Firewallfunktion) mit zwei Ethernetkarten oder ein Gateway mit einer Ethernetkarte in einem privaten Netz und einer Modemverbindung (PPP Interface) zu einem Internetprovider.

Alle Dateien zur Interfacekonfiguration befinden sich unter RedHat in `/etc/sysconfig/network-scripts/`; die Konfiguration für ein Interface des Namens `device` ist in `/etc/sysconfig/network-scripts/ifconfig-device` festgelegt. Hier wird die IP-Adresse, die Netzmaske, das Netzwerk und die Broadcastadresse eingestellt. Weiters lässt sich in dieser Datei festlegen, ob das Interface bereits beim Booten oder später händisch gestartet werden soll. Bei Ethernetkarten wird man in den allermeisten Fällen `ONBOOT` auf `YES` setzen; bei PPP-Devices hingegen wird man eventuell mit `USERCTL=YES` allen Benutzern erlauben, das Interface zu (de)aktivieren.

Interfacekonfiguration

```
# cat ifcfg-eth0
 DEVICE=eth0
 IPADDR=131.130.145.112
 NETMASK=255.255.255.0
 NETWORK=193.130.145.0
 BROADCAST=193.130.145.255
 ONBOOT=yes

#cat ifcfg-ppp0
 DEVICE=ppp0
 USERCTL=yes
 DEFROUTE=yes
 ONBOOT=no
 INITSTRING=ATZ
 MODEMPORT=/dev/modem
 LINESPEED=115200
 ESCAPECHARS=no
 PAPNAME=steinbr5
```

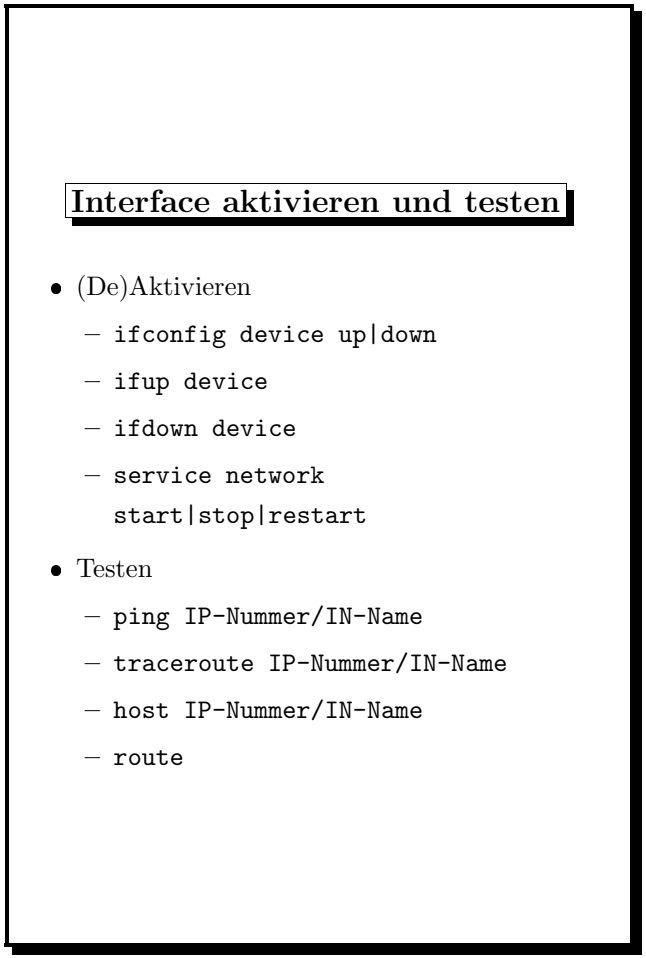
Folie 177

Es gibt auch die Möglichkeit, Netzwerkinterfaces automatisch mittels eines *Bootprotokolls* zu konfigurieren. Ein Beispiel dafür ist DHCP (Dynamic Host Configuration Protocol) ein Client-Server basierter Netzwerkdienst. Der Client sucht (mittels Broadcast) einen DHCP-Server im LAN; in der Antwort vom Server sind Daten wie IP-Adresse, Hostname oder zu verwendendes Gateway und Nameserver enthalten. Diese Form der Netzwerkkonfiguration bietet sich besonders bei internen größeren Netzen mit systemweiter Defaultkonfiguration an (zB PC-Labors). Um ein Interface mittels DHCP zu konfigurieren, muss in `ifcfg-device` der Eintrag `BOOTPROTO=DHCP` vorgenommen werden. Ein anderes Bootprotokoll zur automatischen Konfiguration von Netzwerkinterfaces ist das meist für sog. Diskless Clients verwendete BOOTP.

14.3 Aktivieren und Testen der Netzwerkinterfaces

Hat man die Konfigurationsarbeit vorgenommen, kann man nun darangehen, die Interfaces zu aktivieren und auf ihre Funktionstüchtigkeit zu testen. Der Befehl zur Aktivierung eines Interfaces, der unter beinahe allen Unix/Linux-Varianten verfügbar ist, ist `ifconfig`. Mit `ifconfig eth0 up|down` resp. `ifup eth0` oder `ifdown eth0` lässt sich ein Interface aktivieren bzw. deaktivieren. Gibt man `ifconfig` ohne Parameter ein, werden alle aktiven Interfaces aufgelistet. Hier sollte zumindest ein Eintrag für `lo` (Loopback) und ein weiteres Device aufscheinen, um von einer erfolgreichen Aktivierung des Netzwerkes ausgehen zu können.
Alle (`ONBOOT=YES`)-Interfaces können gleichzeitig mittels des entsprechenden Initscripts `/etc/init.d/network start|stop` (de)aktiviert werden; dabei wird im wesentlichen das `ifconfig`-Kommando mit den passenden Optionen und Argumenten ausgeführt und mittels `route` die Routen zu den verschiedenen Netzwerken gesetzt. Ein praktisch bedeutsames Detail ist, dass das Ändern der Netzwerkkonfiguration im laufenden Betrieb (aber heruntergefahrenem Device) erfolgen kann und kein Booten des Systems nötig ist.

Beim Testen überzeugt man sich zuerst davon, dass das Interface ordnungsgemäß geladen wurde (`ifconfig`) und dass die Routen richtig gesetzt sind (`route`). Danach kann man versuchsweise in folgender Reihenfolge IPs zu `ping`en beginnen (das `ping` Kommando dient – vereinfacht – dazu, die Kommunikation mit einem anderen Rechner durch ein Anfrage-Antwort-Verfahren mittels ICMP Protokoll zu testen, siehe Abschnitt 152); `localhost` (Loopback), eigene IP, Gateway, DNS Server und wenn das alles klappt, einen Rechner außerhalb des eigenen Subnetzes (etwa einen bekannten Webserver, der üblicherweise Pings akzeptiert). Durch diese Systematik kann man meist einfach erkennen, wo genau der Fehler liegt (sofern man Hardwareprobleme wie etwa ein nicht angestecktes Netzwerkkabel ausschließen kann).
Wenn Netzwerkpakete nicht an ihrem Zielort ankommen, die Verzögerung der Pakete sehr hoch ist oder man eine Fehlermeldung „No route to host“ erhält, ist es möglich, mittels `traceroute` den Weg eines Paketes vom eigenen Rechner über verschiedene Router zum Ziel zu verfolgen und dabei auch zu sehen, wie viel Zeit das Paket von einem „Hop“ zum nächsten benötigt.
Wenn alle vorherigen Schritte erfolgreich waren, man aber zB bei `ping www.orf.at` die Fehlermeldung „Unknown host www.orf.at“ zurückbekommt, funktioniert das Nameservice nicht richtig. Meist liegt es an der Nichterreichbarkeit eines DNS-Servers, was man leicht durch ein `ping` überprüfen kann. Tools zur Überprüfung der korrekten Funktionsweise (und manuellen *Verwendung*) des Nameservices sind `host` und `nslookup` (veraltet). Gibt man etwa `host www.mat.univie.ac.at` ein erhält man die dem Hostnamen assoziierte IP-Adresse (`131.130.14.152`). Das funktioniert auch umgekehrt und so liefert etwa `host 131.130.1.11` den Hostnamen `ns3.univie.ac.at` zurück.



Folie 178

ifconfig

```
[root@milkwood /root]# ifconfig
eth0 Link encap:Ethernet  HWaddr 00:90:27:54:80:3A
     inet addr:131.130.1.17 Bcast:131.130.145.255 Mask:255.255.255.0
     UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
     RX packets:41535881 errors:0 dropped:0 overruns:0 frame:0
     TX packets:6051210 errors:0 dropped:0 overruns:0 carrier:0
     collisions:0 txqueuelen:100
     Interrupt:9 Base address:0x1000

eth1 Link encap:Ethernet  HWaddr 00:00:21:DE:E2:A1
     inet addr:10.10.0.1  Bcast:10.10.0.255  Mask:255.255.255.0
     UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
     RX packets:6877430 errors:3 dropped:0 overruns:0 frame:0
     TX packets:4276200 errors:0 dropped:0 overruns:0 carrier:0
     collisions:0 txqueuelen:100
     Interrupt:10 Base address:0xfc00
```

Folie 179


```
lo   Link encap:Local Loopback
     inet addr:127.0.0.1  Mask:255.0.0.0
     UP LOOPBACK RUNNING  MTU:3924  Metric:1
     RX packets:64616 errors:0 dropped:0 overruns:0 frame:0
     TX packets:64616 errors:0 dropped:0 overruns:0 carrier:0
     collisions:0 txqueuelen:0
```

Folie 180

ping

```
[roli@pablo roli]$ ping 131.130.1.11
PING 131.130.1.11 (131.130.1.11) from 192.168.1.110
From 192.168.1.100: Destination Net Unreachable

[root@ken /root]# ping 131.130.1.11
connect: Network is unreachable

[root@ken /root]# ifup eth0
[root@ken /root]# !ping
PING 131.130.1.11 (131.130.1.11) from 62.178.139.47
64 bytes from 131.130.1.11: icmp_seq=0 ttl=249 time=19.606 msec
64 bytes from 131.130.1.11: icmp_seq=1 ttl=249 time=18.998 msec
```

Folie 181

traceroute, host

```
bash-2.04$ /usr/sbin/traceroute www.orf.at
traceroute to www.orf.at 30 hops max, 38 byte
 1  pan.cc.univie.ac.at  1.476 ms  0.956 ms 0.860 ms
 2  iris.cc.univie.ac.at   1.534 ms  1.363 ms 1.760 ms
 3  Vienna-RBS.aco.net   1.804 ms  1.520 ms 1.440 ms
 4  cvix1.apa.net   2.051 ms  1.880 ms  1.543 ms
 5  cvixatm1-l1.apa.net 3.263 ms 3.331 ms 3.445 ms
 6  apain1.apa.at 4.690 ms  5.641 ms  3.988 ms


bash-2.04$ host www.univie.ac.at
www.univie.ac.at. has address 131.130.1.78
bash-2.04$ host 131.130.14.152
152.14.130.131.in-addr.arpa. domain name pointer radon.mat.univie.ac.at.
```

Folie 182

15 Internetdienste und Internetdaemon

Dieses Kapitel beschäftigt sich mit „einfachen“ Netzwerkdiensten und ihrer Konfiguration. Insbesondere besprechen wir den Internetdaemon `(x)inetd`, einen Superserver, der viele der Daemonen, die einfache Netzwerkdienste vermitteln managt. Schließlich erwähnen wir kurz die TCP-Wrapper, die eine einfache Zugangskontrolle zu und damit eine einfache Sicherheitsvorkehrung für Netzwerkdienste ermöglichen.

Die allermeisten Netzwerkdienste sind als Client-Server-Applikationen konzipiert. Der Clientprozess (zB `ssh`) wird vom Benutzer am Clienthost gestartet und versucht eine Verbindung mit dem entsprechenden Serverprozess am Serverhost aufzubauen. Der Serverprozess (zB `sshd`, der Secure Shell Daemon) wird am Serverhost als Daemon meist beim Booten gestartet (Initscript) und läuft mit root-Privilegien oder unter einem eigenen Systemaccount. Er wartet am ihm zugewiesenen Port (hier 22; vgl. Kapitel 13) auf eingehende Anfragen von Clientprozessen von Remotehosts. Geht eine solche Anfrage ein, so wird gegebenenfalls eine Authentifizierung vorgenommen, Logeinträge geschrieben und die Verbindung eröffnet. Meist wird dazu ein weiterer Serverprozess gestartet, der dann nur diese Session managt und nach ihrem Ende ebenfalls beendet wird.

Einfache Netzwerkdienste

- Clientprozess am Clienthost vom Benutzer gestartet
- Serverprozess am Serverhost als Daemon
  - wartet auf eingehende Anfragen
  - root oder andere Privilegien
  - beim Booten gestartet
  - Authentifizierung, Logging
  - forkt und managt Session

Folie 183

15.1 Der Internetdaemon

Um nicht eine zu große Anzahl verschiedener Server laufen zu haben (Performance, Konfigurationschaos, ...) wird oft ein *Internetdaemon* genannter Superserver verwendet – `inetd` oder der neuere `xinetd` („x“ steht hier für e**x**tended und hat nichts mit X zu tun!). Dabei handelt es sich um einen Daemon, der eine Vielzahl von Ports auf eingehende Verbindungsanfragen überwacht und gegebenenfalls den zuständigen Serverdaemon startet.
Services resp. Daemonen die üblicherweise über den Internetdaemon gestartet werden sind `telnetd, ftpd, talkd,` die r-Dienste `rlogind, rshd,...`, `linuxconf-web` (vgl. Abschnitt 2.2) etc. Andere Services werden typischerweise als Standalone Server betrieben; Beispiele dafür sind Secure Shell Server `sshd`, Webserver `httpd`, Mailserver `sendmail,` NIS und NFS Daemonen (siehe Kapitel 16).

Als Internetdaemon wird entweder der `inetd` oder seine Erweiterung der `xinetd` verwendet, deren Konfiguration recht unterschiedlich ist. Der `inetd` wird in einem einzigen File (`/etc/inetd.conf`) konfiguriert, während der `xinetd` sowohl ein globales Konfigurationsfile (`/etc/xinetd.conf`), wie auch ein Konfigurationsfile pro verwalteten Dienst (`/etc/xinetd.d/service`) berücksichtigt. Da in modernen Distributionen hauptsächlich der `xinetd` verwendet wird, beschränken wir uns im Folgenden auf diesen; die Konfiguration ist auf den folgenden Folien erklärt. Weitere Details sind den Manpages `xinetd` und `xinetd.conf` bzw. der Seite `http://www.xinetd.org` zu entnehmen.

Der Internetdaemon

- Prinzipiell für jedes Internetservice ein Daemon
- Prinzipiell jeder bei Systemboot gestartet
- Vereinfachung `(x)inetd` (Internetdaemon)
  - kontrolliert telnetd, ftpd, rlogind,...
  - RedHat < 7.0 und SuSE < 7.3 verwenden einfacheren `inetd`
- trotzdem individuell – als Standalone Server – gestartet:
  sshd, httpd, Nfs, Nis, Samba,...

Folie 184

xinetd-Konfiguration

- Konfigurationsdateien `/etc/xinetd.conf` und `/etc/xinetd.d/*`
- für jeden Dienst (service) ist ein Eintrag der Form

```
service name
{
    option1 = value1 value2 ...
    option2 = value1 value2 ...
    ...
}
```

erforderlich, wobei `name` der Name des Dienstes ist (zB: ftp).
Außerdem gibt es die Möglichkeit eines Default-Eintrags.

Folie 185

/etc/xinetd.conf

```
# Simple configuration file for xinetd
# Some defaults, and include /etc/xinetd.d/

defaults
{
        instances       = 60
        log_type        = SYSLOG authpriv
        log_on_success  = HOST PID
        log_on_failure  = HOST
}

includedir /etc/xinetd.d
```

Folie 186

/etc/xinetd.d/telnet

```
# default: on
# description: The telnet server serves telnet
# sessions; it uses unencrypted username/password
# pairs for authentication.
service telnet
{
        flags           = REUSE
        socket_type     = stream
        wait            = no
        user            = root
        server          = /usr/sbin/in.telnetd
        log_on_failure  = USERID
}
```

Folie 187

xinetd und Security

- editieren von `/etc/xinetd.d/*`
  - nicht benötigte Dienste durch die Option `disable = yes` deaktivieren oder zugehöriges Paket deinstallieren
  - Zugang nur für bestimmte Hosts erlauben (siehe nächste Folie)
- `xinetd` neustarten
  - `service xinetd restart`

Folie 188

Zugangskontrolle für den `xinetd`

Folgende Optionen schränken den Zugriff auf einzelne Dienste ein:

- `only_from`: Erlaubt den Zugriff nur für aufgelistete Hosts. Mögliche Werte sind eine beliebige Kombination von (Auswahl)
  - Numerische IP-Adresse, zB: `131.130.14.152` oder Hostname (CNAME), zB: `radon.mat.univie.ac.at`
  - Domainame, zB: `.univie.ac.at`
  - Netzwerkname aus `/etc/networks`
  - Ein Netzwerkbereich der Form `address/netmask`
- `no_access`: Verbietet den Zugriff nur für aufgelistete Hosts. Mögliche Werte sind wie bei `only_from`.
- `access_times`: Erlaubt den Zugriff nur zu bestimmten Zeiten welche in der Form `hh:mm-hh:mm` angegeben werden

Folie 189

Ein typisches Beispiel

```
service ftp
{
        socket_type                = stream
        ...
        only_from       = .mat.univie.ac.at
        no_access       = evil.mat.univie.ac.at
        access_times    = 8:00-16:30
}
```

Diese Konfiguration erlaubt FTP-Verbindungen nur von Rechnern aus der Domäne `mat.univie.ac.at` außer dem Rechner `evil.mat.univie.ac.at` in den Zeiten von 8:00 bis 16:30.

Folie 190

15.2 TCP-Wrapper

Eine weitere, schon etwas ältere Methode den Zugang zu verschiedenen Netzwerkdiensten zu kontrollieren, ist die Verwendung der *TCP-Wrapper*. Diese können auf zwei Arten verwendet werden. Entweder ist der Daemon, der einen Dienst vermittelt mit TCP-Wrapper Unterstützung compiliert (zB: `sshd`, `sendmail`, ...) oder, falls er über keine interne Wrapper Unterstützung verfügt, kann diese extern über den TCP-Wrapper genannten `tcpd`-Daemon implementiert werden. In beiden Fällen werden die Dateien `/etc/hosts.deny` und `/etc/hosts.allow` ausgewertet (deren Syntax auf den Folien erklärt wird) und die darin festgelegten Regeln für den Zugang für die verschiedenen Diensten befolgt.

Für einen Server ohne interne Wrapper Unterstützung kann diese auf folgendem Wege implementiert werden. Der Internetdaemon wird so konfiguriert, dass er bei Anfragen an den entsprechenden Port den `tcpd`-Daemon startet. Dieser übernimmt die Überprüfung der Zugriffsberechtigungen gemäß `/etc/hosts.deny|allow` und startet bei positivem Ausgang den Daemon, der eigentlich den Dienst vermittelt. Diese Vorgangsweise ist beim `xinetd` nicht besonders sinnvoll, da dieser eine interne Zugangskontrolle bereitstellt (siehe oben), ist aber die gängigste Möglichkeit Zugangsbeschränkungen mittels des älteren `inetd` zu realisieren. Beispielkonfigurationen für beide Internetdaemonen finden sich auf den Folien.

TCP-Wrapper

- Zugangsbeschränkung für bestimmte Dienste die mit TCP-Wrapper Support übersetzt wurden (zB `sshd`, `sendmail`)
- Zugangsbeschränkung für Dienste ohne internen TCP-Wrapper Support über `tcpd`
- Konfiguration
  - Service-, Benutzer- und Host-spezifisch
  - `/etc/hosts.allow` (stärker)
  - `/etc/hosts.deny`
- Loggen der Anfragen über `syslogd`
  - `/var/log/messages`
  - `/var/log/secure`

Folie 191

TCP-Wrapper-Konfiguration

- `/etc/hosts.allow(deny)`-Syntax
  - `daemon_list : client_list [ : shell_command ]`
  - `daemon_list : ... user_pattern@host_pattern ...`
- Konfiguration testen mit
  - `tcpdmatch daemon[@host] [user@]host`
  - `tcpdchk`

Folie 192

/etc/hosts.deny

```
bash# cat etc/hosts.deny
#
# hosts.deny    This file describes the names of the hosts
#               which are *not* allowed to use the local
#               INET services, as decided by the
#               '/usr/sbin/tcpd' server.
#

ALL: ALL@ALL : spawn ( /usr/local/sbin/secrep %h %d | \
/bin/mail -s ALKO_secrep_%d roland.steinbauer@univie.ac.at )
```

Folie 193

/etc/hosts.allow

```
[stein@doppler stein]# cat /etc/hosts.allow
#ALL: 131.130.26., 131.130.87., 131.130.11., 131.130.1.26
#      5. stock     akh          ap            mailbox

ALL: 131.130.26., 131.130.87.67, 131.130.87.94,\
   131.130.87.91, 131.130.87.95, 131.130.87.93

in.talkd: 136.142.123.77, 131.130.26.130, 131.130.87.
#           saschas raven.phyast.pitt.edu

sshd2, sshd1, sshd, sshdfwd-X11: ALL EXCEPT .com,\
      .mil, .net, .org, 131.130.38.,  131.130.44.,\
       131.130.39., a-sa7-42.tin.it, \
```

Folie 194

xinetd und TCP-Wrapper

```
$ cat /etc/xinetd.d/telnet

service telnet
{
        flags       = REUSE NAMEINARGS
        protocol    = tcp
        socket_type = stream
        wait        = no
        user        = telnetd
        server      = /usr/sbin/tcpd
        server_args = /usr/sbin/in.telnetd
}
```

Folie 195

inetd und TCP-Wrapper

```
root@dukana# cat /etc/inetd.conf
# inetd.conf
# Echo, discard, daytime, and chargen are used
# primarily for testing.
echo    dgram   udp  wait    root  internal
discard stream  tcp  nowait  root  internal
discard dgram   udp  wait    root  internal
#
# These are standard services.
#
ftp    stream tcp nowait root /usr/sbin/tcpd in.ftpd -l -a
telnet stream tcp nowait root /usr/sbin/tcpd in.telnetd
```

Folie 196

Ein typisches Szenario

```
[root@mut /root]# cat /etc/hosts.deny
ALL:ALL
[root@mut /root]# cat /etc/hosts.allow
[root@mut /root]#
    [dylan@milkwood /home/dylan]# telnet mut
    Trying 192.168.0.129...
    Connected to mut.
    Escape character is '^]'.
    Connection closed by foreign host.
    [dylan@milkwood /home/dylan]#
[root@mut /root]# tail -1 /var/log/secure
Mar 29 20:37:15 localhost in.telnetd[1866]: refused
                connect from 192.168.0.1
```

Folie 197

15.3 Einfache Internetdienste

Zum Schluss dieses Kapitels behandeln wir die Internetdienste Telnet, Ftp, die r-Dienste sowie deren „sicheren“ Ersatz die Secure Shell `ssh`.

TELNET ist ein Protokoll im Application Layer der TCP/IP-Protokollfamilie (vgl. Kapitel 13) und dient zum Login auf einem Host über das Netzwerk. Serverseitig – also auf dem Host, auf den man sich übers Netz einloggen will – muss ein Telnetserver laufen; dieser heißt meist `telnetd` oder `in.telnetd` und wird fast immer vom Internetdaemon gestartet. Der Client heißt `telnet`, die Syntax ist `telnet hostname`. Der Loginname wird interaktiv abgefragt; für Details zur Syntax und auch den interaktiven Modus siehe die Manpage bzw. Folie 198.

FTP ist ebenfalls ein Application-Layer-Protokoll und dient dem Transfer von Dateien über ein Netzwerk; FTP steht für File Transfer Protokoll. Unter Linux stehen mehrere Ftp-Server-Pakete zu Verfügung (siehe Abschnitt 17.1), die teilweise über den Internetdaemon oder als Standalone Server betrieben werde. Es existiert eine Vielzahl von Client-Programmen. Unter ihnen das auf jedem System vorhandene, doch recht krude `ftp` und meist auch das komfortable `ncftp`. Letzteres stellt eine Commandline Completion und einen automatischen Anonymen Login zur Verfügung. Anonymes Ftp wird vorallem von großen Ftp-Servern im Internet angeboten, die so den anonymen Download von Daten erlauben. Ist man per Ftp eingeloggt, so können mittels des Kommandos `get remotefile` Dateien herunterladen bzw. mittels `put localfile` upgeloaded werden (falls das vom Server erlaubt wird). Für die Syntax siehe auch Folien 199 - 201 bzw. die Manpages.

Die *r-Dienste* sind eine Familie (älterer) Unix Services, die ein Remotelogin `rlogin, rsh`, Remotecopy `rcp` (in der Syntax ähnlich dem gewöhnlichen `cp`) und Remote Commandexecution `rexec` bereitstellen. Die Server werden über den Internetdaemon gestartet, für die Syntax der Clients siehe die Folie 202 und die Manpages. Da die Authentifizierung sehr unsicher ist (jeder Benutzer kann zB im File `~/.rhosts` Host/Usernamen-Paare angeben, um diesen ein Benutzen der Services *ohne* Passwortabfrage zu ermöglichen!!!) werden diese Services aber kaum noch benutzt.

Telnet

```
[roli@pablo roli]$ telnet merlin.ap.univie.ac.at
Trying 131.130.11.52...
Connected to merlin.ap.univie.ac.at.
Escape character is '^]'.

Compaq Tru64 UNIX V5.1 (Rev. 732) (balin.ap.univie.ac.at) (pts/6)

login: steinbau
Password:

Willkommen auf MERLIN     Mixed Architecture Unix Cluster MERLIN
Aussenstelle Physik             Vienna University Computer Center

You have mail.
--- Diskusage: 56%. ---

bash-2.03$
```

Folie 198

Ftp

```
[roli@pablo roli]$ ftp radon
Connected to radon (131.130.14.152).
220 ProFTPD 1.2.2 Server (Department of Mathematics) [radon.mat.univie.ac.at]
Name (radon:roli): anonymous
331 Anonymous login ok, send your complete email address as your password.
Password:
230 Anonymous access granted, restrictions apply.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
227 Entering Passive Mode (131,130,14,152,9,14).
150 Opening ASCII mode data connection for file list
drwxr-sr-x   5 root     ftp          4096 Nov 11 10:53 pub
drwxrwsrwx   2 martin   ftp          4096 Mar 31 20:54 ttt
226 Transfer complete.
```

Folie 199


```
ftp> get mutt_1.3.25-1.dsc
local: mutt_1.3.25-1.dsc remote: mutt_1.3.25-1.dsc
227 Entering Passive Mode (131,130,14,152,9,22).
150 Opening BINARY mode data connection for mutt_1.3.25-1.dsc (665 bytes).
226 Transfer complete.
665 bytes received in 0.00709 secs (92 Kbytes/sec)
ftp> help
Commands may be abbreviated.  Commands are:
!               debug           mdir            sendport        site
$               dir             mget            put             size
account         disconnect      mkdir           pwd             status
append          exit            mls             quit            struct
ascii           form            mode            quote           system
bell            get             modtime         recv            sunique
binary          glob            mput            reget           tenex
[...]
ftp> quit
[roli@pablo roli]$
```

Folie 200

NcFtp

```
[roli@pablo roli]$ ncftp ftp.univie.ac.at
NcFTP 3.0.3 (April 15, 2001) by Mike Gleason (ncftp@ncftp.com).
Connecting to ftp.univie.ac.at...

                    Welcome to FTP.UNIVIE.AC.AT
                    ===========================
   you are user #46 of 500 simultaneous users allowed.
Anonymous access granted, restrictions apply.
Logged in to ftp.univie.ac.at.
ncftp / > get systems/linux/distributions/mandrake/iso/README
README:                                    2.00 kB   23.18 kB/s
ncftp / > quit
[roli@pablo roli]$
```

Folie 201

Die r-Kommandos

- `in.rlogind`
- benutzerfreundlich, Unix-Standard
  - `rlogin`... analog `telnet`
  - `rsh`... remote Commandexecution
  - `rcp`... Filetransfer, Syntax ähnlich `cp`
- können Passwortauthentifizierung umgehen!
  - `/etc/hosts.equiv` (zuerst gelesen)
  - `~/.rhosts` (per-User Konfiguration)
  - `/.rhosts` (root-Zugang)
  - `/.rhosts`-Syntax: [+|-] hostname username

Folie 202

Telnet Ftp und die r-Services haben ein großes Sicherheitsmanko; sie versenden Klartextpasswörter über das Netz. Gelingt es einem Angreifer (etwa mit einem Portsniffer; siehe Kapitel 18) die Kommunikation „zu belauschen“, so kann er auf einfache Weise Username/Passwort-Paare in Erfahrung bringen.
Einen sicheren Ersatz stellt die *Secure Shell* zur Verfügung. Das Secure-Shell-Protokoll ist ebenfalls ein Application-Layer-Protokoll; sein User-End ist dem von Telnet und Ftp sehr ähnlich. Der große Unterschied besteht darin, dass die gesamte Session verschlüsselt über das Netzwerk übertragen wird. Die Basissyntax ist auf Folie 203 erklärt. Die Konfiguration des (fast immer als Standalone Server betriebenen) Secure Shell Servers erfolgt in der Datei `/etc/ssh/sshd_config`. In den meisten Linux-Distributionen ist der `sshd` mit TCP-Wrapper Unterstützung compiliert, dh. liest die Konfiguration in `/etc/hosts.allow|deny`. Die Secure Shell kennt zwei Protokollvarianten, Version 1 und Version 2; beide bieten die Möglichkeit einer *schlüsselbasierten Authentifizierung* und die Möglichkeit mittels des Authentication Agents (`ssh-agent`) Keys zu verwalten. Mit `ssh-keygen` generiert der Benutzer ein Public/Private Key-Paar, das durch eine Passphrase geschützt ist. Der Private Key liegt in `~/.ssh/` und muss geheim gehalten werden (Mode 400), der Public Key muss auf den Remotehost in die Datei `~/.ssh/authorized_keys` kopiert werden. Auf dem lokalen Rechner muss der `ssh-agent` laufen. Zweckmäßigerweise wird oft die gesamte X-Session vom `ssh-agent` aus gestartet (zB mittels Eintrag `/usr/sbin/ssh-agent /usr/bin/startkde` in `~/.xsession`). Sonst kann zB auch eine Shell vom Agent aus gestartet werden (Eingabe: `ssh-agent bash`). Läuft der Agent so muss mittels `ssh-add` der Private Key geladen werden, wobei die Passphrase abgefragt wird. Jede Secure Shell Verbindung zum Remotehost wird jetzt über das Public/Private-Key-Paar statt das Passwort authentifiziert. Insbesondere und praktisch relevant muss nur einmal (pro lokaler Session) die Passphrase eingegeben werden, alle `ssh`-basierten Verbindungen (auch `scp`, `sftp`) erfolgen nun ohne weitere Notwendigkeit einer interaktiven Authentifizierung.
Für Details (insbesondere die genauen Dateinamen für die verschiedenen Protokoll und Key-Versionen) siehe Folie 204 und die entsprechenden Manpages.

Zusammengefasst verwendet der sicherheitsbewusste Benutzer `ssh` statt Telnet und `sftp` bzw. `scp` statt Ftp und `rcp`; Ftp sollte nur für anonymen Filetransfer verwendet werden. Der sicherheitsbewusste Administartor verzichtet auf die r-Dienste, den Telnetserver und den nichtanonymen Ftp-Server.

Secure Shell

- Syntax
  - Remote Login: `ssh user@host` oder `ssh -l user host`
  - Filetransfer: `scp user@host:sourcefile destinationfile` oder `scp sourcefile user@host:destinationfile`
  - Filetransfer interaktiv: `sftp user@host`
- Konfiguration
  - Client: `/etc/ssh/ssh_config`, `~/.ssh/`
  - Server: `/etc/ssh/sshd_config`

Folie 203

ssh-Keys

- erstellen: `ssh-keygen` Public/Private Key-Paar mit Passphrase
- Private Key: in `~/.ssh/` am lokalen Host, geheim (Mode 400)
- Public Key: in `~/.ssh/authorized_keys` am Remote Host
- Agent: `ssh-agent command` (zB `startkde, bash`)
- Key laden: `ssh-add` Passphrase wird abgefragt
- alle `ssh`-Verbindungen über Keys authentifiziert

Folie 204

16 NFS und NIS

In diesem Kapitel besprechen wir zwei prominenten Netzwerkdienste, die auf RPC (Remote Procedure Call) aufbauen. Das Network File System (NFS) erlaubt es Dateisysteme über ein Netzwerk zu verteilen; ein Fileserver stellt seine Dateisysteme über das Netz den Clienthosts zur Verfügung. Das „Administrative Database System" NIS (Network Information Service) erlaubt es spezielle Systemdateien wiederum von einem Server über ein Netzwerk an Clienthosts zu übertragen.

16.1 Remote Procedure Call (RPC)

Das *Remote Procedure Call (RPC)*-Protokoll von Sun definiert einen systemunahbängigen Standard für die Kommunikation von Prozessen über ein Netzwerk. Es besteht aus einer Bibliothek, die es Programmen ermöglicht Procedure Calls an entfernte Hosts in einem Netzwerk zu senden. Der Client sendet einen RPC Call an den Server, der eigene Routinen benutzt um die angefragten Operationen auszuführen und schließlich eine Antwort zurück an den Client sendet.

RPC stellt eine weitere Abstraktionsebene über den Application-Layer-Protokollen des TCP/IP-Stacks dar. Um RPC-Protokolle verwenden zu können muss ein eigener Server – der *RPC-Portmapper* meist `portmap` oder `rpcbind` genannt – am System laufen. Startet ein RPC-Server, so teilt er dem Portmapper mit, welche Services – geregelt über die sog. RPC-Servicenummern (analog zu den TCP/IP-Ports) – er anbietet und auf welchen Ports er kontaktiert werden kann. Ein RPC-Client nimmt immer zunächst Verbindung mit dem Portmapper auf, um herauszufinden, wie (d.h. auf welchem Port) er den Server – sprich ein Service bezeichnet durch eine RPC-Servicenummer – kontaktieren kann.
Mit dem Kommando `rpcinfo` kann man abfragen welche RPC-Services ein Host anbietet; siehe dazu Folie 206 bzw. die Manpage.

RPC bringt also eine zusätzliche Protokollebene mit sich. Der Vorteil besteht darin dass RPC-Protokolle unabhängig vom TL-Protokoll funktionieren und so sowohl UDP als auch TCP verwenden können.

Remote Procedure Call (RPC)

- von Sun Microsystems entwickelt
- systemunabhängiges Protokoll für Prozesskommunikation übers Netz
- ermöglicht Programmen Procedure Calls auf entfernten Hosts
- zusätzliche Abstraktionsebene über TCP/IP AL-Protokollen
- Services definiert über RPC-Servicenummern (analog Portnummern)
- benötigt eigenen Dienst: RPC-Portmapper (`portmap`)
  - RPC-Server registriert sich beim Start beim Portmapper
  - Portmapper verbindet RPC-Servicenummern mit TCP- bzw. UDP-Ports
  - RPC-Client kontaktiert zuerst Portmapper

Folie 205

rpcinfo

```
[roli@pablo roli]$ /usr/sbin/rpcinfo -p ken
   program vers proto   port
    100000    2   tcp    111  portmapper
    100000    2   udp    111  portmapper
    100004    2   udp    960  ypserv
    100004    1   udp    960  ypserv
    100004    2   tcp    963  ypserv
    100004    1   tcp    963  ypserv
    100007    2   udp    980  ypbind
    100007    1   udp    980  ypbind
    100007    2   tcp    983  ypbind
    100007    1   tcp    983  ypbind
    100011    1   udp    691  rquotad
    100011    2   udp    691  rquotad
    100011    1   tcp    694  rquotad
    100011    2   tcp    694  rquotad
    100005    1   udp  32769  mountd
    100005    1   tcp  32769  mountd
    100005    2   udp  32769  mountd
    100005    2   tcp  32769  mountd
    100005    3   udp  32769  mountd
    100005    3   tcp  32769  mountd
    100003    2   udp   2049  nfs
    100003    3   udp   2049  nfs
    100009    1   udp    729  yppasswdd
[roli@pablo roli]$
```

Folie 206

16.2 Network File System (NFS)

Das Network File System ist wahrscheinlich der prominenteste Netzwerkdienst, der RPC verwendet. Ursprünglich 1986 von Sun entwickelt, verbreitete es sich rasch auf alle gängigen Unix-Varianten, da die Protokollspezifikationen von Anfang an frei verfügbar waren. Es wurden auch einige Versuche unternommen, NFS auf anderen Betriebssystemen zu verbreiten (zum Beispiel MS-DOS). Als Standard hielt es sich allerdings nur in der Unix-Welt.
Das NFS-Protokoll hat sich über die Jahre hinweg als äußerst stabil erwiesen. Die erste veröffentlichte Version war Version 2, einige Verbesserungen wurden Anfang der 90er Jahre in die Version 3 implementiert, die aber völlig rückwärtskompatibel ist. Im Februar 2000 schließlich hat Sun die gesamten Quellen unter einer GPL-ähnlichen Lizenz freigegeben.

Einfach gesprochen ermöglicht NFS das Mounten von Dateisystemen über ein Netzwerk. Ein NFS-Client kann ein Dateisystem eines NFS-Servers wie ein lokales Dateisystem mounten (vgl. Abschnitt 8.1). Da (normalerweise) nur root Mounts vornehmen kann, ist unter NFS – anders als in der Windows-Welt (siehe auch Kapitel 19), wo jeder Benutzer Netzwerklaufwerke verbinden kann – das Einrichten von Netzwerkverzeichnissen dem Administrator vorbehalten und wird meist mit einer geeigneten Automatisierung des `mount`-Kommandos (`automount`, `amd`) erledigt.

NFS ist *transparent*, d.h. man kann auf Daten des Servers genauso zugreifen, wie auf lokale Dateien. Das zu Grunde liegende Dateisystem ist dabei nicht von Bedeutung. Das System ist zustandsunabhängig (*stateless*), d.h. der Server speichert keine Zustandsinformationen über die angebundenen Clients. Ist die Netzwerkverbindung unterbrochen, so zieht das den Server überhaupt nicht in Mitleidenschaft (den Client natürlich schon).

NFS besteht aus mehreren Komponenten, darunter ein Mountprotokoll und ein Mountserver `rpc.mountd`, Dämonen, die das Dateiservice selbst vermitteln (`nfs` und andere) und einige Diagnoseprogramme. Ein Großteil dieser sowohl server- als auch clientseitigen Software ist Teil des Kernels und benötigen keinerlei Konfiguration. Allerdings muss man bevor NFS überhaupt verwendet werden kann – sei es als Client oder Server – sicherstellen, dass der NFS-Support im Kernel eincompiliert ist. Das überprüft frau am einfachsten mittels `cat /proc/filesystems`. Erscheint `nfs` in dieser Liste, ist alles in Ordnung. Andernfalls muss man eventuell das entsprechende Modul laden oder den Kernel neu compilieren.

Darüberhinaus ist clientseitig nur die Konfiguration und gegebenenfalls eine geeignete Automatisierung der NFS-Mounts nötig. Serverseitig muss konfiguriert werden, welche Teile des Verzeichnisbaums an welche Clients *exportiert* (also freigegeben) werden. Außerdem müssen sowohl am Client, wie auch am Server der `portmap`-Daemon laufen, am Server noch andere Daemonen, die wir im weiteren Verlauf besprechen.

Was ist NFS?

- Dateien und Verzeichnisse über ein Netzwerk verwenden
- Client-Server Architektur
- Client mountet Dateisysteme vom Server wie lokale Dateisysteme
- transparent und stateless
- Vorteile
  - Gleiche Homedirectories im ganzen Netzwerk
  - Sparen von Plattenplatz
  - zentrale Administration
- entwickelt von SUN, Standard auf allen UNIX-Systemen(!)

Folie 207

Der NFS-Server
Ein NFS-Server exportiert Teile seines Verzeichnisbaums an die NFS-Clients, die diese dann mounten können. Der Prozess am Server, den die Clients beim Mounten kontaktieren ist völlig getrennt vom Prozess, der dann den Zugriff auf die Dateien ermöglicht. Erstere Aufgabe wird vom Mountdaemon, dem `rpc.mountd` wahrgenommen, letztere vom NFS-Daemon `nfsd`. Diese beiden Daemonen müssen also am NFS-Server zusätzlich zum Portmapper `portmap` und *nach* diesem gestartet werden. `rpc.mountd` und `nfsd` werden über ein gemeinsames Initscript (`/etc/init.d/nfs`) mit den passenden Optionen und in ausreichender Zahl (es laufen immer mehrere Kopien von `nfsd`; für Performanceoptimierung siehe die lokale Dokumentation) gestartet.

Die NFS-Exports, also die freigegebenen Verzeichnisse werden in der Datei `/etc/exports` konfiguriert. Hier werden Verzeichnisse und verschiedenen Parameter, die die Zugriffsrechte der Clients regeln eingetragen. Gemäß dieser Einträge entscheidet `rpc.mountd`, ob einkommende Mount-Requests von Clients berechtigt sind oder nicht und lässt die Mounts zu oder lehnt sie ab.
Ist ein NFS-Verzeichnis gemountet, so kann auf alle unterliegenden Dateien und Verzeichnisse zugegriffen werden (sofern in der Konfiguration nicht explizit ausgeschlossen; siehe zB [1], p. 498). Die Zugriffsberechtigungen werden über die ganz normalen Dateiberechtigungen bestimmt, daher ist die beste Regelung wenn zB die UID 615 am Server mit demselben Benutzer assoziiert ist wie am Client. Dies kann durch eine Synchronisierung der Passwortdateien erreicht werden zB durch die Verwendung von NIS (siehe Abschnitt 16.3). Es ist zwar ein Mappen der UIDs möglich (siehe unten) wegen der größeren Kompliziertheit und dem Administrationsaufwand aber nicht empfehlenswert. Einzige Ausnahme ist der root-Account: root am Client wird standardmäßig auf den Gastaccount nobody am Server gemappt. Dies ist aber nur ein sehr schwacher Schutz des Server-Dateisystems vor root am Client, da dieser ja mittels `su` auf jeden Account am Client einloggen und so mit dessen Rechten auf das NFS-Verzeichnis zugreifen kann.

NFS-Daemonen

- `rpc.mountd` (Mountdaemon) überprüft Berechtigung von Mount-Requests
- `nfsd` (eigentlicher NFS-Daemon) vermittelt Dateizugriff
- `rpc.ugidd` übersetzt UIDs zwischen Clients und Server
- `rpc.rquotad` Quotas für NFS-Benutzer
- `rpc.statd` Reboot Notification
- `rpc.lockd` lockt NFS-exportierte Files; meist vom Kernel gestartet

Folie 208

In jeder Zeile von `/etc/exports` steht zuerst das Verzeichnis, das exportiert werden soll, danach ein Leerzeichen, dann die Clients mit den jeweiligen Zugriffsoptionen in Klammern und ohne Leerzeichen zwischen Client und Klammer. Die Syntax von `/etc/exports` ist äußerst heikel und ein Leerzeichen zu viel oder zu wenig stört die ordnungsgemäße Funktion des NFS-Servers! Die Client-Hosts können per Name oder IP-Adresse angegeben werden. Außerdem kann man ganze Subnetze angeben, indem man die entsprechenden Oktette weglässt. Eine Beispieldatei befindet sich auf Folie 209. Wir erläutern einige gängige Optionen für die Datei `/etc/exports`.

- `secure` der Port, von dem die Anfrage kommt, muss < 1024 sein.
- `insecure` Gegenteil von `secure`
- `ro` Nur Lesezugriffe auf das Verzeichnis möglich; Standardeinstellung
- `rw` Schreib- und Lesezugriff
- `root_squash` übersetzt die UID 0 – also root – auf nobody
- `link_relative` verwandelt absolute Links (die mit einem / anfangen) in relative. Das ist aber nur sinnvoll, wenn das gesamte Filesystem exportiert wird. Sonst können die Links ins Nichts führen
- `link_absolute` lässt absolute Links unverändert
- `map_identity` der Server geht davon aus, dass der Client dieselben UIDs verwendet; Standardeinstellung
- `map_daemon` der Server fragt `rpc.uigdd` zur Übersetzung der UIDs (siehe unten)
- `map_static` die UIDs werden in einer Datei statisch übersetzt

/etc/exports

- Zugangsbeschränkung über `/etc/exports`
- Syntax: Directory Host(Optionen)

```
$ cat /etc/exports

/home           131.130.87.(ro) 131.130.145.63(rw)
/usr/local      dukana(insecure,ro)
#/mnt/cdrom     diana(ro,no_root_squash)
/usr/doc        131.130.145.(insecure,ro)
```

Folie 209

NFS-Exports Optionen

- `ro` read-only
- `rw` read-write
- `secure` Anfragen brauchen Port < 1024
- `root_squash` root@client = nobody@server
- `link_relative` absolute Links in relative umwandeln
- `map_*` gibt an, wo der Server das UID Mapping hernehmen soll

Folie 210

Alle Exports resp. NFS-Mounts können (auch Remote) mittels `showmount`-Kommando erfragt werden. Die Option `-a` zeigt alle Verbindungen im *host:verzeichnis* Format. Mit der Option `-d` zeigt `showmount` alle exportierten Verzeichnisse an; siehe auch Folie 211.

Das Kommando `exportfs` dient zur Wartung der NFS-Exports. Wird eine Änderung in `/etc/exports` vorgenommen, so muss diese mit `exportfs -r` an das NFS-System weitergegeben werden, oder alternativ aber weniger empfehlenswert das ganze NFS-Service mittels Initscripts neugestartet werden.

Weitere NFS-Daemonen die (meist) auch von `/etc/init.d/nfs` gestartet werden sind:

- `rpc.ugidd` übersetzt die UIDs zwischen Server und den Clients
- `rpc.quotad` NFS-Quotadaemon; setzt lokale Quotas voraus.
- `rpc.lockd` kümmert sich um das Sperren der vom Netzwerk aus verwendeten Dateien; meist vom Kernel automatisch gestartet.
- `rpc.statd` überwacht *nicht* den Status der Verbindungen sondern verständigt nach einem Reboot des Servers die Clients vom Crash.

Zum Schluss sei für alle weiteren Details auf das ausführliche NFS-HOWTO verwiesen, das auch eine Schritt-für-Schritt Anleitung zum Aufsetzen eines NFS-Servers enthält.

showmount

- `-d` zeigt alle gemounteten Verzeichnisse
- `-a` zeigt alle gemounteten Verzeichnisse und deren Hosts
- `-e` zeigt die exportierten Verzeichnisse an (gem. `/etc/exports`)

```
bash-2.04$ /usr/sbin/showmount -a phobos
All mount points on phobos:
131.130.14.152:/users/neum
131.130.14.152:/users/susanne
131.130.145.102:/dist
131.130.145.108:/dist/redhat-7.1
131.130.145.108:/users/flo
```

Folie 211

NFS-Mounts

Das mounten eines NFS-Verzeichnisses funktioniert analog dem Mounten eines lokalen Filesystems, allerdings mit einer etwas veränderten Syntax. Will man zB auf einer lokalen Workstation das Verzeichnis `/nethome` vom Server `dukana` auf den Mountpoint (= leeres lokales Verzeichnis) `/users` zu mounten, gibt man als root Folgendes ein:
`mount -t nfs dukana:/nethome /users`.
Mount versucht nun Verbindung via RPC zum `rpc.mountd` auf `dukana` herzustellen. Der Mountdaemon am Server überprüft, ob der Client überhaupt berechtigt ist, auf das angeforderte Verzeichnis zuzugreifen und wenn ja, übermittelt er ihm einen sogenannten *File Handle*. Diesen benutzt nun der Client in allen Anforderungen für Dateien unterhalb von `/users`.
Greift nun ein Benutzer (nicht notwendigerweise root) auf eine Datei in `/users` zu, so sendet der Kernel des lokalen Rechners einen RPC Aufruf an `rpc.nfsd` (den NFS-Daemon) auf dem Server. In diesem Aufruf befindet sich der File Handle, der Name der gewünschten Datei und die UID und GIDs des Benutzers als Parameter. Diese werden gebraucht, um die Zugriffsrechte des Files auslesen zu können.

Der NFS-Client

Zunächst klären wir die genaue Syntax des `mount` Kommandos für NFS:

`mount -t nfs [optionen] nfs_quelle lokales_verzeichnis`

Für `nfs_quelle` verwendet man `nfs_server:entferntes_verzeichnis`. Da diese Notation eindeutig (gegenüber lokalen Mounts) ist, kann man `-t nfs` auch weglassen.
Es gibt zahlreiche Optionen, die man beim Mounten eines NFS-Verzeichnisses einstellen kann. Man kann sie mittels `-o` an der Kommandozeile übergeben oder für feste Mounts in `/etc/fstab` angeben. In beiden Fällen werden mehrere Optionen mit einem Beistrich getrennt und dürfen kein Leerzeichen enthalten. Die Optionen am Prompt überschreiben immer die in `/etc/fstab`. Hier ein Beispieleintrag in `/etc/fstab` (vgl. auch Folie 78) :

```
#volume                mount point     type    options
news:/var/spool/news   /var/spool/news nfs     timeo=42
```

NFS-Mounts

- Syntax, zB:

```
mount -t nfs dukana:/nethome /users
```

- `rpc.mountd`: vergibt File Handles für spätere Verwendung
- Server: `rpc.nfsd` liefert Dateien im per File Handle angegebenen Verzeichnis
- Mit `cat /proc/filesystems` überprüfen, ob der Kernel NFS überhaupt versteht

Folie 212

Alle Optionen von `mount` sind in der Manpage von `nfs` aufgelistet und erklärt. Wir stellen hier die wichtigsten vor.

- *rsize=n* bzw. *wsize=n* geben die Größe des Datenblocks bei Schreib- bzw. Lesevorgängen an, der angefordert wird. Normalerweise 1024 Byte, für optimierte Performance höher.
- *timeo=n* ist die Zeit in Zehntelsekunden, die der Client wartet, bis seine Anforderung erfüllt wird. Was passiert, wenn diese Zeit überschritten wird, hängt von den folgenden Optionen ab.
- *hard* setzt diese Quelle explizit als „hart“ gelinkt. D.h. der Client versucht nach einer Zeitüberschreitung noch einmal, die Anforderung zu versenden (und diesmal rechtzeitig zu empfangen). Es gibt kein Limit, wie oft der Client versucht, eine Antwort zu bekommen.
- *soft* Antwortet der Server hier nicht, gibt `rpc.mountd` dem aufrufenden Programm einen I/O Fehler zurück.
- *intr* Erlaubt es, eine NFS-Aufruf zu unterbrechen. Nützlich, wenn der Server nicht mehr reagiert.

Von `rsize` und `wsize` einmal abgesehen, betreffen alle Optionen das Verhalten des Clients, wenn die Verbindung zum Server abbrechen sollte. Sie arbeiten wie folgt zusammen: Sendet der Client eine Anforderung an den NFS-Server, so erwartet er, dass dieser nach einem gegebenen Zeitraum (mit der `timeo` Option) antwortet. Kommt keine Bestätigung vom Server, so sendet der Client die Anforderung erneut, diesmal mit dem doppelten Timeout. Ist der maximale Wert von 60 Sekunden erreicht, so gibt es ein großes Timeout. Standardmäßig wird dann eine Warnung ausgegeben und die Prozedur fängt von vorne an. Theoretisch geht das unendlich lange so weiter. NFS-Quellen, die ihre Anforderungen stur wiederholen, nennt man hart gemountet. Im Gegensatz dazu liefern weich gemountete Quellen einen Fehler zurück, wenn es ein großes Timeout gibt. Da normalerweise erst in den Buffer geschrieben wird, kommt der Fehler bei einem Schreibbefehl nicht an dem eigentlich auslösenden Prozess an. Daher kann man bei weich gemounteten Quellen nie sicher sein, dass die Schreiboperation auch wirklich erfolgreich war.

Welche dieser beiden Methoden man einsetzt, ist Geschmackssache. Allerdings sollte man Daten, die unbedingt konsistent bleiben müssen, hart einbinden. Wenn man zum Beispiel die X Programme über NFS einbindet, so sollte einem nicht die ganze Sitzung verloren gehen, nur weil die Verbindung kurz unterbrochen ist. Hingegen braucht man das FTP Archiv nur weich einzubinden, da sonst der ganze Prozess hängt, wenn die Verbindung nicht ganz so gut ist. Bei einem Server hinter einem Router sollte man die `timeo` Option unbedingt weiter hinauf setzen.
Hart gemountete Quellen stellen ein Problem dar, weil die Dateioperationen nicht unterbrochen werden können. Der Prozess steht dann, bis der Server wieder erreichbar ist. Der User kann nichts tun, um diesen Vorgang abzubrechen. Ist zusätzlich die `intr` Option gesetzt, so unterbricht der Prozess beim Empfang eines Signals jede Schreiboperation. Die Daten gehen dann aber verloren.

Der Automounter
In mittleren bis großen Netzen ist der Einsatz eines Dienstes, der NFS-Verzeichnisse (zB NFS-exportierte Homedirectories, aber auch lokale CDROMs und Floppies) erst bei Bedarf mountet und nach einem Timeout wieder unmountet besonders vorteilhaft. Das schützt zudem auch vor der Gefahr, die droht, wenn ein Server abstürzt bzw. nicht erreichbar ist, von dem man Verzeichnisse hart gemountet hat. Es gibt zwei Programmpakete, die diesen Dienst bereitstellen, `amd` und `automount`, das ursprünglich von SUN entwickelt wurde. Wir besprechen hier kurz das letztere.
`automount` wird über sogenannte Maps konfiguriert. Die Master Map `/etc/auto.master` gibt die den Mountpoints übergeordneten Directories und die dazugehörigen Maps an. In diesen wiederum sind die Mountpoints und die Devices samt Mountoptionen eingetragen. Beispieldateien finden sich auf der Folie.
Nach dem (Neu-)start des `autofs` Services (Initscript) reicht es dann aus, in ein automount-Verzeichnis (zB `/auto.mnt/floppy`) zu wechseln, um das dorthin gemappte Gerät/Verzeichnis zu mounten. Achtung, das Verzeichnis scheint *vorher* in einem Listing *nicht* auf, da es ja nicht gemountet ist. Dieses Problem kann man aber mittels Setzen symbolischer Links auf die Mountpoints umgehen.

NFS-Mountoptionen

- *rsize=n* und *wsize=n* Größe der Datenblocks beim Lesen/Schreiben
- *timeo=n* Timeout in 1/10-Sekunden angeben
- *hard* warten, bis der Server antwortet
- *soft* gibt nach dem timeout einen Fehler zurück
- *intr* erlaubt es, den Verbindungsaufbau wieder abzubrechen

Folie 213

Automounter

- Mounten nur so lange, wie etwas gebraucht wird
- Remote hart gemountete Verzeichnisse Risiko beim Crash des Servers
- Auch für Floppy, CD-ROM, ...
- Bei Zugriff auf Mountpoint wird Directory gemountet
- einfach konfigurierbar und stabil (Treiber im Kernel)
- `amd` und `automount`

Folie 214

Automounter Maps

```
[roli@pablo roli]$ cat /etc/auto.master
 # Format of this file:
 # mountpoint map options
 /auto.mnt       /etc/auto.mnt           --timeout 5
 /kusers         /etc/auto.kusers        --timeout 300

[roli@pablo roli]$ cat /etc/auto.mnt
 # This is an automounter map and it has the following format
 # key [ -mount-options-separated-by-comma ] location
 redhat   phobos:/dist/redhat-7.0
 cdrom    -fstype=iso9660,ro,exec,nosuid,nodev        :/dev/cdrom
 floppy   -fstype=auto,rw,sync,exec,nosuid,nodev,user :/dev/fd0
[roli@pablo roli]$ cat /etc/auto.kusers
 *       ken.macondo:/users/&
```

Folie 215

16.3 Network Information Service (NIS)

Das *Network Information Service* ist ein „Administrative Database System“ das es ermöglicht, Systemdateien eines Servers über ein Netzwerk für Clients verfügbar zu machen. Meist dient es dazu, die drei Dateien `/etc/passwd`, `/etc/group` und `/etc/shadow` eines Servers über ein Netzwerk zu verteilen und so einheitliche Accounts in einer sogenannten „Nis-Domäne“ (Server+Clients) zu definieren. In Kombination mit NFS gelingt es so, auch große Netzwerke übersichtlich zu verwalten und netzwerkweite Logins mit gleichen Homedirectories bereitzustellen. Solche kombinierten NFS/NIS-Systeme eignen sich zB besonders gut für Instituts/Firmennetze oder PC-Labors.

Entwickelt wurde NIS von SUN in den 80ern unter dem Namen „Yellow Pages“ (der dann aufgrund von Copyright Problemen mit der British Telecom geändert werden musste) und viele der Daemonen und Kommandos haben noch immer ein „yp“ im Namen. NIS ist Standard in der ganzen Unix-Welt und es können – ähnlich zu NFS – gemischte NIS-Domänen mit verschiedenen Unix-Varianten als Server und oder Clients betrieben werden. SUN vertreibt auch ein aus NIS weiterentwickeltes „Administrative Database System“ NIS+ das weniger verbreitet ist und von Linux nicht unterstützt wird. Ein alternatives System ist etwa LDAP (Lightweight Directory Access Protocol); siehe `http://www.openldap.org/`.

Gewöhnliche Anwendungen und Programme am System müssen nichts von NIS wissen, um es zu verwenden. Vielmehr erledigen die Funktionsaufrufe der Unix-C-Bibliothek diese Aufgabe (konfiguriert u.a. in `/etc/nsswitch`).

Funktionsweise
NIS-Dateien (die aus Performancegründen in einem binären Format gespeichert werden; sogenannte NIS-Maps) befinden sich gewöhnlich in `/var/yp/` in einem Unterverzeichnis mit dem Namen der NIS-Domäne. Jedes Mal, wenn man Änderungen an den über NIS-exportierten Dateien vornimmt (zB wenn man einen Benutzer hinzufügt), muss man nach `/var/yp/` wechseln und `make` ausführen. Damit werden die binären Dateien geupdated. Diese Prozedur wird man natürlich durch ein entsprechendes Script automatisieren.

NIS

- Auf RPC basierendes Client/Server System
- Systemdateien eines Servers auf Clients verfügbar machen
- Entwickelt von SUN in den 80ern; Unix-Standard
- Server+Clients in NIS-Domäne zusammengefasst
- Meist zur netzwerkweiten Benutzerverwaltung eingesetzt
- Kombination NIS/NFS ermöglicht netzwerkweite Logins mit gleichem Homedirectory
- Master/Slave-Server: Last verringern, Ausfallssicherheit

Folie 216

NIS-Dämonen Der NIS-Dienst wird server- und clientseitig durch die jeweiligen Daemonen vermittelt. Am Client muss das YP-Bind-Service (`ypbind`) und am Server *zusätzlich* das YP-Server-Service (`ypserv`) gestartet werden. Achtung ebenso wie bei NFS muss sowohl am NIS-Server als auch am NIS-Client der Portmapper laufen.

Der `ypbind` wird über die Datei `/etc/yp.conf` konfiguriert, die in etwa wie folgt aussieht:

```
domain meine.nis.domain server mein.nis.server
```

Außerdem ist es notwendig, dass alle NIS-Server in `/etc/hosts` eingetragen sind und der NIS-Domänenname gesetzt ist. Dieser kann händisch mit dem Kommando `nisdomainname meine.nis.domain` (ohne Argument gibt das Kommando den aktuell gesetzten NIS-Domänenname aus) eingegeben oder dauerhaft (unter RedHat) in `/etc/sysconfig/network` mittels Eintrags `NISDOMAIN=meine.nis.domain` konfiguriert werden.

Der YP-Server wird durch mehrere Dateien konfiguriert. In `/etc/yp.conf` werden einige globale Einstellungen vorgenommen. Meist muss an den Defaulteinstellungen nichts verändert werden – für Details siehe `man ypserv.conf`. In `/var/yp/securenets` ist eingetragen, welche Hosts berechtigt sind die Maps zu verwenden, also in die NIS-Domäne eingebunden sind. Eine Beispieldatei befindet sich auf Folie 217. Für weitere Details siehe die Manpages.

Will man, dass Benutzer ihre NIS-Passwörter – mit dem dafür vorgesehenen Befehl `yppasswd` – ändern können, muss serverseitig der `yppasswdd`-Daemon laufen. Dieser kann einfach mittels Initscripts gestartet werden und muss in den meisten Fällen nicht extra konfiguriert werden.

`/etc/securenets`

```
#
# securenets    This file defines the access rights to your NIS server
#               for NIS clients. This file contains netmask/network
#               pairs. A clients IP address needs to match with at least
#               one of those.
#               One can use the word "host" instead of a netmask of
#               255.255.255.255. Only IP addresses are allowed in this
#               file, not hostnames.
# Always allow access for localhost
255.0.0.0       127.0.0.0
# This line gives access to everybody. PLEASE ADJUST!
#0.0.0.0                 0.0.0.0
# Clients
host            131.130.16.20
host            131.130.16.60
host            131.130.16.24
```

Folie 217

Um die Systemlast auf einem NIS-Server möglichst gering zu halten bzw. um bei Ausfall eines Servers Schäden und Verzögerungen möglichst gering zu halten, gibt es die Möglichkeit, mehrere *NIS-Slave-Server* einzurichten, die die vom *Master-Server* verteilten Dateien mit diesem synchronisieren. Für die Clients spielt es keine Rolle, ob sie die Dateien von einem Master- oder Slave-Server übernehmen.

Aufsetzen einer NIS-Domäne
Zuerst legt man einen NIS-Domainnamen (zB `praxis.compsys`) fest. Diesen teilt man nun dem/den Server(n) und den Clients mittels `nisdomainname praxis.compsys` mit (dauerhaft mittels Eintrag in Netzwerkkonfiguration; siehe oben).

- Master-Server
  Hier initialisiert man die Domäne und erstellt die zur Domäne gehörigen Dateien (Maps) und startet die Server. Welche Maps installiert werden wird in `/etc/ypserv.conf` festgelegt. Diese Datei kann meist in der Defaultform verwendet werden.

  ```
  /usr/lib/yp/ypinit -m
  service portmap start
  service ypserv start
  service ypbind start
  ```

  Dann müssen in der Datei `/var/yp/securenets` die IP-Adressen der Clients eingetragen werden, damit diese vom Server in der Domäne akzeptiert werden (siehe auch Folie 217). Wichtig ist, dass auch am NIS-Server immer der Clientprozess `ypbind` laufen muss, damit auch der Server in die Domäne eingebunden ist. Schließlich sollte der `yppasswdd`-Daemon gestartet werden und das Starten der YP-Daemonen (etwa mittels `chkconfig`) beim Systemstart eingerichtet werden.

- Slave-Server
  Der einzige Unterschied zum Master-Server ist die Option `-s`, der man den Hostnamen des Masters mitangeben muss:

  ```
  /usr/lib/yp/ypinit -s master_der_domain
  service portmap start
  service ypserv start
  service ypbind start
  ```

- Clients
  Hier genügt es, die `/etc/yp.conf` wie oben angegeben zu konfigurieren (also Server und Domäne anzugeben, je eine Zeile für den Master und jeden Slave-Server) und dann den `ypbind` zu starten:

  ```
  service portmap start
  service ypbind start
  ```


Wichtige NIS-Kommandos sind auf der letzten Folie des Kapitels zusammengestellt. Schließlich folgt der Verweis auf das NIS-HOWTO für alle weiteren Details.

NIS verwenden

- Dateien in `/var/yp`
- Nach Änderung exportierter Daten dort `make` aufrufen.
- `ypserv`, `ypbind`, `yppasswdd` Services
- Portmapper muss am Client und Server gestartet sein
- Client Konfiguration in `/etc/yp.conf`
- Server Konfiguration in
  - `/etc/ypserv.conf`
  - `/var/yp/securenets`

Folie 218

NIS-Domäne erstellen

- `nisdomainname` setzen
- Master-Server: `ypinit -m`,
  `portmap`, `ypserv`, `ypclient`, `yppasswdd` starten
- Slave-Server: `ypinit -s master`, Services wie oben
- In `/var/yp/securenets` Clients eintragen
- Clients: `/etc/yp.conf` konfigurieren, `portmap` und `ypbind` starten

Folie 219

NIS-Kommandos

- `ypwhich` mit welchem NIS-Server verbunden?
- `ypcat exp` zeigt Inhalt einer exportierten Map
- `yppasswd user` ändert das Passwort von `user`
- `ypchfn user` ändert Informationen über `user`
- `ypchsh user` ändert die Shell von `user`

Folie 220

17 FTP- Web- und Mailserver

In diesem Kapitel besprechen wir drei wichtige Internetservices resp. ihre Server-Implementierungen unter Linux; wir stellen den FTP-Server `proftp`, den Webserver `apache` und den Mailserver `sendmail` vor.

17.1 FTP-Server

FTP (File Transfer Protocol) – obwohl eines der ältesten Internetservices – erfreut sich noch immer großer Beliebtheit. Abgesehen von interner Verwendung (zB als eine zentralisierte Rechner-Installationsmöglichkeit) beschränkt sich der Einsatz heute hauptsächlich auf das sogenannte anonyme FTP, das Benutzern, die keinen Account auf dem jeweiligen Rechner(-netz) besitzen, das Herunterladen bestimmter öffentlicher Daten gestattet. Zu diesen Daten gehören hauptsächlich Programmpakete, Bugfixes, Dokumente oder Musikdateien. Der wesentliche Vorteil gegenüber dem HTTP-Protokoll ist, dass der User selbst mit gewohnten Unix-Befehlen durch den Verzeichnisbaum navigieren darf, wogegen man auf einer Seite am Webserver immer einen Link auf zB neu hinzugekommene Dateien setzen muss, um sie dem Benutzer bekannt zu machen.
Eine besondere Warnung sei hier – noch einmal (vgl. Abschnitt 15.3) – bezüglich des nicht-anonymen (also benutzerbasierten) FTP gegeben: das Passwort, das der User eingibt, geht unverschlüsselt über die Datenleitung und kann mitgesnifft werden. Obwohl viele Seiten im Internet nicht-anonymes FTP zB für Webseitenaktualisierung ermöglichen, raten wir prinzipiell davon ab und wollen uns im Folgenden nur dem anonymen FTP-Server widmen.

FTP

- File Transfer Protocol
- Einer der ältesten Dienste
- Öffentliche Bereitstellung von Daten
- Interne Verwendung für zB Rechner-Installation
- Anonym – nicht-anonym (unsicher!)
- Vom User selbst navigierbar

Folie 221

Verschiedene Server-Pakete

- `wuftpd` Lange Zeit Standard, komfortabel, unsicher
- `ncftpd` Komfortabel, relativ sicher, keine freie Software, keine offenen Sourcen
- `proftpd` Umfangreich konfigurierbar, sicher
- Andere Server (meist nur anonym): `anonftpd`, `vsftpd`, `trollftpd`, ...

Folie 222

Der FTP Server, der früher besonders beliebt war (weil er einfach zu konfigurieren und bei den meisten Distributionen enthalten ist), ist der `wuftpd`, der an der Washington University entwickelt wurde (daher auch der Name) und traditionellerweise vom Internetdämon gemanagt wird. Gerade in letzter Zeit hat man immer wieder große Sicherheitslücken darin entdeckt und auch die ersten Linux-Würmer nutzen unter anderem seine Schwächen aus. Sicherere Alternativen sind der `ncftpd` und der `proftpd`. Da ersterer kommerziell ist, man sich den Sourcecode nicht ansehen darf und er außerdem unter einer besonderen Lizenz steht, die nur für „Educational Use“ freien Einsatz gestattet, beschäftigen wir uns in Folgenden nur mit dem `proftpd`, der noch dazu dem Apache Webserver sehr ähnliche Konfigurationsdateien hat. Neben diesen beiden „Big Players“ stehen noch kleinere spezialisierte FTP-Server zur Verfügung (`oftpd`, `anonftpd`, `trollftpd`, ...), die im Allgemeinen auch relativ sicher sind (einige erlauben sogar überhaupt keine auf Dateien schreibend zugreifende Aktionen und stellen daher vermutlich das Optimum an Sicherheit, jedoch nicht an Komfort dar). Eine neuere Entwicklung ist der `vsftpd`, der schon vom frühesten Stadium an in Hinblick auf höchste Sicherheit programmiert wurde.

Der Proftp-Server

`proftpd` wird bei den meisten Distributionen leider nicht mitgeliefert, sodass wir das entsprechende Paket aus dem Internet herunterladen müssen. Egal, ob man dabei die Sourcen selbst compiliert, das RPM- oder Debian-Paket nimmt, man erhält direkt nach der Installation einen bereits gut vorkonfigurierten FTP Server, dessen Konfigurationsdatei `/etc/proftpd.conf` ist. Genauer beinhaltet das proftpd-standalone Zusatzpaket diese Konfigurationsfile und ein entsprechendes Initscript. Der `proftpd` kann demzufolge sowohl als Standalone Server als auch aus dem Internetdämon heraus verwendet werden.

Im Prinzip reicht es aus, den Server zu starten, um einen voll funktionstüchtigen FTP Server vorzufinden, mit dem man sich sogleich mittels `ftp localhost` verbinden kann:

```
martin@notebook:~$ /usr/bin/ftp localhost
Connected to localhost.
220 ProFTPD 1.2.1 Server (Debian) [notebook]
Name (localhost:martin): anonymous
331 Anonymous login ok, send your complete email
    address as your password.
Password: (Mailadresse eingeben)
230 Anonymous access granted, restrictions apply.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Auffallend ist hier, dass der Server scheinbar in der Standardeinstellung auch nicht-anonymen Zugang (er schlägt als FTP Benutzername `martin` vor) erlaubt. Um sich das lästige Eintippen von `anonymous` und Mailadresse bei jeder Connection zum Server zu ersparen, sollte man übrigens den `ncftp` Client verwenden, der auch ansonsten durch große Benutzerfreundlichkeit glänzt (Tab-Completion, etc., siehe auch Abschnitt 15.3).
Am `ftp>` Prompt kann man nun wie gewohnt Unix-Befehle wie `ls` oder `cd` eingeben, die der FTP-Server im Repository (das die Daten, die man freigibt, enthält und gewöhnlich das Homedirectory des Systembenutzers `ftp` ist, also etwa `/home/ftp`) ausführt. Eine Auflistung aller möglichen Befehle bekommt man durch Eingabe von `help`, spezifische Hilfe zu einem Kommando mit `help kommando` (zB `help mget`).

ProFTPD

- in vielen Distributionen nicht enthalten
- `http://www.proftpd.net`
- Pakete für viele Distributionen verfügbar
- Gut vorkonfiguriert
- Umfassend konfigurierbar (`/etc/proftpd.conf`)
- genau auf Bugs „durchleuchtet“
- Läuft als nicht-privilegierter User

Folie 223

Konfiguration
Wir wollen nun die wichtigsten Optionen der Konfigurationsdatei herausgreifen und Schritt für Schritt durchgehen:

```
ServerName                      "Mein FTP Server"
ServerType                      standalone
```

Die `ServerName` Direktive ist mehr von kosmetischer Natur; sie zeigt beim Einloggen am Server den eingestellten Namen neben der ProFTPD Versionsnummer. Der `ServerType` dagegen bestimmt, ob der Server „standalone“ bzw. über den `(x)inetd` gestartet werden soll.

```
TimeoutNoTransfer               600
TimeoutStalled                  600
TimeoutIdle                     1200
```

Viele Benutzer verbinden mit einem FTP Server, laden etwas herunter und vergessen dann, die Verbindung auch wieder zu trennen. Da es natürlich ein Maximum an gestarteten Serverprozessen geben muss, könnten zB 30 vergessliche User einen FTP Server lahmlegen. Damit es gar nicht soweit kommt, definieren wir Timeouts (in Sekunden) für verschiedene Aktionen, nach denen der Benutzer automatisch einen Disconnect bekommt.

```
DisplayLogin                    welcome.msg
DisplayFirstChdir               .message
LsDefaultOptions                "-l"
```

Wieder mehr kosmetischer Natur sind diese drei Optionen, die jeweils beim Login bzw. beim Wechsel in ein Verzeichnis eine Meldung ausgeben, die in der besagten Datei liegt. Das kann auf großen FTP-Servern mit zB Spiegelungen von Linux-Distributionen bei der Navigation enorm von Vorteil sein. Die letzte Direktive sagt aus, dass der Benutzer auf jeden Fall bei der Eingabe von `ls` ein langes Listing bekommen soll (was im Allgemeinen erwünscht sein dürfte, da man bei FTP sicher gerne die Dateigröße erfährt).

```
Port                            21
```

Dieser Punkt sollte selbsterklärend sein. Eine interessante Möglichkeit, um den Server ein wenig mehr zu schützen, ist, ihn auf einen anderen Port zu legen. Zu viel Steigerung der Sicherheit sollte man sich davon nicht erwarten, denn gegen Tools wie `nmap` ist auch das machtlos. Zumindest aber sichert man sich gegen zufällige Verbindungen von neugierigen Menschen besser ab.

```
MaxInstances                    30
```

Hier kann man die maximale Anzahl an Prozessen für den FTP Server begrenzen. Bei kleineren Servern ist der Defaultwert sicher akzeptabel; für größere sollte man ihn entsprechend erhöhen.

```
User                            nobody
Group                           nogroup
```

Dies sind zwei sicherheitstechnisch wichtige Optionen, die festlegen, unter welchem Benutzer der FTP-Daemon laufen soll. Natürlich muss er zum Starten und Binden auf den (privilegierten) Port 21 root Rechte haben, diese legt er aber danach ab, was ihn auch relativ unempfindlich gegen „Buffer Overflow“ Attacken macht, denn im schlimmsten Fall erhält der Hacker eine nobody Shell statt einer root Shell.
Die generellen Optionen sind damit abgeschlossen, wir wenden uns den verzeichnisspezifischen Direktiven zu und da den Regeln für anonymes FTP.

```
<Anonymous ~ftp>
  User                          ftp
  Group                         nogroup
  UserAlias                     anonymous ftp
```

Die erste Zeile sagt uns, dass die folgenden Regeln bis zum schließenden „Tag“ nur für anonyme Connections und das Homeverzeichnis des ftp Accounts gelten sollen. Und da setzen wir auch gleich den Benutzer auf `ftp`, die Gruppe auf `nogroup`, d.h. wenn sich ein User mit dem FTP-Server anonym verbindet, ist er in Wirklichkeit am Server der Benutzer `ftp` (Gruppe `nogroup`). Außerdem wollen wir erreichen, dass auch der Benutzername `anonymous` am Login Prompt akzeptiert wird, was man mit `UserAlias` bewirkt.


```
<Directory *>
 <Limit WRITE>
   DenyAll
 </Limit>
</Directory>
```

Die obigen Zeilen entziehen dem anonymen FTP-User jedwege Schreibberechtigung, d.h. auch wenn der Benutzer `ftp` irgendwo im über FTP erreichbaren Bereich des Dateisystems Schreibrechte hat, werden diese dem anonymen FTP-User entzogen.

```
</Anonymous>
```

beendet die `Anonymous` Sektion und zugleich die gesamte Konfigurationsdatei.

Nützliche FTP Kommandos
Zum Abschluss dieses Abschnitts stellen wir noch einige nützliche FTP-Befehle (sowohl server- als auch clientseitig) vor (siehe auch Folie 225).

- `ftpwho` zeigt Informationen über die gerade per FTP eingeloggten Benutzer an
- `ftpcount` zählt die gesamten per FTP eingeloggten User
- `ftpshut time [warn]` beendet zur angegebenen Zeit alle FTP Serverprozesse und gibt optional eine Warnung aus (zB `ftpshut +3 Server down for maintainance` deaktiviert den Server in 3 Minuten)

Proftpd Konfiguration

```
ServerName          "Mein FTP Server"
ServerType          standalone
TimeoutNoTransfer   600
TimeoutStalled      600
TimeoutIdle         1200
DisplayLogin        welcome.msg
DisplayFirstChdir   .message
LsDefaultOptions    "-l"
Port                21
MaxInstances        30
User                nobody
Group               nogroup
<Anonymous ~ftp>
  User              ftp
  Group             nogroup
  UserAlias         anonymous ftp
<Directory *>
 <Limit WRITE>
   DenyAll
 </Limit>
</Directory>
</Anonymous>
```

Folie 224

FTP Kommandos

- Serverseitig
  - `ftpwho` Infos über FTP-Benutzer
  - `ftpcount` Anzahl der FTP-User
  - `ftpshut` FTP-Server deaktivieren
- Clientseitig
  - `ftp` Standard, wenig komfortabel
  - `ncftp` Sehr bequem, Filename-Completion
  - `kbear` Komfortabel, Graphisch

Folie 225

17.2 Der Apache Webserver

Das wohl bekannteste Service im Internet ist das World Wide Web (WWW) oder Hyper Text Transfer Protocol (HTTP), das es gestattet, mittels Client, d.h. Webbrowser (Internet Explorer, Konqueror, Opera, Mozilla, Netscape, ...) Text-, Grafik-, Sound-, etc. Files aus dem Netz herunterzuladen und sogenannten Hyperlinks von einem Server zum anderen zu folgen.

Das HTTP-Service wird von Webservern bereitgestellt. Obwohl es mehrere Anbieter gibt, ist der (Open Source) Webserver *Apache* mit ca. 55% Marktanteil der am weitesten verbeitete Server und wird in (fast) jeder Linux-Distribution mitgeliefert; wir konzentrieren uns daher ausschließlich auf ihn.

Der „A PAtCHy sErver“ wurde 1995 aus dem NCSCA (National Center for Supercomputing Applications) HTTPD mittels vieler bereits vorhandener Patches entwickelt; außerdem ist der Name eine bewusste Anspielung auf den indigenen Stamm. Derzeit wird der Server von der Apache Software Foundation, einer Nonprofit Organisation, unter einer GPL-artigen Open Source Lizenz weiterentwickelt; die letzte Version ist 1.3.24. resp. 2.0.35. Für alle Detailinformationen verweisen wir auf die Apache Homepage unter `http://www.apache.org`.

Apache ist nicht nur für alle gängigen Unix-Systeme, sondern auch für MacOS, OS/2 und sogar Windows (95–ME, NT4.0–2000) frei verfügbar und in fast alle Linux-Distributionen sehr gut integriert.

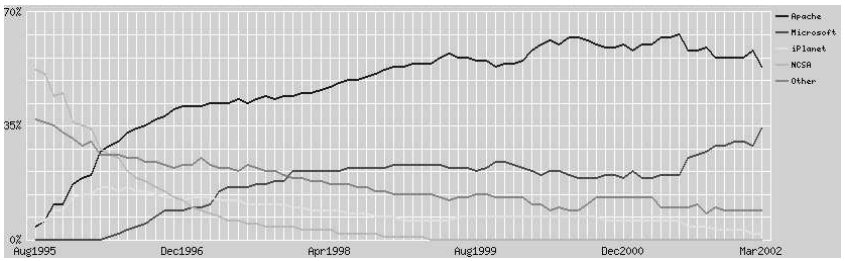
Webserver

- Server für WWW-Hypertext-Dokumente
- verwendet HTTP-Protokoll (Hyper Text Transfer Protocol)
- sendet
  - Text (vor allem HTML)
  - Grafik
  - Sound, ...

  an Client (Browser)
  - Internet Explorer
  - Konqueror
  - Mozilla, ...

Folie 226

HTTP-Server Marktanteile



Folie 227

Der Apache Webserver

- A PAtCHy sErver aufbauend auf NCSA-HTTPD
- opensource, Apache Licence
- für gängige Plattformen (Unix, NT, Mac, OS/2,...)
- eng an HTTP-Standards orientiert
- `http://www.apache.org`
- aktuelle Version: 1.3.24, 2.0.35
- Erweiterungen: PHP-, Perl-Module, Java-Servlets, CGI-Scripts

Folie 228

Apache für (Redhat) Linux

- RPMs erhältlich
  - `apache`
  - `apache-manual`
- Daemon `/sbin/httpd`
- Initscript `/etc/init.d/httpd`
- Konfigurationsdateien `/etc/httpd/conf/`
- Logfiles `/var/log/httpd/`
- Bibliotheken, Module `/usr/lib/apache/`
- Server Root `/var/www/` (früher `/home/httpd/`)

Folie 229

Meist wird der Apache als Standalone Server betrieben und mittels des entsprechenden Initscripts `/etc/init.d/httpd` gestartet; Nach der Installation (mittels `rpm` oder Tarball) steht bereits eine gut dokumentierte Defaultkonfiguration zur Verfügung und wir können den Server starten. Der erste Test ist nun, sich mittels Browser auf das Loopback Device zu verbinden (`http://127.0.0.1/`). Wenn alles geklappt hat, kommt man auf die Default Willkommensseite des lokalen Apache-Servers, wo bereits Links zur mitgelieferten Online Dokumentation (falls installiert) bzw. zur Apache Homepage eingetragen sind.

Wir besprechen im folgenden die grundsätzlichen Konfigurationsoptionen des Apachen und verweisen für Details auf die Homepage bzw. auf die sehr angenehm zu lesende „Apache Administrationsbibel“ [14].
Die wichtigsten Einstellungen für den laufenden Betrieb von Apache werden in der Datei `httpd.conf` gemacht, welche sich je nach Distribution im Verzeichnis `/etc/` oder in einem Apache-spezifischen Unterverzeichnis zB `/etc/httpd/conf/` befindet.
Zunächst befassen wir uns mit der Funktionsweise eines Webservers. Ein User gibt eine HTTP-Adresse (zB `http://www.univie.ac.at`) in seinem Browser an. Über einen Nameserver bzw. über eine Hosts-Datei wird die IP-Adresse ermittelt und ein Request an den Server gesendet; (standardmäßig) an Port 80. Dort wartet der Apache auf Anfragen. Im Konfigurationsfile `httpd.conf` müssen wir beides eintragen; den Namen des Servers sowie seine IP-Adresse und den Port.
Erreicht den Server der Request so kommt der Eintrag `DocumentRoot /var/www/html` im Konfigurationsfile zum tragen; er definiert das Haupt(dokumenten)verzeichnis des Webservers. Weiters kann man angeben, welche Datei er aus diesem Verzeichnis an den User schicken soll, wenn nicht explizit eine Datei angegeben wurde. Das ist in den meisten Fällen `index.html`. Es können (optional) auch mehrere Dateien angegeben werden, zB `index.php` etc. Fassen wir die bisherigen Einträge zusammen (Kommentare werden durch „`//`“ markiert).

```
ServerName      www.studentenfutter.at  //ServerName
Listen          08.15.47.11:80          //IP Adresse und Port
DocumentRoot    /var/lib/apache/htdocs
DirectoryIndex index.html index.htm index.php index.shtml
```

Apache Installation

- installieren: `rpm -ihv apache.sowieso.rpm`
- Achtung: trägt sich in `/etc/rc[3,5].d` ein
- starten: `/etc/init.d/httpd start`
- 1. Test: Browser auf `http://127.0.0.1`

  „Willkommensseite“
- Link auf Dokumentation, Info

Folie 230

Außerdem verwendet unser Apache auch einen eigenen Useraccount (vgl. FTP-Server);wir tragen also ein:

```
User apache
Group apache
```

Achtung der Account für den Webserver kann je nach Distribution verschieden heissen; im Normalfall sollte die Einstellung aus dem Defaultkonfigurationsfile verwendet werden.
Wesentlich hierbei ist, dass Apache unter diesen Berechtigungen die Dateien holt resp. liest. Dürfte der User `apache` nicht auf `index.html` zugreifen würde der User am Browser eine Fehlermeldung angezeigt bekommen. In dieser Fehlermeldung erscheint auch die Adresse des Serveradmins; einzutragen mit:

```
Serveradmin ich@bins.net
```

In unserem einfachen Fall hat der User eine HTML-Datei geholt, die als ASCII-Datei auf dem Server liegt. Der Server sendet diese Datei an den Browser und dieser stellt sie dar.

Weitere wichtige Konfigurationsdirektiven des Apachen sind

- `UserDir` bezeichnet den Namen des Standard Verzeichnisses, in dem die User des Unix-Systems ihre Homepages ablegen können; default: `public_html`; diese Seiten sind dann unter `http://www. studentenfutter.at/~user` erreichbar.
- `ErrorLog` bezeichnet das Fehlerlogfile; default: `/var/log/httpd /error_log`
- `LogLevel` analog zu den Priorities für den Syslog Daemon
- `CustomLog` gibt das Access-Logfile an (jeder Zugriff wird mitgeschrieben); default: `/var/log/httpd/access_log`

Der Apache kennt auch eigene Berechtigungskonzepte. Man kann in der `httpd.conf` mit

```
<Directory /var/lib/apache/WWW/studentenfresser>
Options
....
</Directory>
```

Zugriffsberechtigungen pro Verzeichnis setzen, eigene Gruppen und User für den Apache einrichten etc. Diese sind unabhängig von den Gruppen und Usern des Betriebssystems. Außerdem können mittels `Options` Direktive pro Directory weitere Optionen angegeben werden.

Bei der Apache Konfiguration ebenfalls sehr wichtig sind die *Module*, die hauptsächlich für dynamische Webseiten eingebunden werden müssen. Der Unterschied ist, dass die HTML-Datei nicht am Server liegt, sondern erst bei einem Request dynamisch erstellt wird, wie ein kleines Programm, das statt purem Text dann eben HTML-Code ausgibt. Beliebte Programmiersprachen dafür sind Perl oder PHP.

Für die weiteren wichtigen und sicherheitsrelevanten Punkte CGI-Scripts (Common Gateway Interface) bzw. SSL (Secure Socket Layer) verweisen wir auf die Online Dokumentation, die einschlägigen HOWTOS und das Buch [9].

Außerdem ist ein GUI zur Konfiguration des Apachen namens Comanche (**Co**nfiguration **Mana**ger for Apa**che**) verfügbar (siehe auch Folie 233).

Apache Konfiguration

- Online-Dokumentation, Homepage
- gut dokumentierte Beispielfiles
- `/etc/httpd/conf/httpd.conf` Basiskonfiguration
- `/etc/httpd/conf/access.conf` (veraltet)
- `/etc/httpd/conf/srm.conf` (veraltet)
- GUI Comanche (**Co**nfiguration **Mana**ger for Apa**che**)

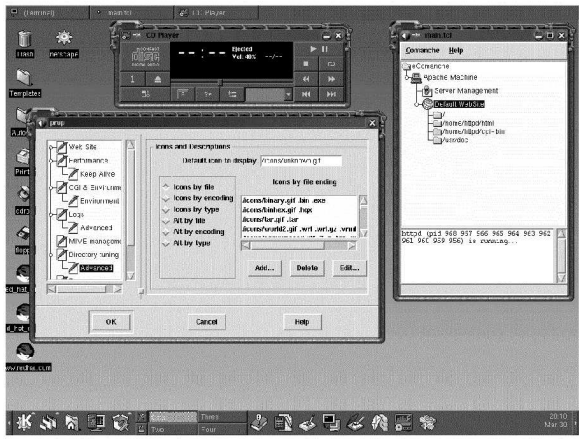
Folie 231

/etc/httpd/conf/httpd.conf

```
ServerType standalone
Port 80
HostnameLookups off
User nobody
Group nobody
ServerAdmin root@localhost
ServerRoot /etc/httpd
ErrorLog logs/error_log
LogLevel warn
LoadModule env_module  modules/mod_env.so
LogFormat "%h %l %u %t %>s %b" common
Timeout 300
KeepAlive On
MaxKeepAliveRequests 100
StartServers 10
MaxClients 150
MaxRequestsPerChild 100
```

Folie 232

Comanche



Folie 233

17.3 Der Sendmail Mailserver

Neben dem Surfen im World Wide Web ist das Kommunikationsmittel Email der am häufigsten genutzte Dienst im Internet. Laut verschiedener Schätzungen liegt die weltweite Anzahl versendeter Emails bei weit über fünf Milliarden täglich bzw. einem Drittel des gesamten Datenverkehrs des Internet.

Aus diesen Daten wird der besondere Anspruch an einen Mailserver (und nicht zuletzt an seinen Administrator, der auch Postmaster genannt wird) sichtbar. Als besonders stabil, performant und flexibel hat sich der Mailerdämon `sendmail` erwiesen, der heute einen Anteil von über 60% aller im Internet laufenden Mailserver innehält. Dieser Dämon läuft am Server auf Port 25 und nimmt Daten von einem Netzwerkclient entgegen, die dem Format des SMTP (Simple Mail Transfer Protocol) entsprechen (für Wissbegierige: Die Funktionsweise von SMTP wird in RFC 821 festgelegt, das etwa über `http://www.sendmail.org/rfc/0821.html` erhältlich ist). Im gängigen Administratorjargon wird ein Maildämon übrigens häufig MTA (Mail Transfer Agent) - im Gegensatz zum MUA (Mail User Agent), der Client, mit dem der Benutzer seine Email-Nachrichten verfaßt - genannt. Bevor wir zur Konfiguration von `sendmail` kommen, muß aber die Funktionsweise des Mailverkehrs erläutert werden.

Mailserver - `sendmail`

- über 5 Milliarden Emails täglich
- sendmail über 60% Marktanteil
- `http://www.sendmail.org`
- stabil, performant, flexibel
- lauscht auf Port 25
- kommuniziert über SMTP
- SMTP definiert in RFC 821
- Mail Transfer Agent

Folie 234

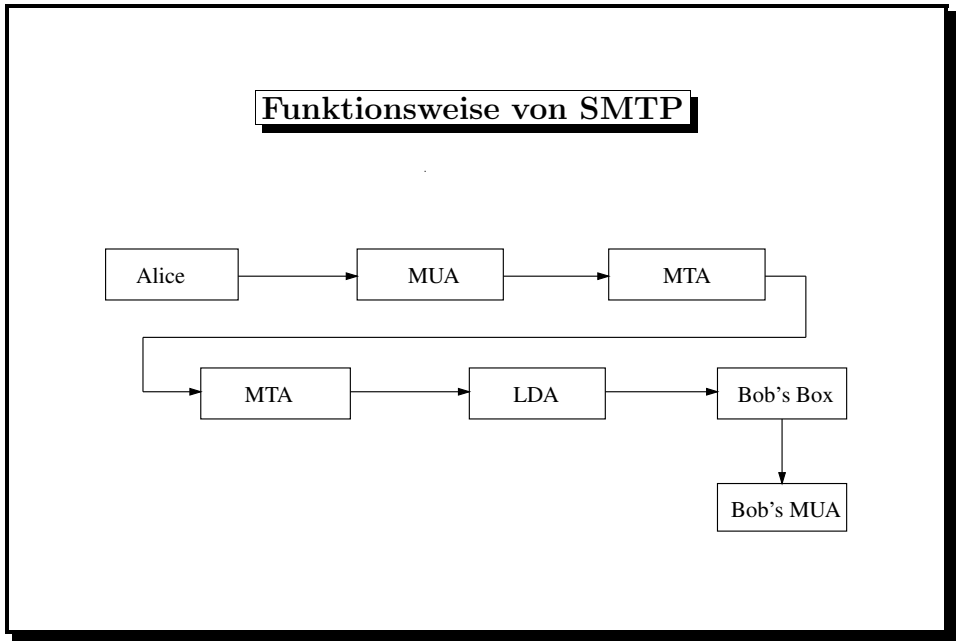
Funktionsweise

Ohne uns in die Untiefen der Protokollebene zu stürzen, wollen wir hier kurz den Weg einer Email-Nachricht vom Verfasser (Alice) zum Empfänger (Bob) nachvollziehen.

Alice öffnet ihren MUA (zB mutt, kmail oder pine), tippt dort ihre Nachricht und eine Empfängeradresse ein und teilt dem Programm mit, daß sie die Nachricht nun versenden möchte. Dieses verpackt den Text zusammen mit einem Header, der unter anderem Sender, Empfänger, Betreff, Datum und einige andere Informationen enthält, in das, was man gewöhnlich eine Email nennt. Sodann wird, je nach Konfiguration des MUA, auf unterschiedliche Weise - über den lokalen MTA oder über einen Zwischenmailserver (Smarthost) - eine Netzwerkverbindung auf Port 25 des Empfängers geöffnet und nach einer Anmeldeprozedur die Email auf den Zielrechner übertragen. Dort übergibt sie der MTA dem LDA (Local Delivery Agent), der die Email in das System-Mailverzeichnis legt (gewöhnlich `/var/spool/mail/`). Ein sehr populärer und mächtiger LDA ist `procmail`. Er kann auch zusätzlich verschiedene Dinge überprüfen, zB ob die empfangene Mail Spam ist, ob Mailanhänge Viren enthalten o.ä..

Bob loggt sich nun zum Lesen seiner Emails entweder direkt am Empfängerrechner ein oder lädt Mails mittels des POP3- oder IMAP-Protokolls vom Server auf seinen Rechner zuhause herunter.

Der Weg vom Sender-MTA zum Empfänger-MTA ist übrigens wesentlich komplexer als es hier den Anschein hat, der Pfad einer Email geht oft auch über mehr als 3-4 Rechner, etwa wenn der Zielrechner hinter einer Firewall steht und der Firewallserver SMTP-Anfragen von außen nach innen weiterleiten muß. Eine ähnliche Situation liegt vor, wenn man einen Rechner (MX-Host genannt) definiert, der Mails für ein Rechnernetz empfangen soll (was auch immer er dann genau tut, zB ob vom Senderrechner überhaupt Emails akzeptiert werden sollen), bevor sie am Zielort angelangen. Im allgemeinen sind aber solche Zwischenschritte für den Sender oder Empfänger transparent und durch das Ansehen der Email-Header nachvollziehbar.



Folie 235

Konfiguration
`sendmail` war bis vor einigen Jahre für seine sehr komplexe Konfiguration über die berühmt-berüchtigte Datei `/etc/sendmail.cf` gefürchtet (zur „Abschreckung“ findet sich auf Folie 237 ein Auszug einer `/etc/sendmail.cf` eines Produktionsservers). Heute wird üblicherweise nicht mehr diese Datei direkt bearbeitet, sondern mittels der Makrosprache `m4` aus dem File `/etc/mail/sendmail.mc`, das ein erheblich vereinfachtes Format hat, eine `sendmail.cf` erstellt.

Im Verzeichnis `/etc/mail/` liegen gewöhnlich noch einige andere Dateien, von denen der Großteil aber nur für fortgeschrittene Aufgaben eingesetzt wird. Lediglich `local-host-names`, in die alle Hostnamen des Mailservers eingetragen werden sollten, für die man zusätzlich zum eigentlichen Hostnamen Mail empfangen will (zB weil am Rechner ein Virtual Web Host definiert ist), und `access`, um bestimmten Rechnern oder Benutzern Zugang zum `sendmail`-Dämon zu ermöglichen oder verbieten.
Schließlich ist noch das File `/etc/aliases` zu nennen, in dem Empfängernamen definiert werden können, die an andere Email-Adressen weitergeleitet werden sollen (zB werden so gewöhnlich Emails für `webmaster` an `root` geschickt). Dies ist auch dann nützlich, wenn Benutzer ihren Account am Server aufgegeben haben und ihre Emails an eine neue Adresse weitergeleitet werden sollen. Auf diesem Wege kann man auch Mails für einen Empfänger auf mehrere Email-Adressen weiterleiten und so einfach Mailinglisten erstellen.

Achtung: Wenn man Änderungen an der `aliases` vornimmt, muß man das Programm `newaliases` ausführen, damit diese aktiv werden. Generell sollte man vor Änderungen in allen Konfigurationsdateien die jeweilige Manpage lesen und alle Modifikationen genau überprüfen, da `sendmail` bei ungültigen Einträgen in einem seiner Konfigurationsfiles meist den Start verweigert und das gerade bei einem so wichtigen Dienst vermieden werden muß.

`sendmail`-Konfiguration

- `/etc/sendmail.cf` komplex, undurchschaubar
- `/etc/mail/sendmail.mc` einfacher, übersichtlicher
- `/etc/mail/local-host-names` zusätzliche Hostnamen des Rechners, für die Mail empfangen werden soll
- `/etc/mail/access` Zugriffssteuerung auf Benutzer/Rechner-Ebene
- `/etc/aliases` Empfänger-Aliases

Folie 236

Beginn einer `sendmail.cf`

```
Cwlocalhost
Fw/etc/mail/local-host-names
CP.
DS
CO @ % !
C..
C[[
C{Accept}OK RELAY
Kresolve host -a<OK> -T<TEMP>
```

Folie 237

Beispiel `sendmail.mc`

```
include(‘../m4/cf.m4’)
VERSIONID(‘M4 Example Configuration’)dnl
OSTYPE(linux)dnl
FEATURE(nouucp)dnl
FEATURE(always_add_domain)dnl
define(‘LUSER_RELAY’,‘local:postmaster’)dnl
define(‘SMART_HOST’, mail.domain.at)dnl
MAILER(local)dnl
MAILER(smtp)dnl
```

Folie 238

Das `sendmail`-Paket enthält auch verschiedene Clientprogramme. Eines davon ist das eigentliche `sendmail`-Binary, das zum Versenden von Mails verwendet wird. Gleichzeitig enthält es, wenn bestimmte Optionen übergeben werden, auch den Programmcode für den Server-Dämon. Man kann übrigens mit `sendmail` Mails von der Kommandozeile aus verschicken, indem man die Ausgabe eines anderen Programms nach `sendmail` pipet und als Argument (mindestens) eine Mailadresse übergibt; also etwa:

```
echo "Hallo" | sendmail martin@mat.univie.ac.at
```

Ein besonders bei Problemen nützliches Hilfsprogramm ist `mailq`, mit dem man die Warteschlange für noch zu versendende Emails einsehen kann. Meist bleiben dort Mails hängen, bei denen zB der DNS-Name des Zielsystems ungültig ist. Diese Mails werden gewöhnlich nach einer bestimmten Wartezeit, in der alle paar Stunden der Versand wieder versucht wird, aus der Warteschlange entfernt und der Absender benachrichtigt.

Für eine genauere Beschreibung von `sendmail` verweisen wir angehende Postmaster auf jeden Fall zumindest an die diversen Manpages, die `sendmail`-Dokumentation, das Mail-Administrator-HOWTO und die ausgezeichneten Bücher [10] und [13] um den Überblick über dieses doch einigermaßen komplexe Programm zu behalten und bei Problemen „das richtige“ zu tun. `sendmail` führt auch eine hilfreiche Log-Datei, die bei Redhat Linux in `/var/log/maillog` zu finden ist und bei vielen Fehlern Aufschluß über die Ursachen bringen kann.

18 Netzwerksicherheit

Häufig hört man als Antwort auf Kritik über mangelnde Sicherheit von Computersystemen die rethorische Frage: „Was haben wir schon für wichtige Daten?“ oder: „Wir haben ohnehin eine Firewall!“ Im folgenden soll darauf eingegangen werden, warum diese Aussagen unüberlegt sind und wovor man sich schützen soll.

18.1 Allgemeines

Jedes Computersystem hat einen gewissen Erhaltungswert. Dieser kann sehr hoch sein, wie zB im Fall von gespeicherten sensiblen Daten oder Systemen deren Ausfall Geld oder Leben kostet, oder sehr niedrig sein. Er ist aber fast nie gleich null. Die Wiederherstellung eines Systems kostet zumindest ein bißchen Zeit. Des weiteren werden durch fahrlässig administrierte Computer oft andere Teile eines Computernetzes in Mitleidenschaft gezogen. Es gibt in Zeiten von automatischen Angriffsmechanismen (wie etwa den Internetwürmern Codered und Nimda) auch keinen Computer im Internet der für niemanden interessant ist. Automaten unterscheiden das nicht! Schlecht administrierte Computer könnten in Zukunft das Internet in seiner jetzigen Form unbenutzbar machen.
Hinter der Absicherung und dem Angriff auf ein Computersystem stehen in keiner Weise mystische Geheimnisse, wie oft suggeriert wird. Ganz im Gegenteil: Ein klares technisches Verständnis der Vorgänge und ein eher tabellarisches Wissen von bekannten Angriffspunkten verschiedener Betriebssysteme und Server ist von Nöten.

Allgemeines

Warum Sicherheit?

- Erhaltungswert des Systems
- Schutz vor Angriffsautomaten
- Andere nicht in Mitleidenschaft ziehen

Was ist bei der Absicherung wichtig?

- Ordentliche Administration
- Testen auf Sicherheitslöcher
- Gutes Verständnis der Netzwerktechnik

Folie 239

18.2 Updates

Typischerweise nutzen Angreifer aus dem Netz bekannte Fehler in Serversoftware aus. Dazu braucht es oft nur wenige bis keine besonderen Fähigkeiten. Wer sucht, findet im Internet Angriffswerkzeuge, die selbsttätig bekannte Fehler ausnutzen. Oft muß man solchen Angriffswerkzeugen nur sein Ziel sagen. Es soll schon vorgekommen sein, dass ein Administrator eines Unixsystems bei der Aufarbeitung eines Angriffs in den Logfiles die hilflosen Versuche eines - offenbar nur auf Windowssystemen versierten - Einbrechers vorgefunden hat, mit dem Befehl `dir` wenigstens ein sinnvolles Kommando abzugeben.
Weiters gibt es das Phänomen von Internetwürmern. Das sind autark handelnde Programme, die versuchen mit einprogrammierten Angriffen Computer zu knacken, sich auf diesen einzunisten und von dort aus weiterzuverbreiten.
Gegen derartige Angriffe gibt es nur ein Mittel: Das regelmäßige Updaten des Systems. Dies passiert am besten per täglichem Cronjob. Die häufig geäusserte Regel „Never change a running system“ ist hierbei ein unangebrachter Zugang. Auch Firewalls können einem Administrator das Update nicht ersparen.

Updates

- Distributoren beheben sicherheitskritische Fehler
- Schutz vor Angriffsautomaten und Script-Kiddies
- Am besten täglich und automatisch
- „Never change a running system“?

Folie 240

18.3 Sniffer

Das beste Passwort ist vollkommen wertlos, wenn man es im Klartext (also unverschlüsselt) über das Netz verschickt. Leider gibt es viele Programme bzw. Protokolle, die noch immer Passwörter im Klartext verschicken und trotzdem verwendet werden. Einige prominente Vertreter sind

- Telnet
- FTP (authentifiziert)
- POP
- HTTP (Logins auf Webseiten)
- SMB (Windows Freigaben)

Der letzte Punkt ist nur bedingt richtig, da in den neueren Versionen von Windows und Samba eine verschlüsselte Authentifizierung stattfindet kann. Für alle anderen Programme gibt es entweder ein Ersatzprogramm mit Verschlüsselung (Telnet ↔ Ssh, FTP ↔ SFTP, HTTP ↔ HTTPS) oder die Möglichkeit die Programme über sogenannte Ssh-Tunnel zu betreiben (POP).
Der Inhalt jedes Datenpaketes kann zumindest auf jedem Knoten (Router/Gateway) über den es läuft gelesen werden. Das können sehr viele Stationen sein (siehe Folie 241).
Im Beispielfall gehen also beim Klicken des „Senden und Empfangen“-Buttons des Mailprogramms der Username, das Passwort und der Inhalt aller übertragenen Mails im Klartext über 16 Computer.
Doch das sind bei weitem nicht die einzigen Computer, die mithören können. Ist ein Netzwerk per BNC-Kabel oder mit einem Hub zusammengeschlossen, so kann jeder Computer im Netzwerk den Datenverkehr aller anderen abhören. Und selbst in Netzwerken, die über einen Switch verbunden sind, kann jeder Computer im Netzwerk mit ein wenig mehr Aufwand den gesamten Verkehr abhören. (ARP spoofing, ARP table overflow am Switch, etc.)
Oft installiert ein Cracker, der sich Zugang zu einem Computer eines Netzes verschafft hat auf diesem einen Sniffer, der Benutzername/Passwort-Paare in eine Datei mitloggt. Diese Datei kann er entweder bei Zeiten abholen oder sich automatisch,

anonym und verschlüsselt in irgend ein öffentliches Forum im Internet posten. Mit dieser Methode kann man in kürzester Zeit viele Logins von vielen Computern - auch außerhalb des kompromitierten Netzwerks - beschaffen. Und wenn ein Angreifer einen Account eines Systems kennt, dann ist es für ihn schon sehr viel leichter. Hätte in diesem Fall ein Administrator auf den root-Account über ein unverschlüsseltes Protokol zugegriffen, so wäre der Angriff schon perfekt. Deshalb sollte ein Administrator niemals unverschlüsselt über das Netz auf den root-Account zugreifen. Ein `su -` innerhalb einer Telnetsession ist dabei natürlich um nichts besser.
Wir werden uns nun am einem Beispiel ansehen, wie einfach es ist, Klartextpasswörter mitzulesen. Das Programm, das wir dazu verwenden heißt `ngrep`. Wir lesen damit den Benutzernamen und das Passwort aus einer authentifizierten FTP-Session aus (siehe Folie 242).

`traceroute www.gmx.de`

```
1  center2-sued-wien.chello.at (10.34.11.2)  17.078 ms  19.695..
2  213.47.218.249 (213.47.218.249)  8.873 ms  38.098 ms  3.737..
3  at-vie-rd-03-ge-2-1.chellonetwork.com (213.46.173.21)  4.13..
4  at-vie-rc-01-ge-2-1.chellonetwork.com (213.46.160.129)  26...
5  * 213.46.160.113 (213.46.160.113)  27.846 ms  8.483 ms
6  uk-lon-rc-01-pos-5-0.chellonetwork.com (213.46.160.117)  62..
7  213.46.160.137 (213.46.160.137)  86.378 ms  83.870 ms  67.9..
8  de-fra-rc-02-pos-30.chellonetwork.com (213.46.160.90)  78.4..
9  de-fra-rc-01-pos-4-0.chellonetwork.com (213.46.160.85)  60...
...
14  atm-10102.gw-backbone-a.muc.schlund.net (212.227.112.118) ..
15  to-gmx.schlund.net (212.227.112.42)  139.813 ms  87.667 ms..
16  www.gmx.net (213.165.65.100)  86.669 ms  97.269 ms *
```

Folie 241

```
ngrep -qd lo port 21

T 192.168.0.10:21 -> 192.168.0.10:41833 [AP]
220 ProFTPD 1.2.4 Server (Debian) [carla.doppler]..

T 192.168.0.10:41833 -> 192.168.0.10:21 [AP]
USER ferdinand..

T 192.168.0.10:21 -> 192.168.0.10:41833 [AP]
331 Password required for ferdinand...

T 192.168.0.10:41833 -> 192.168.0.10:21 [AP]
PASS w8h7RLNZ..

T 192.168.0.10:21 -> 192.168.0.10:41833 [AP]
230 User ferdinand logged in...
```

Folie 242

18.4 Portscanner

Ein wichtiger Punkt für die Sicherheit eines Systems ist es, keine nicht benötigten - und damit meist nicht administrierten - Dienste laufen zu lassen. Eine Methode das festzustellen, ist direkt am untersuchten Computer mit `netstat` oder `lsof` von Servern belegte Ports aufzulisten (siehe Folie 243).
Das heißt aber nicht unbedingt, dass ein anderer Rechner die gleichen Services sieht. Einerseits können Ports für andere Computer mit dem TCP-Wrapper oder einem Paketfilter unsichtbar gemacht werden, andererseits könnte - im schlimmsten Fall - der Computer bereits gecrackt sein und das `netstat`-Kommando verändert worden sein.
Daher sollte man offene Ports auch mit einem Portscanner von einem anderen Computer aus überprüfen. Ein Portscanner versucht im wesentlichen nichts anderes, als sich auf allen möglichen Ports mit seinem Ziel zu verbinden und meldet dann, auf welchen Ports dies möglich war. Oftmals hinterlegt ein erfolgreicher Angreifer ein Backdoor, um zu einem späteren Zeitpunkt wieder leicht in das System einsteigen zu können. Oft sind Backdoors ganz einfache Server, die auf einem hohen Port auf eine Verbindung warten und gegebenenfalls eine root-Shell liefern. Auch zum finden solcher Backdoors eignen sich Portscanner.
WARNUNG! Portscans sollte man nur auf die Rechnern loslassen, die man selbst administriert, um Sicherheitslücken aufzuspüren. Nur böse Buben scannen fremde Computer, um Angriffe vorzubereiten. Ein Portscan ist auch sehr leicht am angegriffenen Rechner nachzuweisen und unter normalen Bedingungen lässt sich auch der Angreifer feststellen.
Wir schauen uns nun einen der verbreitetsten Portscanner, nämlich `nmap`, an. Wir werden nur ein elementares Beispiel sehen. Die lesenswerte Manpage von `nmap` lässt aber schon ahnen, dass das Spiel hier noch lange nicht am Ende ist (siehe Folie 244).
Ein weiteres sehr interessantes Werkzeug zur Untersuchung von Computern und deren Services ist `nessus`. Es versucht nicht nur eine Verbindung zu allen Ports zu öffnen, sondern auch festzustellen, welcher Dienst hinter diesem Port zu finden ist. Am Ende der Prozedur wird ein Bericht erstellt, der auf Sicherheitsmängel hinweist (siehe Folie 245). Zu Testzwecken haben wir in diesem Fall einen Ssh-Server anstatt wie üblich auf Port

22, auf Port 9876 laufen lassen. An diesem Beispiel erkennt man auch leicht, dass das „Verstecken“eines Services auf einem untypischen Port keinerlei Sicherheit bringt.

netstat -l

```
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address     Foreign Address  State
tcp        0      0 *:pop3           *:*              LISTEN
tcp        0      0 *:auth           *:*              LISTEN
tcp        0      0 zulu:domain      *:*              LISTEN
tcp        0      0 localhost:domain *:*              LISTEN
tcp        0      0 *:ssh            *:*              LISTEN
tcp        0      0 *:ipp            *:*              LISTEN
tcp        0      0 *:smtp           *:*              LISTEN
udp        0      0 *:1037           *:*
udp        0      0 *:10000          *:*
udp        0      0 zulu:domain      *:*
udp        0      0 localhost:domain *:*
```

Folie 243

`nmap 192.168.0.13`

```
Starting nmap V. 2.54BETA30 ( www.insecure.org/nmap/ )
Interesting ports on zulu.doppler (192.168.0.13):
(The 1541 ports scanned but not shown below are in state: closed)
Port       State       Service
22/tcp     open        ssh
25/tcp     open        smtp
53/tcp     open        domain
110/tcp    open        pop-3
113/tcp    open        auth
631/tcp    open        cups
10000/tcp  open        snet-sensor-mgmt

Nmap run completed -- 1 IP address (1 host up) scanned in 1 second
```

Folie 244

`nessus`

Problems regarding : unknown (9876/tcp)

Security holes :

```
You are running a version of OpenSSH which is older than 3.0.2.

Versions prior than 3.0.2 are vulnerable to an enviroment
variables export that can allow a local user to execute
command with root privileges.
This problem affect only versions prior than 3.0.2, and when
the UseLogin feature is enabled (usually disabled by default)

Solution : Upgrade to OpenSSH 3.0.2 or apply the patch for prior
...
```

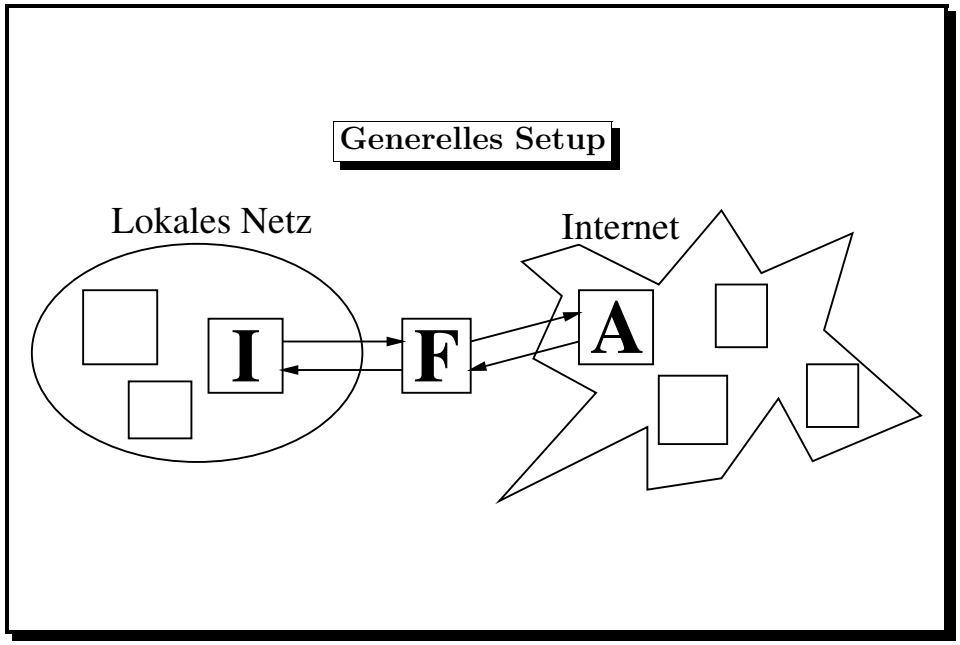
Folie 245

18.5 Firewalls

Eine Firewall ist ein Mechanismus zum Schutz eines oder mehrerer Computer vor unerwünschten Zu- und Angriffen aus dem Netz. Es gibt zwei Grundtypen von Firewalls:

- Proxy Server
- Paketfilter

Wie auch beim Begriff „Server“ wird der Begriff „Firewall“ sowohl für Hardware als auch für Software verwendet. Oft ist eine Firewall ein eigener Computer, der einerseits im internen Netz und andererseits im Internet hängt. Die Firewall soll vordefinierte Verbindungen zwischen Computern innerhalb und außerhalb der Firewall ermöglichen, unerwünschte Zugriffe aber unterbinden. In Weiteren wird **I** einen Computer innerhalb, **A** einen Computer außerhalb und **F** die Firewall selbst bezeichnen.



Folie 246

18.5.1 Proxy Server

Bevor wir uns den Paketfiltern zuwenden, soll hier kurz auf die Funktionsweise und die Arten von Proxy Servern eingegangen werden. Es ist also jetzt **F** ein Proxy Server. Ist ein Netz via Proxy Server an das Internet angebunden, so besteht für einen Computer **I** keine Möglichkeit eine direkte Verbindung zu einem Computer **A** aufzubauen. Anstelle einer solchen Verbindung treten zwei Verbindungen, einerseits von **I** nach **F** und andererseits von **F** nach **A**. Die Software am Rechner **I** muß für die Verwendung des Proxy Servers konfiguriert sein und stellt damit Anfragen nie an **A** selbst, sondern an **F**. **F** verbindet sich mit **A** und liefert das Resultat an **I** zurück.
Die Sicherheitsmechanismen in Proxy Servern erlauben es, Verbindungen auf einige Dienste einzuschränken (zB Web, SSH,...), eine Benutzerauthentifizierung durchzuführen, sämtlichen Datenverkehr mitzuloggen und vieles mehr.
Proxy Server sind in zwei Typen unterteilt:

- Application Proxy
- SOCKS Proxy

Application Proxies (zB *squid*) müssen jedes Application Protocol, dass sie unterstützen verstehen. So kann *squid* nur Web- und FTP-Traffic verarbeiten. Eine Secure Shell-Verbindung kann man über *squid* nicht weiterleiten. Der Vorteil solcher Proxies ist, dass sie sich auch zum Cachen oder zum Filtern von Inhalten eignen.
SOCKS Proxies (zB *dante*) arbeiten auf der Schicht von TCP und UDP. Diese verstehen also die Protokolle des Application Layers nicht und können damit auch nicht zu Caching Zwecken verwendet werden. Der Vorteil ist, dass (fast) beliebige TCP- und UDP-Anwendungen verarbeitet werden können.

18.5.2 Paketfilter

Ein völlig anderer Zugang ist es, auf dem Computer **F** einen Paketfilter zu verwenden. Hierbei werden Verbindungen von **A** nach **I** - wie wenn **F** ein gewöhnlicher Router wäre - direkt durchgeführt. Das hat auch den Vorteil, dass keinerlei Konfiguration des Rechners **A** vonnöten ist. Der Paketfilter auf **F** liest

den Datenverkehr auf verschiedenen Protokollschichten mit, und entscheidet ob das Datenpaket weitergeleitet oder verworfen wird. Im Folgenden eine unvollständige Auflistung von Eigenschaften von Paketen verschiedener Schichten, welche Paketfilter kennen (siehe Folie 247).
Seit Version 2.0 ist im Linux Kernel ein Paketfilter eingebaut. Der diesbezügliche Code wurde seither in jedem neuen Majorrelease geändert. Dementsprechend unterscheiden sich auch die Commandlinetools der verschiedenen Versionen.

Kernel	Komando
2.0	`ipfwadm`
2.2	`ipchains`
2.4	`iptables`

Wir wenden uns nun der Verwendung der iptables zu. Ein Paket durchläuft verschiedene Chains (Ketten) von Regeln (Rules). Drei solcher Chains sind immer vorhanden: INPUT, OUTPUT und FORWARD Chain. Wir betrachten im folgenden die Chains unserer Firewall **F**. Ein Paket, das vom Rechner **I** oder **A** kommt und zum Rechner **F** will, durchläuft die INPUT Chain. Ein Paket, dass am Weg von **I** nach **A** die Firewall **F** trifft, durchläuft die FORWARD Chain. Ein Paket, dass von **F** nach **I** oder **A** geht, durchläuft die OUTPUT Chains. Die Situation auf der Firewall **F** wird am besten durch folgendes Diagramm beschrieben, welches für die Kernelserie 2.4 gilt (siehe Folie 248).
Wir betrachten nun den Werdegang eines Paketes, wenn es eine Chain durchläuft. Der erste Befehl, den wir kennenlernen, listet alle Regeln der INPUT Chain auf (siehe Folie 249).
Dies zeigt uns nun eine Liste aller Regeln, die die INPUT Chain bilden. Ein Paket, das versucht diese Chain zu durchlaufen wird der Reihe nach mit diesen Regeln verglichen. Entspricht ein Paket in allen Punkten einer Regel, so wird das zu dieser Regel gehörige Target auf das Paket angewendet. Targets können einerseits selbstdefinierte Chains sein oder aber eingebaute Targets, von welchen wir im folgenden einige anführen (siehe Folie 250).
In obigem Listing ist das immer ACCEPT. Das Paket darf also passieren, wenn eine der Regeln zutrifft. Wichtig ist zu bemerken, dass, sobald eine Regel zutrifft und ein Target auf das Paket angewendet wird, keine weitere Regel in der Chain mit

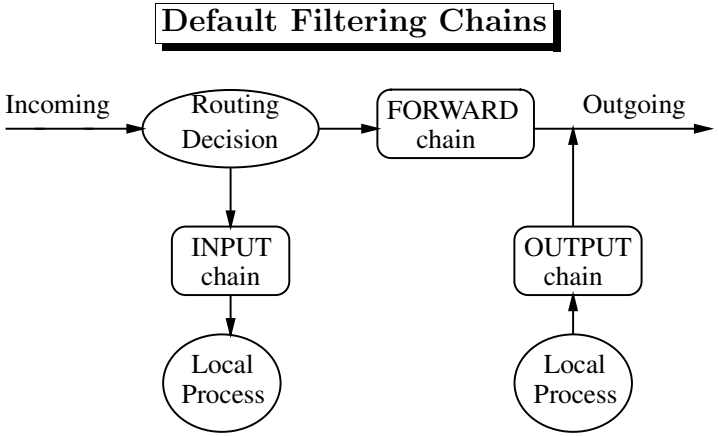
dem Paket verglichen wird. Trifft keine der Regeln einer Chain auf das Paket zu, so wird die Policy auf dieses angewendet. In unserem Fall wird also jedes Paket, auf das keine Regel zutrifft, abgelehnt. Einen etwas wortreicheren Output liefert folgendes Kommando (siehe Folie 251).
Hier sehen wir nun auch Zähler für die Anzahl bzw. die Datenmenge der Pakete, auf die die entsprechende Regel zugetroffen hat. Diese Zähler sind einerseits praktisch zum Messen des Datenverkehrs, andererseits lässt sich anhand dieser Zähler oft auch herausfinden, wo - und damit warum - ein Paket nicht gewünschten Weg ging.
Zum Einfügen einer neuen Regel ans Ende einer Chain verwendet man den Befehl
`# iptables -A` *Chain* `...`.
Da die Reihenfolge der Regeln relevant ist, gibt es auch die Möglichkeit mit
`# iptables -I` *Chain* `[`*number*`] ...`,
eine Regel in eine bestimmte Zeile einzufügen. Die oben beschriebene Policy einer Chain wird mit dem Befehl
`# iptables -P` *Chain target*
gesetzt (siehe Folie 252).
Wir listen nun einige der Optionen von `iptables` auf, insbesondere einige, welche die Paketeigenschaften in der Tabelle auf Folie 247 betreffen (siehe Folie 253).
Besonders hervorheben möchten wir die `--state` Option. Mit dieser Option kann man Pakete behandeln, die zu einer existierenden Verbindung gehören. Diesen Umstand nutzt auch „Rusty's Really Quick Guide to Packet Filtering“, den wir hier in leicht modifizierter Form wiedergeben möchten (siehe Folie 254). Rusty Russel ist der Linux IP Firewall Maintainer.
Unter der Voraussetzung, dass `eth0` (also die erste Ethernetkarte im Computer) mit dem Internet verbunden ist, lässt diese Firewall jede Verbindung vom lokalen Netz ins Internet zu, verbietet aber im Gegenzug die umgekehrte Richtung vollständig.

Eigenschaften von Datenpaketen

Layer	Protocol	Eigenschaft
Network Access	Ethernet	MAC Adresse
Internet	IP	Source IP, Destination IP
		Incoming-/Outgoing-Interface
	ICMP	ICMP Type
Transport	TCP	Port, Flags (zB SYN),
		Connection Tracking
	UDP	Port, Connection Tracking
Application	FTP	Zugeordnete Datenverbindung

Folie 247

Default Filtering Chains



Folie 248

Listing einer Chain

```
[root@milch root]# iptables -L INPUT
Chain INPUT (policy DROP)
target     prot opt source     destination
ACCEPT     all  --  anywhere   anywhere
ACCEPT     all  --  anywhere   anywhere         state RELATED,ESTABLISHED
ACCEPT     all  --  phobos     milch
ACCEPT     tcp  --  anywhere   milchtcp dpt:ssh
```

Folie 249

Targets

Target	Beschreibung
ACCEPT	Das Paket wird akzeptiert.
DROP	Das Paket wird verworfen.
REJECT	Das Paket wird verworfen, dem Sender wird ein ICMP 'port unreachable' Paket zurückgesandt.
LOG	Ein Eintrag, der das Paket beschreibt, wird in ein Logfile geschrieben.
MASQUERADE	siehe 18.5.4

Folie 250

Langes Listing einer Chain

```
[root@milch root]# iptables -v -L INPUT
Chain INPUT (policy DROP 8180 packets, 2125K bytes)
 pkts bytes target  prot opt in   out  source    destination
 3662  468K ACCEPT  all  --  lo   any  anywhere  anywhere
 130K   67M ACCEPT  all  --  any  any  anywhere  anywhere   state REL...
    0     0 ACCEPT  all  --  any  any  phobos    milch
    1    60 ACCEPT  tcp  --  any  any  anywhere  milchtcp dpt:ssh
```

Folie 251

Neue Regel Einfügen

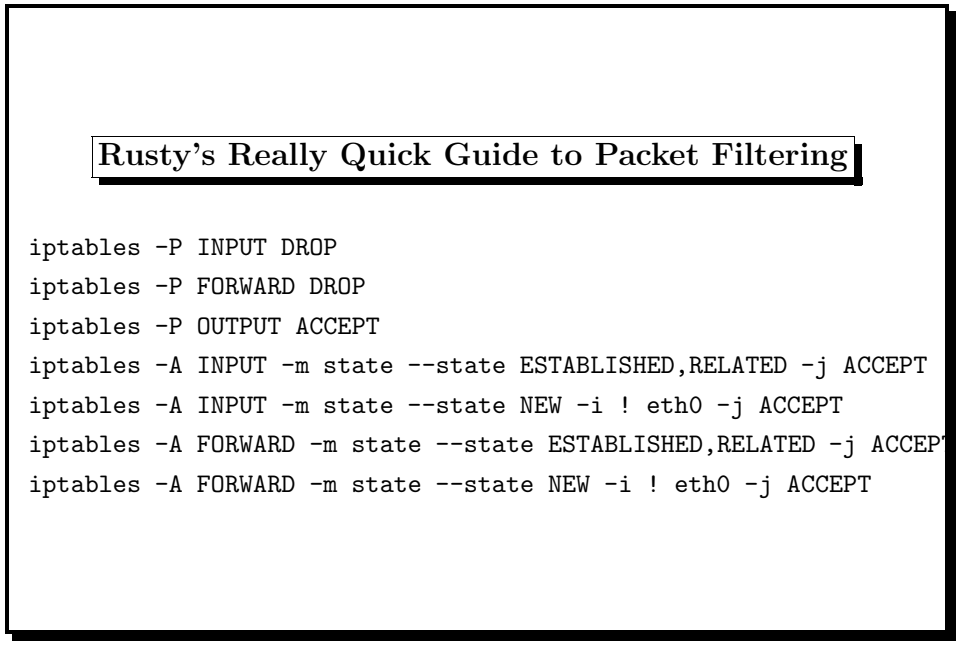
```
[root@milch root]# iptables -A INPUT -p tcp -s 131.130.16.0/24 --sport
     1024:65535 -d milch --dport finger -i eth0 -j ACCEPT
[root@milch root]# iptables -v -L INPUT
Chain INPUT (policy DROP 8180 packets, 2125K bytes)
.. target  prot opt in   out  source    destination
.. ACCEPT  all  --  lo   any  anywhere  anywhere
.. ACCEPT  all  --  any  any  anywhere  anywhere   state REL...
.. ACCEPT  all  --  any  any  phobos    milch
.. ACCEPT  tcp  --  any  any  anywhere  milchtcp dpt:ssh
.. ACCEPT  tcp  --  eth0 any  131.130.16.0/24
     milchtcp spts:1024:65535 dpt:finger
```

Folie 252

iptables Optionen (Auszug)

`--mac-source` *MAC*	MAC Quelladresse
`-s` *IP*	IP Quelladresse
`-d` *IP*	IP Zieladresse
`-i` *Interface*	Eingehendes Interface
`-o` *Interface*	Ausgehendes Interface
`-p` *Protocol*	`tcp`, `udp`, `icmp` oder `all`
`--icmp-type` *Typname*	ICMP Typ
`--source-port` *Port*	TCP- bzw. UDP-Quellports
`--destination-port` *Port*	TCP- bzw. UDP-Zielports
`--syn`	TCP-Verbindungaufbau
`--state`	Status einer Verbindung

Folie 253



Folie 254

18.5.3 Paketfilter stoppen und starten

Nachdem der Aufruf des Kommandos `iptables` direkt in die Chains im Kernel schreibt, gehen diese bei einem Reboot verloren. Um die Chains bei einem Reboot wiederherzustellen, sollte man die `iptables` Kommandos in ein Startscript geschrieben werden. Wir werden hier den Standardweg von Redhat durchgehen.
Hierbei schreibt man ein Shellscript, das die Firewall in den gewünschten Zustand bringt und speichert es in `/etc/sysconfig/iptables.sh`. Am Ende des Scripts sollte die Zeile

```
iptables-save > /etc/sysconfig/iptables
```

stehen. Beim Ausführen des Scripts bewirkt diese Zeile, dass die aktuellen Regeln in die Datei `/etc/sysconfig/iptables` gespeichert werden, von wo sie das Script `/etc/init.d/iptables` beim Booten einliest.

Redhat `iptables` Startscripts

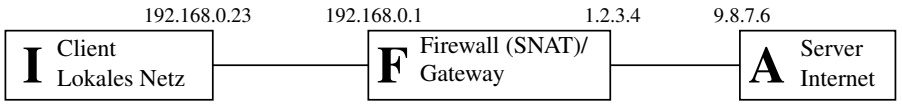
```
# vim /etc/sysconfig/iptables.sh
# chmod 755 /etc/sysconfig/iptables.sh
# /etc/sysconfig/iptables.sh
# chkconfig --add iptables
# /etc/init.d/iptables restart
Flushing all current rules and user defined chains:   [  OK  ]
Clearing all current rules and user defined chains:   [  OK  ]
Applying iptables firewall rules:                     [  OK  ]
```

Folie 255

18.5.4 Masquerading (Source NAT)

Oft ist man vor das Problem gestellt, mehreren Computern einen Internetzugang zu ermöglichen, obwohl man nur eine offizielle IP Adresse zur Verfügung hat (zB via ein Modem). Das lässt sich erreichen, indem man in unserem Standardbeispiel am Rechner **F** einen Proxy Server oder aber IP-Masquerading bzw SNAT (Source Network Address Translation) betreibt. **F** wird dann oft als masquerading Gateway bezeichnet.
Dabei werden bei allen IP-Paketen, die von einem internen Computer **I** über den Gateway **F** ins Internet gehen, die IP-Quelladressen auf die im Internet gültige IP-Adresse des Gateways umgeschrieben, sodass der Server **A** glaubt, mit **F** zu kommunizieren. Bei den Antwortpaketen von **A** schreibt der Gateway **F** die IP-Zieladressen wieder auf die des Computers **I** um, sodass dieser die Antwort erhält. Für den Computer **I** ist das Verfahren transparent, das heißt er glaubt direkt mit **A** zu sprechen (siehe Folie 256).
Hier hat Rusty Russel sich selbst übertroffen und die Minimalkonfiguration des Paketfilters auf der Firewall **F** extrem kurz beschrieben (siehe Folie 257). Es wird davon ausgegangen, dass die Firewall über ein Modem (`ppp0`) ans Internet angebunden ist. Diese Minimalkonfiguration beinhaltet keinerlei Filterregeln zum Verbot bestimmter Verbindungen. Um die Firewall gegen äußere Rechner **A** abzuschotten, sollte man dieses Kochrezept mit dem der Folie 254 verbinden. Die Computer innerhalb der Firewall genießen bei dieser Technik automatisch einen recht hohen Schutz, da sie keine im Internet gültigen IP-Adressen haben und somit aus dem Internet nicht erreichbar sind.
Durch laden des Kernelmoduls `iptable_nat` stehen drei weitere Chains zur Verfügung: PREROUTING, POSTROUTING und OUTPUT. Diese lassen sich mit dem `iptables`-Kommando unter Angabe der Option `-t nat` bedienen. Eine Auflistung dieser drei Chains erhält man also mit
`# iptables -t nat -L`.
Für Masquerading ist ausschließlich die POSTROUTING Chain von Belang.

Masquerading



IP-Header: Paket von I nach A	S: 192.168.0.23 D: 9.8.7.6	S: 1.2.3.4 D: 9.8.7.6
IP-Header: Paket von A nach I	S: 9.8.7.6 D: 192.168.0.23	S: 9.8.7.6 D: 1.2.3.4

Folie 256

Rusty's Three Line Guide to Masquerading

```
modprobe iptable_nat
iptables -t nat -A POSTROUTING -o ppp0 -j MASQERADE
echo 1 > /proc/sys/net/ipv4/ip_forward
```

Folie 257

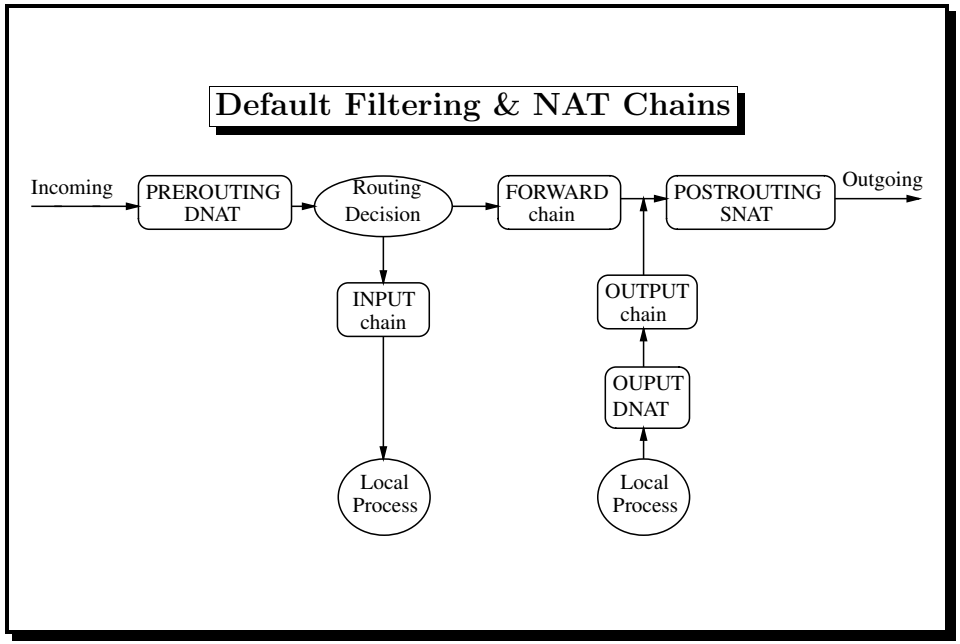
18.5.5 Portforwarding (Destination NAT)

Wie zuvor besprochen kann ein Computer **I** im lokalen Netz von aussen nicht erreicht werden. Was aber, wenn man zB einen Webserver betreiben will. Man könnte diesen auf der Firewall **F** betreiben. Das wird meist aber nicht gemacht, da es die Sicherheit der Firewall unter Umständen kompromitiert. Meist geht man folgenden Weg: Auf der Firewall laufen keinerlei Dienste ausser Ssh zu administrativen Zwecken. Der Webserver läuft am Rechner `I` im masquierten Netz. Kommt nun eine Anfrage an die Firewall **F** auf Port 80, so wird diese zum Computer `I` weitergeleitet. Die Antwort von `I` leitet **F** zurück an `A`. Dieses Verfahren nennt man Portforwarding oder DNAT (Destination Network Address Translation). Der anfragende Computer `A` hat dabei den Eindruck mit der Firewall `F` zu kommunizieren.
Wir werden uns nun die Regel für den beschriebenen Fall anschauen. Portforwarding findet in der PREROUTING Chain statt (siehe Folie 258).
Zum Abschluß eine Übersicht über die Filter- und NAT-Chains und wie sie durchlaufen werden (siehe Folie 259).

Webserver Portforwarding

```
modprobe iptable_nat
iptables -t nat -A PREROUTING -p tcp --dport www -j DNAT
   --to-destination I
echo 1 > /proc/sys/net/ipv4/ip_forward
```

Folie 258



Folie 259

18.5.6 Wovor schützt eine Firewall?

Nachdem wir nunmehr einen technischen Überblick über die Arten und Vorgehensweisen von Firewalls gegeben haben, können wir die Schutzwirkung abschätzen. Grundsätzlich ist anzumerken, dass eine Firewall in keiner Weise ein angebotenes Service schützt. Wird ein Webserver betrieben, so muß er auch erreichbar und damit von der Firewall uneingeschränkt sein. Der Webserver selbst (das Programm auf Port 80) ist in diesem Fall mit genauso angreifbar wie ohne Firewall. Auch vor Viren, die Personen im lokalen Netz auf ihre Computer per Email oder Web herunterladen, bringt eine Firewall keinerlei Schutz.
Eine Firewall kann aber ein Service, das nur im lokalen Netz angeboten werden soll, vor Zugriffen von aussen schützen. Auch kann damit verhindert werden, dass Computer im lokalen Netz unerwünschter Weise Services (oder auch Backdoors) nach aussen anbieten. Und man kann damit auch Teile des Internets für die Benutzer im lokalen Netz sperren.
Der Aufwand des Administrator steigt aber exponentiell mit der Komplexität der Firewall. Starke Einschränkungen führen häufig auch zu unerwünschten Behinderungen. Wenn keine besonderen Anforderungen an die Firewall gestellt werden, sollte man das Regelwerk so schmal wie möglich halten.

Wovor schützt eine Firewall?

JA

- Unerwünschte Server im lokalen Netz
- Zugriff auf Services für den internen Bereich
- Unerwünschte Zugriffe von Benutzern auf Internetdienste
- ...

NEIN

- Angriffe auf angebotene Services
- Viren per Email oder Web
- ...

Folie 260

19 Samba

Das Samba Paket bietet eine Implementation des SMB (Server Message Block) Protokolls für Unix und andere Plattformen, die so in eine MS-Windows Netzwerkumgebung eingebunden werden können. Wir besprechen hier detailliert sowohl das SMB-Protokoll, als auch die Konfiguration von Samba unter Linux.

Im folgenden wird der Begriff Windows NT (oder kurz NT) synonym für die Familie der aus Windows NT abgeleiteten Betriebsysteme verwendet und steht somit für Windows NT, Windows 2000 und Windows XP.

Was ist Samba?
Samba integriert einen Unix Rechner in die Windows Netzwerkumgebung (durch Implementation des SMB (Server Message Block) Protokolls). Genauer gesagt lässt Samba jeden Unixrechner in der Netzwerkumgebung von Windows erscheinen und erlaubt Datei- und Druckfreigaben zu erstellen. Das heißt, unter Unix vorhandener Plattenplatz kann ganz normal unter Windows genutzt werden, und unter Unix vorhandene Drucker kann man als Netzwerkdrucker unter Windows ansteuern. Darüber hinaus bietet Samba viele Dienste, die sonst nur von Windows NT geleistet werden. Dazu gehören:

- **WINS Server** (Windows Namensauflösung)
- **Computersuchdienst**
- **Logon Server** für Windows 95/98
- **PDC** (NT Primary Domain Controller)

Um Samba zu verstehen, müssen wir zunächste einige Netzwerkfunktionalitäten und Netzwerkprotokolle unter Windows erkären.

Was ist Samba?

- Der Linux-Rechner „erscheint“ in der Netzwerkumgebung der Windows Maschinen
- Linux kann als Fileserver bequemen Zugriff von Windows aus zulassen
- Der/die Drucker des Linux Rechners können von Windows aus benutzt werden
- Verhält sich wie ein echter Windows NT Server

Folie 261

19.1 NetBIOS

Sobald Windowsrechner Dateisysteme austauschen, sich gegenseitig in der Netzwerkumgebung sehen oder Drucker freigeben, funktioniert die Kommunikation über NetBIOS. NetBIOS ist eine reine Softwareschnittstelle zur Kommunikation von Rechnern, die Programmen unterschiedliche Dienste zur Kommunikation zur Verfügung stellt.
NetBIOS wurde entworfen, um in kleinen, lokalen Netzen Kommunikation zu ermöglichen. Dabei lag der Schwerpunkt des Entwurfs auf der Einfachheit der Anwendung. Auf Skalierbarkeit und die Andwendung in Weitverkehrsnetzen wurde beim Design nicht geachtet. Die Kommunikation mit NetBIOS wurde in drei Teilbereiche aufgeteilt, in den Namensdienst, den Datagramm- und den Sitzungsdienst.

- **Namensdienst** Im Rahmen des Namensdienstes sind die Rechner in der Lage, sich gegenseitig im Netz zu identifizieren. Es sei an dieser Stelle betont, dass der NetBIOS-Namensdienst nichts mit der Anzeige in der Netzwerkumgebung zu tun hat. Der Computersuchdienst, der für die Netzwerkumgebung zuständig ist, hängt jedoch sehr stark von einem korrekt funktionierenden Namensdienst ab.
- **Datagrammdienst** Betrachtet man die Rechnerkommunikation auf dem Netz, so sieht man, dass die versendeten Daten in einzelne Pakete aufgeteilt werden. Diese einzelnen Pakete werden dann vom Netz nach bestem Bemühen an einen Zielrechner ausgeliefert. Geht ein Paket verloren, kann man nichts machen, man bekommt unter Umständen nicht einmal eine Benachrichtigung darüber, dass etwas nicht stimmt. Aufeinander folgende Pakete können in vertauschter Reihenfolge beim Empfänger ankommen. Es kann sogar sein, dass Pakete auf dem Weg dupliziert werden, also mehrfach ankommen. Diese Unzuverlässigkeit des Netzes wird durch den Datagrammdienst an die Benutzerprogramme weitergegeben. Der Datagrammdienst hat jedoch nicht nur Nachteile. Zwei Vorteile sind der geringe Aufwand, mit dem Pakete verschickt werden können, und die Möglichkeit, ein Datagramm an mehrere Rechner gleichzeitig zu verschicken. Die Anwendung muss selbst entscheiden, wie sie mit der Unzuverlässigkeit des Dienstes klarkommt.

- **Sitzungsdienst** Die Unzuverlässigkeit des Netzes ist für bestimmte Applikationen wie Dateitransfer oder Terminalanwendungen nicht akzeptabel. Wenn man eine Datei überträgt, möchte man sicher sein, dass die Datei komplett und korrekt übertragen wurde. Für diese höheren Anforderungen wurde der Sitzungsdienst entworfen. Zwei Rechner vereinbaren eine NetBIOS-Sitzung. Die Daten, die über diese Verbindung übertragen werden, kommen auf jeden Fall an, und zwar in der richtigen Reihenfolge. Können Daten einmal nicht übertragen werden, so erhält die versendende Applikation eine Fehlermeldung. Die Applikation kann nun versuchen, die abgebrochene Sitzung neu aufzubauen. Dieser Zuverlässigkeit steht ein erhöhter Aufwand beim Sitzungsauf- und -abbau gegenüber.

Zwei Rechner, die kommunizieren wollen, müssen sich zunächst gegenseitig identifizieren. NetBIOS sieht hierfür bis zu 16 Zeichen lange Namen vor. Jede Applikation kann für sich beliebig viele Namen reservieren und unter einem dieser Namen Verbindungen aufbauen und Daten austauschen. Diese Reservierung von Namen gilt sowohl für Server, die vom Netz aus erreichbar sein müssen, als auch für Clients, die Server im Netz erreichen wollen, da Server wissen müssen, wohin die Antworten gehen müssen.
Zwei Anwendungen wollen nun per NetBIOS miteinander kommunizieren. Dazu muss zunächst der Server seine Bereitschaft kundtun, Verbindungen entgegenzunehmen. Dazu meldet er sich im Netz mit seinem Namen an. Diese Anmeldung geschieht per Broadcast, so dass alle im Netz mithören können. Jeder Rechner ist frei, beliebige Namen im Netz für sich zu beanspruchen, sofern diese noch nicht belegt sind. Eine Reservierung geschieht also, indem ein Rechner per Broadcast ankündigt, dass er unter einem bestimmten Namen erreichbar ist. Dann wartet er auf Protest. Beklagt sich niemand, schickt er eine zweite Reservierung und wartet wieder. Nach der dritten Reservierung ist der Rechner ausreichend sicher, dass kein anderer den Namen bereits für sich eingenommen hat, und sieht ihn als für sich reserviert an.
Wenn nun ein Client mit einem Server reden möchte, dann muss er sich wie der Server einen eindeutigen Namen „ausdenken“ und im Netz reservieren. Das Verfahren dazu ist identisch. Zusätzlich

muss der Client jedoch die MAC-Adresse des Servers herausbekommen. Die Mechanismen, wie dies geschieht, hängen davon ab, wie NetBIOS implementiert ist.
NetBIOS kann mit unterschiedlichen Protokollen implementiert werden. NetBEUI, IPX und TCP/IP sind drei heute verwendete Protokolle, wobei für Neuinstallationen TCP/IP das bevorzugte Protokoll sein sollte. (Samba ist ausschließlich in der Lage, NetBIOS über TCP/IP zu benutzen.) Der Ablauf der Namensauflösung soll an einem Beispiel verdeutlicht werden.
Auf einem Client soll eine Verbindung zu dem Server `pdc` aufgebaut werden. Direkt erreicht man dies, indem man in der Taskleiste Start → Ausführen → \\`pdc` eingibt.
Bei TCP/IP muss der Client die IP-Adresse des Servers herausfinden. Dies geschieht wie bei den anderen Protokollen per Broadcast im lokalen Netz. IP-Router können nicht angewiesen werden, die Anfragen per Broadcast in alle angeschlossenen Netze weiterzuleiten. Aus diesem Grund gibt es hier andere Mechanismen, die im Folgenden beschrieben werden. Nachdem die IP-Adresse herausgefunden wurde, kommen die bekannten Mechanismen von IP zum tragen.

NetBIOS

- NetBIOS ist Software-Schnittstelle, entworfen für kleine Netze
- Verwendet eigenen Namensraum (NetBIOS Name $\neq$ DNS Name)
- beliebig viele Namen pro Rechner
- Kommunikation über Broadcasts
- Samba funktioniert nur über TCP/IP

Folie 262

19.2 Bestandteile von Samba

Das Programmpaket Samba besteht aus mehreren Teilen, von denen einige der Serverseite und andere der Clientseite zugeordnet werden können. Die Servertools:

- `smbd` ist der zentrale Serverprozess, der für die eigentlichen Datei- und Druckdienste zuständig ist. Sie werden mehrere smbds im System finden. Einer dieser Prozesse lauscht auf dem TCP-Port 139, und nimmt neue Verbindungen entgegen. Jede neue Verbindung stößt einen neuen Prozess smbd an. Samba ist im Hauptspeicherverbrauch recht sparsam. Jeder aktive Client benötigt etwa 1 MB Hauptspeicher auf dem Server. Clients, die gerade nicht aktiv Dateien mit dem Sambaserver austauschen, benötigen praktisch überhaupt keine Resourcen. Viel Hauptspeicher kann von Samba selbstverständlich gut als Cache genutzt werden.
- `nmbd` ist für die NetBIOS Namens- und Datagrammdienste zuständig. Dieser Prozess reserviert beim Start von Samba die entsprechenden NetBIOS-Namen, er ist WINS-Server und für den Computersuchdienst zuständig.
- `testparm` Mit diesem Programm kann man die smb.conf auf syntaktische Korrektheit prüfen.
- `smbpasswd` wird zur Pflege der verschlüsselten Passwörter auf Serverseite verwendet (siehe unten).

Die Clients sind:

- `smbclient` Mit dem Programm smbclient kann man auf Freigaben von NT-Rechnern zugreifen. Man kann auf von NT zur Verfügung gestellten Druckern drucken und man kann NT-Freigaben in tar-Dateien sichern. Weiterhin wird mit smbclient die Liste der Server im Netz erfragt, analog zu der Netzwerkumgebung unter Windows.
- `nmblookup` ist ein Diagnosewerkzeug für die NetBIOS-Namensauflösung. Wenn zwei Computer mit Windows sich nicht finden können, kann man mit `nmblookup` deren Versuche, sich gegenseitig zu finden, genau nachstellen. Ebenso können WINS-Server befragt werden und ein NetBIOS Node Status abgefragt werden. Das entsprechende Programm

auf Seiten von Windows ist das Kommandozeilenprogramm `nbtstat`.

- `smbmount` erlaubt das Mounten von SMB Shares.
- `smbprint` ermöglicht das Drucken auf SMB Druckern.

Auf der Serverseite finden sich noch weitere Komponenten:

- `smb.conf` ist die zentrale Konfigurationsdatei von Samba; meits in `/etc/`.
- `/var/lock/samba` für temporäre Lockdateien und Datenbanken
- `/etc/smbpasswd` ist die Passwortdatenbank von Samba, sofern mit verschlüsselten Passwörtern gearbeitet wird in `/usr/local/ samba/private/`

Bestandteile von Samba

Server:

- `smbd` ist der eigentliche Daemon für die Datei- und Druckerfreigabe.
- `nmbd` ist für die NetBIOS Namensauflösung zuständig.
- `testparm` überprüft zentrale Konfigurationsdatei.
- `smbpasswd` ist für die Passwörter der Windows Benutzer zuständig.

Client:

- `smbclient` erlaubt Zugriff auf Windows (und Samba) Shares.
- `smbmount` erlaubt das mounten solcher Shares.
- `smbprint` erlaubt das Drucken auf Printer Shares.

Folie 263

19.3 NetBIOS-Konfiguration mit Samba

Als erstes soll eine minimale Konfiguration von Samba erreicht werden, mit der jeder Rechner in der Netzwerkumgebung zu sehen ist. Dazu sollte die Datei `smb.conf` folgendermaßen aussehen:

```
[global]
workgroup = arbeitsgruppe
interfaces = <IP-Adresse>/<Netzmaske>
```

Der grundsätzliche Aufbau der `smb.conf` gleicht dem Aufbau der .INI-Dateien von Windows 3. Die Datei ist in mehrere Abschnitte unterteilt, die jeweils durch einen Abschnittsnamen eingeleitet werden. Dieser Abschnittsname selbst wird in eckige Klammern gesetzt. Der Inhalt jedes Abschnitts besteht nun aus Parameterzuweisungen. Im Beispiel gibt es nur den Abschnitt global. In diesem werden Festlegungen getroffen, die den Server als ganzes betreffen. Wenn später Freigaben erstellt werden, geschieht dies durch Anlegen von weiteren Abschnitten. Mit dem Parameter `workgroup` wird die Arbeitsgruppe festgelegt, in der sich der Server befinden soll. Der Parameter `interfaces` gibt das Netzwerkdevice an. Zusätzlich kann auch die Broadcastadresse angegeben werden.
Mit diesen beiden Einstellungen wird man direkt den Sambarechner in der Netzwerkumgebung sehen. Zur Vereinfachung sollten noch zwei weitere Parameter gesetzt werden, die später erklärt werden:

```
security = share
encrypt passwords = yes
```

Nun kann Samba (`smb` und `nmbd`) mittels des Initscripts `/etc/init.d/smb` gestartet werden. Meist wird Samba als Standalone Server verwendet. Es ist aber möglich den `smb` (aber nur diesen) über den Internetdaemon zu betreiben.

`/etc/samba/smb.conf`

- einzelne Teile werden mit [...] getrennt
- `[global]` ist der Hauptteil und zwingend erforderlich
- `workgroup` legt fest, in welcher Arbeitsgruppe/Domäne sich der Rechner anmelden soll
- `interfaces` gibt die Netzwerkadressen an, unter denen der Rechner erreichbar sein soll

Folie 264

19.4 Einfache Freigaben

Wenn der Sambarechner nicht nur im Netz gesehen werden soll, sondern auch sinnvolle Dinge tun soll, muss man Freigaben zur Verfügung stellen. Dies tut man, indem man einfach einen neuen Abschnitt beginnt. Um eine Freigabe vollständig zu machen, muss man mit dem Parameter `path` angeben, welches Verzeichnis man freigeben möchte. Eine für alle Zugriffe offene Freigabe des Verzeichnisses `/cdrom` erreicht man mit folgendem Eintrag in `smb.conf`:

```
[cdrom]
path = /cdrom
guest ok = yes
```

Damit entsteht auf dem Server eine Freigabe namens `CD`, die das Verzeichnis `/cdrom` im Netz für alle zum Lesen zur Verfügung stellt.
Achtung: Es findet hier *keine* Überprüfung der Zugriffsrechte statt. Um diese Überprüfung zu ermöglichen, sollte zunächst einmal der Aufbau einer Verbindung zu einer Freigabe genauer beleuchtet werden.
Um *Drucker* unter Samba zur Verfügung zu stellen, müssen diese zunächst unter Unix funktionieren. Alle Drucker, die via LPD, LPRng oder CUPS installiert sind, können als Netzwerkdrucker für Windowsclients freigegeben werden. Druckertreiber unter Windows gehen vom Windows-Metafile-Format aus, und wandeln dies entsprechend um. Das Windows-Metafile-Format enthält Aufrufe an die Graphische Komponente von Windows, das GDI. Wenn man einen Drucker, der über Unix angesprochen wird, von Windows aus nutzen möchte, muss man planen, wo die Aufbereitung in das druckereigene Format geschehen soll. Zwei Wege sind denkbar.

Dateifreigaben

- Dateien müssen zuerst freigegeben werden, um von Windows aus sichtbar zu sein
- Jede Freigabe ist ein eigener Abschnitt (zB: [cdrom]) in `/etc/samba/smb.conf`
- `path` gibt das Verzeichnis an, das freigegeben werden soll

Folie 265

Druckerfreigabe

- Funktioniert genauso wie Dateifreigabe
- `printable` gibt an, dass es sich um einen Drucker handelt
- `printer` gibt die Druckerwarteschlange unter Unix an
- `path` braucht eigenes Spool-Verzeichnis!

Folie 266

- Auf den Arbeitsplätzen wird ein generischer Postscripttreiber installiert. Die Clients müssen nicht wissen, welches Druckermodell sich hinter einer Freigabe verbirgt. Die Umwandlung findet auf dem Druckerserver mittels `ghostscript` statt.
- Auf den Arbeitsplätzen werden für jeden Netzdrucker die korrekten Treiber installiert.

Beide Wege haben Vor- und Nachteile. Im ersten Fall hat man weniger Aufwand mit der Administration auf Clientseite. Man muss den korrekten Druckertreiber nur einmal definieren, am Druckerserver. Beim zweiten Weg kann man die bessere Unterstützung der Druckerhersteller für die Windowsplattformen nutzen. Druckertreiber für Windows bieten in der Regel die Möglichkeit, Sonderfunktionen wie die Auswahl des Papierschachtes zu nutzen. Dieser erhöhte Komfort zieht jedoch nach sich, dass auf jedem Client der korrekte Druckertreiber installiert ist.
Eine Druckfreigabe wird genau wie eine Dateifreigabe in einem eigenen Abschnitt erstellt, wobei für die Druckfunktion drei Optionen notwendig sind:

```
[deskjet]
printable = yes
printer = lp
path = /tmp
```

Zu einer Druckfreigabe wird die Definition durch die Angabe `printable = yes`. Mit der Option `printer =` wird festgelegt, welche Druckerwarteschlange unter Unix angesprochen werden soll. Die Option `path =` legt einen Spoolbereich fest. Ein Druckjob, den ein Windowsrechner an Samba schickt, muss zunächst in einer Datei abgespeichert werden. Wenn diese Datei geschlossen wird, teilt der Client dem Server mit, dass diese nun zum Drucker geschickt werden soll. Samba realisiert dies, indem das Programm `lpr` mit der Druckdatei als Argument aufgerufen wird. Samba muss also für sich die Möglichkeit haben, Druckjobs in Dateien zu speichern, bevor sie an den `lpd` übergeben werden. Dies sollte nicht das Spoolverzeichnis sein, das der `lpd` selbst für den Drucker vorsieht.

19.5 Die Netzwerkumgebung

Die Netzwerkumgebung ist einer der instabileren Aspekte von Windows. Hiermit kann man sich, sofern alles funktioniert, alle Rechner in einer Arbeitsgruppe anzeigen lassen. Dabei dauert es mitunter geraume Zeit, bis ein Rechner in einer Anzeige erscheint, und es dauert unter Umständen noch länger, bis er wieder verschwindet. Eine naive Implementation könnte funktionieren, indem jeder Rechner, der Serverdienste anbietet, dieses regelmäßig per Broadcast im Netz mitteilt. Ein solches Vorgehen hat jedoch mehrere Nachteile. Erstens würde die Last im Netz mit jedem zusätzlichen Rechner stark ansteigen. Zweitens muss jeder Rechner, der die Netzwerkumgebung anzeigen will, relativ komplexe Software laufen lassen. Und drittens scheitert dieses Schema auf jeden Fall an Subnetzgrenzen, die für Broadcasts eine Grenze darstellen. Aus diesen Gründen ist man einen anderen Weg gegangen.
Der *Lokale Master Browser* (im Folgenden auch LMB genannt) ist ein Rechner, der im Netz die Netzwerkumgebung pflegt. Dieser Rechner wird nirgendwo zentral bestimmt, sondern er wird gewählt. Diese Wahl findet immer dann statt, wenn einer der beteiligten Rechner feststellt, dass es im Moment keinen solchen Lokalen Master Browser gibt. Beispielsweise kann der Explorer von Windows eine solche Wahl anstoßen. Wenn Windows 95 die geschwenkte Taschenlampe anzeigt, wird der LMB gesucht. Ist keiner vorhanden, wird eine Wahl angestoßen.
Die Wahl erfolgt mit Datagrammen an den Gruppennamen `arbeits gruppe`. Ein Rechner verschickt ein Datagramm an diesen Namen. Jeder Rechner, der diesen Namen reserviert hat, hört dieses Datagramm und entscheidet, wie er selbst vorgehen soll. In dem Datagramm sind verschiedene Kriterien zur Wahl enthalten, beispielsweise das Betriebssystem des versendenden Rechners.
Empfängt beispielsweise eine Windows NT Workstation ein Paket von einem Windows NT Server, so entscheidet sie, dass sie die Wahl verloren hat. Damit wird sie selbst nicht mehr aktiv. Kommt dieses Paket jedoch von einem Windows 95 Rechner, so hält sie sich selbst für geeigneter, den Lokalen Master Browser zu übernehmen. Dann wird sie selbst ein solches Wahlpaket mit ihren Parametern versenden. Der Windows 95 Rechner empfängt dies, und sieht, dass er verloren hat. Auf diese Weise schaukelt

sich die Wahl hoch, bis der beste Rechner die Wahl gewinnt.
Wenn es nun mehrere Windows NT Workstations im Netz gäbe, dann wäre die Wahl unentschieden. An dieser Stelle kommt die *Uptime* der Rechner ins Spiel. Der Rechner, der am längsten läuft, gewinnt die Wahl. Nun kann es sein, dass nach einem Stromausfall zwei Rechner genau die gleiche Uptime haben. Dann kommt als letztes und eindeutiges Entscheidungskriterium der NetBIOS-Name des Rechners zum Zug. Der alphabetisch vorne stehende Rechner gewinnt. Mit diesen drei Kriterien ist eine eindeutige Wahl gesichert.
Samba ordnet sich in der Standardeinstellung zwischen Windows 95 und Windows NT ein, das heißt, gegen Windows 95 gewinnt Samba die Wahl, überlässt jedoch Windows NT Rechnern den Lokalen Master Browser.
Drei Parameter in der `smb.conf` bestimmen das Verhalten von Samba in der Wahl zum Lokalen Master Browser:

- **os level** Damit wird die Einordnung von Samba in die unterschiedlichen Betriebssysteme geregelt. Diese haben für die Betriebssystemstufe folgende Werte:

Windows for Workgroups	0
Windows 95/98	1
Windows NT Workstation	16
Windows NT Server	32

  Diese Werte sind nicht als fest anzusehen. Wenn ein neues Service Pack für ein Betriebssystem herausgegeben wird, ist es möglich, dass in der Software für den Lokalen Master Browser Fehler bereinigt wurden. Dann ist es sinnvoll, dass diese neue Software die Rolle des LMB übernimmt. Der einfachste Weg ist, den `os level` einfach hochzusetzen. Samba hat hier einen Vorgabewert von 20.
  Der Parameter `os level` kann Werte von 0 bis 255 annehmen. Setzt man ihn auf 255, wird nach einer erfolgreichen Wahl niemand mehr Local Master Browser werden können.

- **local master** Möchte man auf keinen Fall den LMB auf einem Sambarechner haben, so setzt man den Parameter `local master = no`. Dann nimmt Samba an keiner Wahl teil.

- **preferred master** Mit der Standardeinstellung `preferred master = no` sucht Samba beim Start nach einem LMB. Findet er einen, meldet er sich dort. Findet er keinen LMB, bleibt Samba passiv. Jemand anders muss eine Wahl anstoßen. Wenn dann eine Wahl stattfindet, nimmt Samba teil und ordnet sich anhand seines os level ein. Wenn man sicher gehen möchte, dass Samba auf jeden Fall nach dem Start den LMB übernimmt, dann muss man den `os level` hoch genug setzen, und den Parameter `preferred master = yes` setzen. Damit wird Samba beim Start des `nmbd` auf jeden Fall eine Wahl anstoßen und sie dann unter Umständen gewinnen.

Mit den Einstellungen
```
[global]
os level = 66
preferred master = yes
```
kann man sicher sein, dass der Sambarechner immer den LMB innehat. Es sei denn, ein anderer Administrator von Samba kommt auf die Idee, einen noch höheren Wert für den `os level` zu benutzen.
Ein Primary Domain Controller kann unter Umständen erheblich gestört werden, wenn er in seinem Subnetz nicht der LMB ist.

Netzwerkumgebung

- Ein *Local Master Browser* sammelt die Broadcasts des Subnetzes; wird gewählt
- `os level` gibt die „Chance“ an, mit der Samba die Wahl gewinnt
- `local master = no` verhindert, dass Samba an der Wahl teilnimmt
- `preferred master = yes` Samba fängt eine Wahl an, falls er nicht LMB ist

Folie 267

19.6 NetBIOS über Subnetzgrenzen

Wird die Namensreservierung und -auflösung ausschließlich per Broadcast durchgeführt, kann man Rechner, die hinter Routern liegen, nicht erreichen. Broadcasts verbleiben in den Subnetzen, in denen sie ausgesendet wurden.
Sind zum Beispiel zwei Netze über einen Router verbunden, so reserviert jeder der beiden Rechner seinen Namen in dem ihm zugeordneten Subnetz. Die Workstation `WKS` schickt ihre Reservierungen per Broadcast im Subnetz 1, und der Server `SERVER` wird seinen Namen im Subnetz 2 reservieren. Der Router zwischen beiden bekommt diese Reservierungen zwar mit, wird sie aber nicht in das jeweils andere Subnetz weiterleiten. Wenn nun `WKS` ihren Server `SERVER` sucht, geschieht dies ebenfalls per Broadcast im Subnetz 1. Diese Anfrage bleibt in ihrem Subnetz und erreicht `SERVER` gar nicht, so dass dieser auch nicht antworten kann.
Der einfachste Weg, die Namensauflösung über Subnetzgrenzen hinweg zu realisieren, geht über eine statische Tabelle. Unter Windows liegt diese in der Datei `LMHOSTS`. Sie liegt abhängig von der Windowsversion in unterschiedlichen Verzeichnissen und lässt sich am einfachsten mit der Suchfunktion des Desktops finden. Diese Datei ist ähnlich aufgebaut wie die Datei `/etc/hosts` unter Unix. Ein Beispieleintrag ist der folgende:

```
192.168.1.5 samba
```

Die Einträge in der `LMHOSTS` können durch den Zusatz `♯PRE` ergänzt werden. Dieser Zusatz legt fest, in welcher Reihenfolge die Namensauflösung vorgenommen wird. Ist kein `♯PRE` vorhanden, so wird zunächst eine konventionelle Namensauflösung per Broadcast versucht. Erst, wenn diese fehlschlägt, wird in der `LMHOSTS` nachgeschaut. Ist der Zusatz vorhanden, so wird ohne Namensauflösung direkt der Wert in der `LMHOSTS` verwendet.
Die zweite Möglichkeit, das Problem zu lösen, ist eine zentrale Datei `LMHOSTS`. Dazu gibt es den WINS-Server. Ein solcher Server ist ein Rechner, bei dem sich jede Applikation im Netz mit ihren Namen anmeldet. Die IP-Adresse dieses Servers muss jedem Rechner mitgeteilt werden. Bei Windows geschieht dies in den Eigenschaften des TCP/IP Protokolls im Reiter WINS-Adresse. Setzt man DHCP-Server ein, kann man ebenfalls den WINS-Server festlegen. Samba bekommt die Adresse mit dem Parameter `wins server = <ip-adresse>` im Abschnitt `[global]` der `smb.conf` mitgeteilt. Sobald ein Client die IP-Adresse des WINS Servers kennt, ist es völlig gleichgültig, ob sich dieser im gleichen Subnetz befindet oder nicht.

Die Namensreservierung erfolgt nicht mehr per Broadcast, sondern mit einem gerichteten UDP-Paket an den WINS-Server. Gerichtete Pakete leitet der Router wie jedes andere Paket an den WINS-Server weiter. Dieser sieht in seiner Tabelle nach, ob der Name bereits reserviert ist. Ist das nicht der Fall, so wird er spontan eine Bestätigung der Reservierung zurückschicken. Diese Reservierung gilt nun für eine bestimmte Zeit und muss rechtzeitig erneuert werden.
Ist der Name bereits reserviert, wird der WINS-Server den bisherigen Besitzer befragen, ob er den Namen noch benötigt. Bekommt er keine Antwort, wird er dem neuen Besitzer ebenfalls eine Bestätigung schicken. Möchte der alte Besitzer den Namen noch verwenden, so wird der Anfragende eine Ablehnung der Reservierung erhalten. Diese Nachfrage ist notwendig, um einem abgestürzten Rechner das spontane Booten zu ermöglichen, da bei einem Absturz keine Freigabe der Namensreservierung erfolgen kann.
Die Namensanfrage, die den Server nicht erreichte, weil der Router keine Broadcasts weitergibt, wird nun direkt an den WINS-Server gerichtet, der in seiner Tabelle nachsehen kann.
Samba kann ganz normal als WINS-Server konfiguriert werden, indem der Parameter `wins support = yes` gesetzt wird. Ist diese Parameter gesetzt, kann Samba nach einem Neustart bei allen Clients und allen sonstigen Servern als WINS-Server eingetragen werden. Werden diese dann neu gestartet, melden sie sich beim WINS-Server an.
Wenn nun ein Rechner mit Samba als WINS-Server konfiguriert ist, und sich die anderen Rechner dort anmelden, werden diese in der Datei `/var/lock/samba/wins.dat` abgelegt. Der `nmbd` pflegt diese Datei dynamisch, je nach Reservierungen und Abmeldungen. Die Datei `wins.dat` wird in regelmäßigen Abständen geschrieben. Wenn es notwendig sein sollte, den wirklich aktuellen Stand unabhängig von diesem Zeitintervall zu erhalten, so kann man dem `nmbd` das HANGUP-Signal durch den Befehl `killall -HUP nmbd` senden. Außerdem wird die `wins.dat` beim Beenden des `nmbd` geschrieben.
Diese Datenbank wird auf Festplatte gehalten, damit die Da-

ten einen Neustart von Samba überleben. Jeder Rechner, der einen Namen für sich reserviert hat, hat diese Reservierung für einen bestimmten Zeitraum ausgesprochen. Wenn Samba jetzt neu gestartet werden sollte, und dadurch die Datenbank verloren ginge, wäre der gesamte NetBIOS-Namensraum nicht mehr verfügbar. Außerdem kann ein WINS-Server die angeschlossenen Clients weder von sich aus finden, noch sie darum bitten, sich erneut zu registrieren. Daher ist die WINS Datenbank über Neustarts von Samba hinaus zu erhalten.
Die Anfrage, die die Workstation `WKS` absetzt, wird nun nicht mehr per Broadcast gestellt, sondern mit einem gerichteten Paket an den WINS-Server, bei dem sich alle Rechner angemeldet haben.
WINS hat gegenüber der broadcastbasierten Namensreservierung einige Vorteile. Namensreservierung per Broadcast erfolgt durch Wartezeiten. Es wird die Reservierung angekündigt, es wird gewartet, die Reservierung wird erneut angekündigt, und es wird wieder gewartet. Dieses Spiel wiederholt sich mehrfach, bis der Rechner sicher sein kann, dass ein eventueller Vorbesitzer des Namens genug Zeit hatte, sich zu beklagen. Beim Einsatz von WINS entfallen diese Wartezeiten, da hier ein einziger Rechner sämtliche reservierte Namen registriert und in seiner Tabelle nachschauen kann. Daher ist die Reservierung per NetBIOS deutlich schneller, und auch weniger netzbelastend. Selbst wenn man also nur ein einziges Subnetz hat, sollte man zur Reduzierung der Netzlast den Einsatz eines WINS-Servers in Erwägung ziehen.
Zusätzlich sei hier angemerkt, dass es netzwerkweit nur einen einzigen WINS-Server geben darf. Selbst wenn es unterschiedliche Arbeitsgruppen oder Domänen gibt, darf es nicht mehr als einen WINS-Server geben. Setzt man mehrere WINS-Server ein, hat man getrennte Namensräume. Rechner im einen Namensraum können mit Rechnern, die an einem anderen WINS-Server angeschlossen sind, nicht kommunizieren. Es kann trotzdem zu Kollisionen kommen, da Windowsrechner bestimmte Namen unabhängig von WINS-Einstellungen ausschließlich per Broadcast reservieren. Unter Windows NT kann man mehrere WINS-Server einsetzen, die sich gegenseitig abstimmen. Diese WINS-Server treten gegenüber den Clients als ein einziger Server auf, unabhängig von ihrer Anzahl.

Die Abfrage eines WINS Servers durch `nmblookup` erfolgt beispielhaft folgendermaßen:

```
nmblookup -R -U 192.168.1.5 samba
```

Hiermit wird der WINS Server, der auf dem Rechner 192.168.1.5 liegt, nach dem Namen `samba` befragt.
Samba kennt zwei zusätzliche Funktionen, die es im Zusammenhang mit WINS interessant machen. Einerseits kann Samba als WINS Proxy eingerichtet werden, indem `wins proxy = yes` gesetzt wird. Ist diese Einstellung aktiv, dann wird Samba sämtliche Reservierungen und Anfragen, die es aus dem lokalen Netz per Broadcast erhält, an den mit `wins server =` konfigurierten WINS-Server weiterleiten. Damit kann man einen Samba-Server in ein Subnetz stellen. Sämtliche Rechner in diesem Netz werden nun beim WINS angemeldet, und nutzen diesen auch. Dies ist auch dann der Fall, wenn sie entweder selbst keinen WINS-Server ansprechen können oder nicht dafür konfiguriert sind. Man sollte jedoch in jedem Fall eine echte Konfiguration des WINS Servers auf dem Client vorziehen. Ein WINS-Proxy kann nur eine Behelfslösung sein, da man sich damit auf einen weiteren Rechner verlässt.
Unter Windows kann man statische Einträge im WINS vornehmen. Dies geht so direkt unter Samba nicht. Man muss hierzu den Parameter `dns proxy = yes` auf dem WINS-Server setzen. Empfängt der WINS-Server nun eine Anfrage, die er nicht aus seiner Datenbank beantworten kann, wird er eine ganz normale Unix-Hostnamenanfrage machen. Typischerweise wird er in der `/etc/hosts` nachschauen und danach dann das DNS anhand der Konfiguration in der Datei `/etc/resolv.conf` befragen. Damit ist es durch einen Eintrag auf dem WINS Server möglich, den gesamten DNS-Namensraum auch in der NetBIOS-Namenswelt zur Verfügung zu stellen.

WINS Server

- Namensreservierung funktioniert nur im eigenen Subnetz
- `LMHOSTS` nur statische Möglichkeit, einen Server außerhalb zu erreichen
- WINS Server verwaltet alle Rechner im Netzwerk (d.h. Domäne/Arbeitsgruppe)
- `wins server` gibt Samba den WINS Server bekannt
- `wins proxy = yes` lässt Samba die Datenbank des WINS Servers spiegeln
- `wins support = yes` Samba wird selbst WINS Server

Folie 268

19.7 SMB-Sitzungen

Wird am Client eine Verbindung zu einer Freigabe auf einem SMB-Server aufgebaut, so müssen mehrere Schritte durchlaufen werden.

- **NetBIOS-Namensauflösung** Zu einem Rechnernamen muss eine IP-Adresse herausgefunden werden. Dies wurde bereits eingehend behandelt.
- **TCP-Verbindung** Wenn die IP-Adresse klar ist, wird eine TCP-Verbindung zu Port 139 des Servers aufgebaut. Um vorhandene TCP-Verbindungen anzuzeigen, gibt es sowohl auf Unix- als auch auf Windowsrechnern das Werkzeug `netstat`.
- **NetBIOS-Sitzung** Auf einem Serverrechner arbeiten unter Umständen mehrere Applikationen, die Namen für sich reserviert haben. Diese sind alle unter der IP-Adresse des Rechners und dem TCP-Protokoll auf Port 139 erreichbar. Anhand des TCP-Verbindungsaufbaus ist nicht klar, welche Serverapplikation angesprochen werden soll. Die Unterscheidung wird durch den Servernamen getroffen, der in der TCP-Verbindung als erstes übertragen wird.

  Dass der Servername übertragen wird, kann man ganz einfach mit Hilfe des Programms `smbclient` sehen. Man versucht, sich die Liste der Freigaben eines realen Windowsrechners geben zu lassen, indem man Folgendes aufruft:

  ```
  smbclient -L smallwin
  ```

  Damit wird zunächst eine NetBIOS-Namensanfrage ausgelöst, und dann eine Verbindung zum entsprechenden Server ausgelöst. smbclient hat jedoch die Möglichkeit, einen Server unter einem anderen Namen anzusprechen, indem man `smbclient -L test -I ip-adresse` eingibt. `smbclient` wird zunächst versuchen, eine Verbindung zum NetBIOS-Namen `test` aufzubauen, und zwar ohne dass eine NetBIOS-Namensanfrage ausgelöst wird. Stattdessen wird die angegebene IP-Adresse auf Port 139 direkt angesprochen, und der Name `test` als Servername angegeben. Windows merkt, dass das nicht stimmen kann und verweigert den Verbindungsaufbau mit einer Fehlermeldung. Erst im

zweiten Versuch wird es `smbclient` gelingen, eine Verbindung aufzubauen, da diese Verbindung zum allgemeinen Namen `*smbserver` aufgebaut wird. Auch der Clientname wird in der Verbindung übergeben. Dies testet man am besten mit

```
smbclient //win/c\$ -n blafasel
```

und schaut sich die Verbindungstabelle auf der Windowsmaschine mit `nbtstat -s` an.

Mit dem übergebenen Servernamen kann man sehr nette Tricks anstellen. Man stelle sich vor, dass einige Freigaben nur für bestimmte Clientrechner sichtbar sein sollen. Dies ist mit Bordmitteln von Samba so nicht möglich. Man kann zwar mit dem Parameter `browseable` festlegen, ob bestimmte Freigaben in der Netzwerkumgebung erscheinen. Dieser Parameter hat aber zwei Nachteile. Erstens sind die Freigaben nur unsichtbar geworden, darauf zugreifen kann man immer noch. Zweitens kann man Freigaben nur für alle Rechner verstecken oder freigeben.

Samba bietet die Option, unter zwei oder mehreren verschiedenen Namen in der Netzwerkumgebung zu erscheinen. Mit dem Parameter `netbios name` gibt man einen Namen für den Server an. Zusätzliche Namen kann man mit `netbios aliases` vergeben. Mit

```
netbios name = fichte
netbios aliases = birke eiche kiefer buche
```

handelt man sich einen ganzen Wald in der Netzwerkumgebung ein. Klickt man auf die einzelnen Server, sieht man überall die gleichen Freigaben und Zugriffsrechte. Nun kann man für jeden dieser virtuellen Rechner eine eigene Konfigurationsdatei anlegen. Beispielsweise kann man sie `/etc/samba/smb.conf.birke`, `/etc/samba/smb.conf.eiche` und so weiter nennen. Die Datei `/etc/ smb.conf` ist für den Rechner `fichte` zuständig und enthält neben den Einstellungen für `fichte` den Parameter

```
config file = /etc/samba/smb.conf.%L
```

Dabei steht `%L` für den Servernamen, unter dem Samba angesprochen wird. Wenn es eine passende Datei gibt, dann

bewirkt der Parameter `config file`, dass die komplette Konfiguration neu eingelesen wird. Existiert keine passende Datei, so wird der Parameter einfach ignoriert. Um nun den Zugriff nur für einzelne Clients zu erlauben, kann bei den einzelnen virtuellen Servern mit den Parametern `hosts allow` und `hosts deny` der Zugriff geregelt werden.

- **Negotiate Protocol** Die NetBIOS-Sitzung ist nun aufgebaut, und es können Daten übermittelt werden. Innerhalb dieser NetBIOS-Sitzung wird eine SMB-Sitzung schrittweise aufgebaut. SMB ist ein Protokoll, bei dem im Prinzip der Client jede Aktion durch eine Anfrage anstößt, und der Server diese beantwortet.

  Die erste Anfrage, die der Client an den Server schickt, ist ein *Negotiate Protocol Request*. In dieser Anfrage schickt der Client an den Server eine Liste der Protokollvarianten, die er beherrscht. Der Server wählt nun aus dieser Liste der Protokolle eines aus, und schickt eine entsprechende Antwort zurück. Die verschiedenen Protokolle bauen aufeinander auf. Daher kann man mit dem Parameter `protocol` das höchste Protokoll festlegen, mit dem Samba arbeiten soll. In der Antwort auf diese erste Anfrage werden zwei weitere Einstellungen verschickt, die Teile des weiteren Ablaufs festlegen.

  In der Antwort auf diese erste Anfrage werden zwei weitere Einstellungen verschickt, die Teile des weiteren Ablaufs festlegen.

  Der Server entscheidet, ob er die Zugriffssteuerung auf Benutzer- oder auf Freigabeebene regeln möchte. Damit wird festgelegt, zu welchem Zeitpunkt der Benutzer ein Passwort liefern muss. Entweder kann es beim direkt folgenden *Session Setup* erfolgen, oder erst beim *Tree Connect* danach.

  Der Parameter `security` legt fest, welche Art der Zugriffssteuerung gewählt wurde. Mit `security = share` wird die Freigabeebene eingestellt, `security = user` legt die Clients auf die Benutzerebene fest.

  Sichtbar wird diese Unterscheidung in der Windowswelt nur bei Windows 95 und Windows 98. Diese Betriebssysteme

beherrschen zunächst einmal nur die Zugriffssteuerung auf Freigabeebene, da sie nicht über eine Benutzerdatenbank verfügen. Es ist nicht möglich, einzelnen Benutzern den Zugriff auf Freigaben zu gewähren oder zu verweigern. Um trotzdem benutzerbasiert Zugriffssteuerung zu ermöglichen, muss ein Server angegeben werden, der für Windows die Benutzerdatenbank pflegt. Damit können Passwörter benutzerbasiert überprüft werden.

Weiterhin gibt der Server dem Client vor, ob Klartextpasswörter verwendet werden sollen, oder ob die Passwörter verschlüsselt werden. Wenn der Server festlegt, dass verschlüsselte Passwörter verwendet werden, wird zusätzlich die Herausforderung für das *Challenge Response* Verfahren mitgeschickt.

Die Entscheidung über Klartextpasswörter muss also getroffen werden, ohne dass der Server den Benutzernamen, der sich anmelden will, kennt. Es ist also nicht möglich, für einige Benutzer Klartextpasswörter und für andere Benutzer verschlüsselte Passwörter zu verwenden.

- **Session Setup** Nachdem die Protokollversion ausgehandelt ist, wird vom Client ein *Session Setup* verschickt. In diesem Session Setup schickt der Client seinen Benutzernamen an den Server. Sofern dieser `security = user` verlangt hat, wird an dieser Stelle das Passwort mitgeschickt. Damit ist der Server in der Lage, die Identität des Benutzers festzustellen. Wenn `security = share` vereinbart wurde, dann ignoriert der Server ein hier eventuell mitgeschicktes Passwort.

- **Tree Connect** Als letztes legt der Client fest, welche Freigabe er ansprechen will. Der entsprechende Aufruf heißt *Tree Connect*. Sofern `security = share` vereinbart wurde, wird an dieser Stelle das Passwort überprüft. Der Benutzername kann in diesem Fall nicht zur Zugriffsregelung verwendet werden. Dieser wurde unter Umständen gar nicht übermittelt, da der Client den Session Setup komplett auslassen darf. Andererseits hat er bei einem durchgeführten Session Setup kein Passwort angeben müssen, anhand dessen die Identität des Benutzers zweifelsfrei hätte festgestellt werden können.

weitere Optionen

- `smbclient -L <Rechnername>` zeigt die Freigaben am angegebenen Rechner an
- `netbios name` setzt den NetBIOS Namen von Samba (muss nicht der FQDN sein)
- `netbios aliases` weitere Namen, die Samba für sich reserviert
- `config file` weitere Konfigurationsdatei, die eingebunden wird (am besten mit % L verwenden)
- `security = share` setzt die Sicherheit auf Freigabeebene (alle dürfen zugreifen); andere Parameter: `user, server, domain`

Folie 269

19.8 Zugriffsrechte

Bei Windows NT kann man mit zwei unterschiedlichen Mechanismen Rechte vergeben. An einer Freigabe kann man über Schreib- und Lesezugriff entscheiden. Innerhalb des Dateisystems kann man detailiert Rechte vergeben.
Ist bei Samba `security = user` gesetzt, so hat der Server die Möglichkeit, anhand des angemeldeten Benutzers Zugriffsrechte zu vergeben oder zu verweigern. Wenn bezüglich der Zugriffsrechte bei einer Freigabe nichts gesagt wird, hat jeder korrekt angemeldete Benutzer Leserecht. Man kann auch Gastbenutzern Leserecht geben, indem man `guest ok = yes` setzt.
Mit den Optionen zur Rechtevergabe an Freigaben hat man die Möglichkeit, einzelnen Benutzern und ganzen Unixgruppen Rechte zu geben oder zu nehmen. Die Möglichkeiten sind hier deutlich weiter gehend als die Semantik, die Unix mit den Rechtemasken für den Dateibesitzer, die besitzende Gruppe und den Rest der Welt bereit stellt. Von den möglichen Anwendungen sollen hier drei häufig benötigte Fälle dargestellt werden.

- **Alle Benutzer haben gleichen Zugriff**

  ```
  [projekt]
  path = /data/projekt
  ```

  Bei dieser Freigabe bekommen alle Benutzer, die sich mit Namen und Passwort am Server angemeldet haben, *Leserecht* auf die Freigabe. Schreibrecht vergibt man, indem man den Parameter `writeable = yes` setzt:

  ```
  [projekt]
  path = /data/projekt
  writeable = yes
  ```

- **Einige Benutzer haben gleichen Zugriff**

  Will man den Zugriff auf einige Benutzer einschränken, erstellt man eine Liste `valid users` auf:

  ```
  [projekt]
  path = /data/projekt
  valid users = mueller, meier
  ```

  Zu dieser Freigabe haben die Benutzer `mueller` und `meier` Lesezugriff. Sollen diese Benutzer Schreibzugriff bekommen, so ist wie im vorangegangenen Beispiel der Parameter `writeable = yes` zu setzen:

  ```
  [projekt]
  path = /data/projekt
  valid users = mueller, meier
  writeable = yes
  ```

  Für den Parameter `valid users` spielt der Benutzer `root` keine besondere Rolle. Das heißt, dass er auf die Freigabe `projekt` keinen Zugriff hat. Soll er Zugriff bekommen, muss man ihn wie jeden anderen Benutzer in die Liste `valid users` mit aufnehmen.

  Der Parameter `valid users` gibt die Möglichkeit, ganze Unixgruppen in den Zugriff mit aufzunehmen. Um dies zu erreichen, muss man das `@`-Zeichen voranstellen:

  ```
  [projekt]
  path = /data/projekt
  valid users = root, @users
  writeable = yes
  ```

  Mit dieser Einstellung haben alle Benutzer, die in der Unixgruppe users sind, Schreibzugriff auf die Freigabe. Zusätzlich kann der Benutzer root schreiben.

- **Einige Benutzer haben Leserecht, andere Schreibrecht**

  Will man differenziert Rechte vergeben, so muss man sämtliche Benutzer, die überhaupt Zugriff auf die Freigabe bekommen sollen, in die Liste `valid users` aufnehmen, und mit `writeable = no` nur Leserechte vergeben. Die Benutzer, die über diese Standardeinstellung hinaus Schreibrecht bekommen sollen, müssen in die `write list` aufgenommen werden.

  ```
  [projekt]
  path = /data/projekt
  valid users = @users, @admins
  writeable = no
  write list = @admins
  ```

Mit diesen Einstellungen haben die Benutzer der Gruppe users Leserecht, und die Benutzer der Gruppe `admins` haben Schreibrecht.

Zugriffsrechte

- ohne weitere Optionen darf jeder auf die Freigabe zugreifen
- `writable` allgemeiner Schreibschutz
- `valid users` diese User dürfen auf die Freigabe zugreifen
- `write list` diese User dürfen Schreiben (auch wenn `writable =no`

Folie 270

Unix-Zugriffsrechte
Unter Windows NT gibt es zwei Möglichkeiten, Zugriff auf Dateien zu gewähren. Über eine Freigabe kann ein Lese- oder ein Schreibrecht vergeben werden. Im zweiten Schritt können dann über eine Rechtevergabe im Dateisystem weitere Rechte vergeben werden. Samba regelt die Zugriffskontrolle ebenfalls in zwei Schritten. Die freigabebezogenen Rechte werden über Parameter wie `valid users` und `write ok` geregelt. Die Zugriffsrechte innerhalb des Dateisystems regelt Samba nicht selbst, sondern verlässt sich hierfür auf das darunterliegende Betriebssystem Unix.
Zwischen Unix und DOS bestehen große Unterschiede. DOS und alle seine Nachfolger sind Einzelbenutzersysteme, Unix ist von Anfang an als Multiusersystem entworfen worden. Diese Unterschiede werden besonders deutlich, wenn man die Attribute betrachtet, die auf Dateien vergeben werden. DOS kennt vier Attribute:

- **Read-Only** Der Inhalt dieser Datei kann nur gelesen, aber nicht geschrieben werden. Die Datei kann nicht gelöscht werden.
- **System** Diese Datei ist für spezielle Betriebssystemzwecke vorgesehen.
- **Hidden** Diese Datei wird mit dem Kommando „DIR“ nicht angezeigt.
- **Archiv** Das Archivbit wird bei jedem Schreibzugriff gesetzt. Backupprogrammen ist es freigestellt, dieses Bit zurückzusetzen. Damit kann eine inkrementelle Sicherung ermöglicht werden.

Diese Bits können vom Benutzer frei gesetzt und wieder zurückgesetzt werden. Sie bieten also keinen echten Zugriffsschutz, sondern nur eine gewisse Sicherung gegen Fehlbedienung. Unter DOS werden Ausführungsrechte nicht verwendet. Sie stehen für Samba zur Verfügung, um die DOS-Attribute im Unix-Dateisystem abzubilden. Das Schreibschutzbit unter DOS hat mit dem Schreibrecht des Dateibesitzers unter Unix eine Entsprechung. Bis auf die Umsetzung des Schreibschutzbits kann die Umsetzung der Attribute unter Samba mit den entsprechenden

Parametern `map <xxx>` gesteuert werden, wobei das Archivbit ohne Zusatzangabe umgesetzt wird, die anderen beiden Attribute nicht. Die Attribut-Umsetzung geschieht an Hand der folgenden Tabelle:

DOS-Attribut	Unix-Recht	Maske	Parameter	Standard
Schreibschutz	rw-******	200	-	immer
Archiv	r-x******	100	`map archive`	`yes`
System	***r-x***	010	`map system`	`no`
Versteckt	******r-x	001	`map hidden`	`no`

Samba muss nun diese beiden Dateiattribute ineinander überführen. Samba muss neu erstellten Dateien Unixrechte zuordnen. Wird eine Datei neu erstellt, dann gibt der Client dem Server die DOS-Attribute mit, mit der er die Datei erstellt haben möchte. Daraus formt Samba einen Satz von Unix-Zugriffsrechten. Diese Rechte werden vom Parameter create mask eingeschränkt. Die Standardvorgabe für die `create mask` ist gleich `744`, was der Rechtemaske `rwxr-r-` entspricht. Der Dateieigentümer hat Schreib- und Leserecht, alle anderen haben reines Leserecht. Samba schränkt die Rechte ein, indem der gewünschte Satz an Rechten mit einer logischen UND-Operation mit der `create mask` verknüpft wird. Nur die Rechte, die in der `create mask` gesetzt sind, können möglicherweise in der neu erzeugten Datei auftauchen. In einem weiteren Schritt setzt Samba explizit gewünschte Zugriffsrechte anhand des Parameters `force create mode`, dessen Standardwert auf `000` steht. Dies geschieht durch eine ODER-Verknüpfung mit diesem Wert.
Diese Zusammenhänge werden an einem Beispiel deutlicher. Es kann gewünscht sein, dass auf neu erstellten Dateien nur der Dateibesitzer und die Gruppe Leserecht haben sollen. Der Rest der Welt soll diese Dateien nicht lesen können. Das wird dadurch erreicht, dass man die `create mask = 740` setzt, also das Leserecht für den Rest der Welt ausmaskiert. Es kann darüber hinaus gewünscht sein, dass die besitztende Gruppe ein Schreibrecht eingeräumt bekommt. Das kann man durch `force create mode = 020` erreichen. Tabellarisch dargestellt heißt dies:

Wunsch			`rw-r--r--`
`create mask`	740	UND	`rw-r-----` `rw-r-----`
`force create mode`	020	ODER	`----w----`
Ergebnis			`rw-rw----`

Die Ausführungsrechte auf Dateien werden unter DOS nicht verwendet, sie können also verwendet werden, um DOS-Attribute im Unix-Dateisystem abzulegen. Ausführungsrechte auf Dateiverzeichnissen wirken sich jedoch auf das Verhalten von Samba aus, da durch sie der Zugriff zu den Verzeichnissen geregelt wird. Daher kann es wünschenswert sein, dass die Rechtezuweisung auf Dateien und Verzeichnissen unterschiedlich geregelt wird. Die Parameter `create mask` und `force create mode` wirken daher nur auf neu angelegte Dateien. Für Verzeichnisse sind die Parameter `directory mask` und `force directory mode` verantwortlich. Der Vergabewert für `directory mask` ist hierbei `755`, um den Zutritt für die Gruppe und den Rest der Welt zu ermöglichen, die Vorgabe für `force directory mode` besetzt mit dem Wert `000` kein zusätzliches Recht.

Unix-Zugriffsrechte

- `create mask` gibt die Zugriffsrechte im `chmod` Stil für neu erstellte Dateien an
- `force create mode` gibt zusätzliche Zugriffsrechte an, die immer angehängt werden
- `directory mask` gibt die Zugriffsrechte für neu erstellte Verzeichnisse an
- `force directory mode` analog zu `force create mask` für Verzeichnisse

Folie 271

Passwörter
Im SMB-Protokoll wird zur Authentifizierung ein Challenge-Response Verfahren eingesetzt. Der Server verschickt an den Client eine Zufallszahl, die sogenannte Herausforderung. Der Client kennt das Benutzerpasswort und verschlüsselt die Herausforderung mit dem Passwort als Schlüssel. Diesen verschlüsselten Wert verschickt der Client anstelle des Passworts. Der Server kennt das Benutzerpasswort ebenfalls, und kann den verschlüsselten Wert entschlüsseln. Entsteht bei der Entschlüsselung wieder die Herausforderung, so hat der Benutzer die Herausforderung offensichtlich mit dem korrekten Passwort verschlüsselt. Kommt etwas anderes heraus, war das Passwort nicht richtig.
Authentifizierung unter Unix setzt voraus, dass der Client dem Server das Klartextpasswort präsentiert. Der Server kann daraus den Hashwert berechnen, und mit dem gespeicherten Wert vergleichen. Leider verfügt er nicht über das Klartextpasswort des Benutzers, um das Challenge-Response Verfahren durchführen zu können. Daher muss unter Samba für die Passwortverschlüsselung eine zweite Passwortdatenbank gepflegt werden, die Datei `smbpasswd`.
Auch in der Datei `smbpasswd` stehen keine Klartextpasswörter. Bevor die Herausforderung mit dem Passwort verschlüsselt wird, wird das Passwort unter Windows ebenfalls durch eine Hashfunktion geschickt. Von dieser Hashfunktion gibt es zwei Varianten, die beide nicht mit den unter Unix verwendeten Funktionen übereinstimmen. Das heißt, dass man mit den dort enthaltenen Werten so direkt nicht mehr anfangen kann als mit den Werten aus der Datei `/etc/shadow` unter Unix, denn wenn man sie als Passwort eingeben würde, würde Windows sofort wieder den Hash darauf anwenden, und einen anderen, also falschen Wert daraus errechnen. Das Programm `smbclient` muss diese Operation ebenfalls durchführen, nur hat man hierzu den Quellcode und kann die entsprechenden Stellen auskommentieren. So hat man die Möglichkeit, sich anhand der Werte in der `smbpasswd` ohne Einsatz von crack bei einem NT-Rechner anzumelden.
Alles nicht dramatisch, sagt Microsoft. Das Äquivalent zur Datei `smbpasswd` liegt unter NT verschlüsselt vor. Diese Verschlüsselung muss jedoch reversibel sein, um das Challenge-Response Verfahren durchführen zu können. Ein Teil der Sicherheitsargumentation liegt darin, dass dieses Verschlüsselungsverfahren nicht offengelegt wurde. Das Verfahren war solange geheim, bis Jeremy Allison das Programm `pwdump` veröffentlicht hat. Dieses Programm extrahiert aus der Benutzerdatenbank von NT eine Datei, die direkt als `smbpasswd` verwendet werden kann.

Samba als Logon-Server
Wenn sich in einem Netz Windows 95/98 Clients befinden, kann es wünschenswert sein, dass sich die Benutzer dieser Arbeitsplätze nur mit einem Passwort anmelden können, das zentral auf einem Server vorgehalten wird. Dazu muss der entsprechende Server spezielle Aufrufe von Clients entgegennehmen und korrekt beantworten. In der reinen Windowswelt ist dazu ein Windows NT Server notwendig, der als sogenannter Primary Domain Controller (PDC) installiert ist. Samba ist ebenfalls in der Lage, dies zu tun. Dazu ist im Abschnitt `[global]` der Parameter `domain logons = yes` zu setzen. Die Implementation, die Microsoft gewählt hat, um Domänenanmeldungen zu ermöglichen, erzwingt zusätzlich, dass der Domain Master Browser auf dem gleichen Rechner liegt wie der Logon Server. Das heißt, man benötigt für Domänenanmeldungen die folgenden Parameter:

```
[global]
workgroup = samba
domain logons = yes
domain master = yes
```

Hat man diese Parameter gesetzt, kann man in den Eigenschaften des Clients für Microsoft-Netzwerke einstellen, dass der Client sich an der Domäne `samba` anmelden soll. Hat man verschlüsselte Passwörter aktiviert, kann man vom Client aus sein SMB-Passwort ändern, indem man das entsprechende Kontrollfeld in der Systemsteuerung von Windows benutzt.
Samba in Windows NT Domänen
Die Domänenanmeldung unter Windows 95/98 ist eine relativ einfache Sache, da es sich dabei praktisch nur um eine Überprüfung der Benutzerpasswörter handelt. So etwas wie Benutzer kennt Windows 95 praktisch nicht, jeder Benutzer hat vollen Zugriff auf das gesamte System.
Microsoft unterscheidet verschiedene Netzwerkmodelle. Das Peer-To-Peer Netz ist das Modell, das auch Unix zu Grunde

liegt. Hier hat jeder beteiligte Rechner eine eigene Benutzerdatenbank, eigene Passwörter und eigene Rechtezuordnungen. Das Domänenmodell ist das Modell, das sich signifikant von Unix unterscheidet. Mit dem Domänenmodell wird eine Workstation in die Lage versetzt, mehr als eine Benutzerdatenbank zu benutzen. Neben der eigenen Benutzerdatenbank, die jede Workstation hat, kann sie eine Benutzerdatenbank von einem anderen Rechner importieren. In einer Windows NT Domäne gibt es einen Rechner, der seine eigene Benutzerdatenbank anderen zur Verfügung stellt, den sogenannten Primary Domain Controller. Dieser reserviert für sich spezielle NetBIOS-Namen, um sich den Workstations als Logonserver anzubieten. Eine Workstation befragt den Primary Domain Controller nach allen relevanten Daten zu den Benutzern, die sich bei ihr anmelden wollen, und die Rechte auf der Workstation wahrnehmen können.
Es muss jede Workstation explizit in die Domäne aufgenommen werden.
Bei Samba ist es so, dass es zu jedem Benutzer, der ein Passwort in der `/etc/smbpasswd` hat, einen Benutzer im System geben muss. Der zu einer Workstation gehörende Benutzer muss den NetBIOS-Namen der Workstation, ergänzt um ein $-Zeichen, haben. Man benötigt also zwei Schritte, um eine Workstation in die Domäne aufzunehmen. Im ersten Schritt wird der Unixbenutzer angelegt. Dies geschieht in vielen Linuxsystemen mit dem Kommando `useradd -m < user >`. Der angelegte Benutzer benötigt im Unixsystem weder ein Passwort noch ein Heimatverzeichnis. Er ist notwendig, da die Workstation in der Domäne eine eigene SID bekommt, die aus der Unix userid berechnet wird. Dann muss die Workstation ein Passwort in der `/etc/smbpasswd` bekommen, und zwar mit dem Befehl `smbpasswd -a -m <name>`. Ein Beispiel sieht folgendermaßen aus:

```
root@diana: useradd -m wks\$
root@diana: smbpasswd -a -m wks
```

Man beachte, dass beim Befehl `useradd` ein Dollarzeichen, maskiert durch den Backslash, hinzugefügt wurde. Der Befehl `smbpasswd` fügt diesen bei Verwendung des Parameters `-m` selbst hinzu.
Samba als Domänenmitglied

Mit dem Parameter `security` kann man den Zeitpunkt steuern, zu dem das Benutzerpasswort geprüft wird. `security = share` legt fest, dass die Prüfung beim Tree Connect stattfindet, das heißt, wenn die Freigabe angesprochen wird. Ist `security = user` angegeben, wird das Passwort bereits einen Schritt vorher, also beim Session Setup geprüft. Bei `security = user` wird also die Kombination von Benutzer und Passwort geprüft bei `security = share` die Kombination Freigabe und Passwort.
Der Parameter `security` kann noch zwei weitere Werte annehmen: `server` und `domain`. Bei beiden Einstellungen verhält sich Samba gegenüber dem Client genau wie bei `security = user`, der Benutzer muss sich unter seinem Namen beim Server authentifizieren. Die Unterschiede liegen in der Art und Weise, wie das Passwort überprüft wird.

- `security = user` Die Überprüfung findet anhand einer lokalen Datenbank statt. Werden Klartextpasswörter verwendet (`encrypt passwords = no`), so wird die lokale Unix-Passwortdatenbank in `/etc/passwd, /etc/shadow` oder die entsprechende NIS-Tabelle herangezogen. Bei verschlüsselten Passwörtern mit wird die Samba-eigene Passwortdatenbank in der Datei `smbpasswd` zur Überprüfung herangezogen.

- `security = server` Bei dieser Einstellung bekommt der Sambaserver vom Client einen Benutzernamen und ein Passwort präsentiert. Er versucht daraufhin, sich mit diesem Passwort bei einem weiteren Server anzumelden. Funktioniert dies, hat der Benutzer sein Passwort offensichtlich richtig eingegeben. Schlägt dies fehl, wird auch dem Client des Sambaservers der Fehler mitgeteilt und der Zugriff verweigert. Der Passwortserver, der zur Überprüfung herangezogen wird, muss mit seinem NetBIOS-Namen im Parameter `password server` angegeben werden.

- `security = domain` Auch hierbei wird die Überprüfung einem Passwortserver überlassen. Dieser muss jedoch ein Primary Domain Controller sein, der den Sambaserver in die Domäne aufgenommen hat. Der Hauptvorteil gegenüber `security = server` besteht in einer deutlich reduzierten Last auf dem Passwortserver und einer verschlüsselten Kommunikation zwischen Samba und Passwortserver.

Um einen Windowsrechner dazu zu bringen, für einen Sambaserver die Passwortüberprüfung zu Übernehmen, muss man nur `security = server` und den `password server` passend setzen. Dabei übernimmt der Server ausschließlich die Überprüfung der Passwörter. Bei verschlüsselten Passwörtern können Benutzer nur dann in die `smbpasswd` aufgenommen werden, wenn sie in der Unix-Benutzerdatenbank existieren. Genau so verhält es sich bei `security = server`. Benutzer können auf Samba nur dann zugreifen, wenn sie als normale Unixbenutzer existieren.
`security = server` ist nicht die optimale Lösung für die Überprüfung von Passwörtern durch einen weiteren Rechner.
Um die Vorteile der Domänenmitgliedschaft zu nutzen, ist etwas mehr Aufwand notwendig. Mitglied einer Domäne zu sein heißt, mit dem Primary Domain Controller über einen verschlüsselten Kanal kommunizieren zu können. Diese Verschlüsselung wird verwendet, um Benutzerinformationen verdeckt austauschen zu können. Als Verschlüsselungsverfahren kommt ein symmetrisches oder auch secret key Verfahren zum Einsatz. Um ein symmetrisches Verfahren anwenden zu können, müssen sich beide Partner über ein gemeinsames Geheimnis, den secret key einig sein. Ein solches gemeinsames Geheimnis muss regelmäßig geändert werden, um einer großen Klasse von kryptographischen Angriffen auszuweichen. Eine solche Änderung darf selbstverständlich nicht abgehört werden können, da ein Zuhörer damit die gesamte Kommunikation abhören kann. Für die Änderung eines Geheimnisses gab es bereits vor der Implementation des Domänenprotokolls ein fertiges Protokoll, das man direkt verwenden konnte: Die Möglichkeit, Benutzerpasswörter über das Netz zu ändern, war mir einem gesicherten Protokoll implementiert. Um dieses Protokoll zur verschlüsselten Kommunikation zwischen einer Workstation oder einem Mitgliedsserver und dem Domänencontroller nutzen zu können, muss es für jedes Domänenmitglied ein Benutzerkonto geben. Genau dies wird auf dem Domänencontroller erstellt, wenn man eine Workstation oder einen Server mit dem Servermanager in die Domäne aufnimmt. Betritt man danach mit der Workstation die Domäne, wird als erstes das Passwort des Computerkontos geändert.
Um einen Sambaserver in eine Domäne aufzunehmen, sind zwei Schritte notwendig.

- Auf dem Server muss der Sambaserver mit seinem NetBIOS-Namen in die Domäne aufgenommen werden.
- Der Sambaserver selbst muss darüber informiert werden, dass er sich in der Domäne befindet, und er muss sein Passwort ändern. Dies geschieht mit dem Befehl

  ```
  smbpasswd -j DOM -r PDC
  ```

  Dabei steht DOM für die Domäne, die betreten wird. Mit PDC wird der NetBIOS-Name des Domänencontrollers der Domäne benannt.

Mit diesem Kommando wird das Maschinenpasswort auf dem PDC auf einen neuen, zufälligen Wert geändert. Dieses neue Maschinenpasswort für den Samba Server wird in einer Datei im gleichen Verzeichnis wie die Datei `smbpasswd` abgespeichert und hat folgenden Namen:
`<NT DOMAENENNAME>.<Samba Servername>.mac`
Die Endung .mac steht für *Machine ACcount* Passwortdatei. Im obigen Beispiel würde die Datei also DOM.SERV1.mac heißen. Diese Datei wird von root erstellt und ist für keinen anderen Benutzer lesbar. Sie ist der Schlüssel zu Ihrer Domänensicherheit und sollte genau so vorsichtig behandelt werden wie die Datei `/etc/shadow`.
Nach diesen beiden Schritten kann man mit `security = domain`, `password server = PDC BDC1 BDC2` und `encrypt passwords = yes` die Passwortüberprüfung an einen der Domänencontroller delegieren. Dies sind die Primären und Backup Domänencontroller, die Samba der Reihe nach kontaktieren wird, um Benutzer zu authentifizieren. Samba wird sie in der aufgeführten Reihenfolge ansprechen. Sie können also die Reihenfolge verändern, um eine günstigere Lastverteilung zu erreichen. Eine weitere Option ist die Angabe `password server = *`. Damit sucht Samba mit den Standardmethoden von Windows NT nach einem Domänencontroller und befragt die Server, die es bei dieser Anfrage herausbekommen hat.
Warum ist `security = domain` besser als `security = server`? Der Vorteil der Domänensicherheit ist, dass Samba die Authentifizierung über einen gesicherten RPC Kanal schickt, genau wie ein Windows NT Server es tun würde. Das heißt, dass Samba nun genau wie ein Windows NT Server an einer Vertrauensstellung teilnehmen kann. Das heißt, Sie können einen Samba Server in eine Resourcendomäne aufnehmen, und Sie können

die Authentifizierung via Resourcen PDC vom PDC der Benutzerdomäne vornehmen lassen.
Zusätzlich muss in der Einstellung `security = server` der Samba Daemon eine Verbindung zum Authentifizierungsserver während seiner gesamten Laufzeit offenhalten. Dies kann die Anzahl der offenen Verbindungen auf einem Windows NT Server in die Höhe treiben, so dass dieser keine Verbindungen mehr annimmt. Mit `security = domain` verbinden sich die Samba Daemonen nur so lange mit dem PDC, wie es für die Benutzerauthentifizierung notwendig ist. Danach wird die Verbindung wieder abgebaut, so dass die Verbindungen wieder anderweitig verwendbar sind.
Und nicht zuletzt bekommt der Samba Server als Teil der Antwort auf die Authentifizierungsanforderung Informationen über den Security Identifier, die Gruppenzuordnungen und andere Informationen über den Benutzer. Alle diese Informationen werden Samba zukünftig erlauben, in einem sogenannten Appliance Modus zu laufen. In diesem Modus wird kein manuell angelegter Unixbenutzer mehr notwendig sein. Samba wird Unix Benutzer und Gruppen aus der Authentifizierungsantwort des PDC erzeugen. Damit wird Samba wirklich ein Plug and Play Mitglied einer Domäne.
Dieser Appliance Modus kann heute schon annähernd erreicht werden, indem bei Samba der Parameter `add user script` angegeben wird. In diesem Parameter wird ein Unixprogramm angegeben, das dynamisch einen Unixbenutzer erzeugen muss, nachdem ein Passwortserver die Korrektheit eines Passworts bestätigt hat. Ein Beispiel kann sein:

```
add user script = /usr/bin/useradd -m %U
```

Damit wird einfach ein Benutzer hinzugefügt, wenn er noch nicht existiert, aber der PDC das Passwort bestätigt hat.