1. Was tun, wenn root-Password vergessen:

1) - neu booten bis Bootmanager
- im Grub anhalten
- Parameterliste ergänzen mit "init = /bin/bash"
=> nur über die bash wird gestartet
=> Tastaturbelegung ändert sich (default)
=> kennt keine Benutzer
=> System nur im Lese-Modus

2) Tastaturbelegung wieder ändern:
- mit kbd (keyboardeamon) => Treiber wird geladen
- starten: "/etc/init.d/kbd start"

3) System im Schreib-Lese-Zugriff mounten:
- "mount /dev/sda2 / -o remount, rw"
//root-filesystem root optionen: remounten im S/L-Modus

4) /etc/shadow: root-Passwort löschen (keine Leerzeichen lassen)

5) neu starten

6) Start als Root --> PW-Abfrage nicht notwendig --> Eingabe des neuen Root-Passwortes

==> SICHERHEITSLÜCKE:
- offen so lange man im GRUB noch Parameter eingeben kann
- in der Konfiguration des Bootmanagers kann man dies ändern, aber dann ist es nicht mehr möglich als root ohne Passwort zu sarten.

2. Systemüberwachung- und Wartung:

"ps -axl" a: Prozesse aller Nutzer
x: Prozesse, die nicht an ein Terminal gebunden sind
l: ausführliche Ausgabe (Prozessname und ID werden immer angegeben)

"top"

3. Systemprotokolle

- /var/log/messages: alle Protokolle + Nachrichten (unübersichtlich)
- syslogd => syslog-Deamon:
- hat eigene Konfigurationsdatei
- legt fest WER WAS WOHIN schreiben darf (s. Konfigurationsdatei)
- in /etc/syslog.conf
- braucht 3 Informationen:

- WER (welcher Dienst gibt die Meldungen)
- WELCHE Dringlichkeit
- WAS soll syslog tun?

=>	WER	Dringlichkeit	WAS
	kernel	debug	auf Konsole ausgeben
	cron	info	in Datei xy schreiben
	make	notice	an root mailen
	auth	warning	an alle eingeloggten User ausgeben
	...	err	
		crit	
		alert	
		emerg	

- Inhalt in syslog.conf:

  WER.Dringlichkeit (tab)WAS

--> Syntax

"kern.warn; * .err; authpriv.none /dev/tty10"

--> kern: alle Meldungen vom Kernel

--> .warn & .err: alle Meldungen warn / err oder dringender

--> *: alles

--> authpriv.none: nicht berücksichtigen

--> tab als Trenner

"*.emerg *"

--> alle emergency-Meldungen an alle User

4. Übung: auf einer Textkonsole die Login-Info ausgeben:

- Eintag in syslog.conf:

  "auth.* /dev/tty4" ODER

  "auth.debug /dev/tty4"

- nach Änderung syslogd neu starten mit:

  "/ect/init.d/syslog restart" ODER

  "rcsyslog restart"

5. Anmerkung Startskripte:

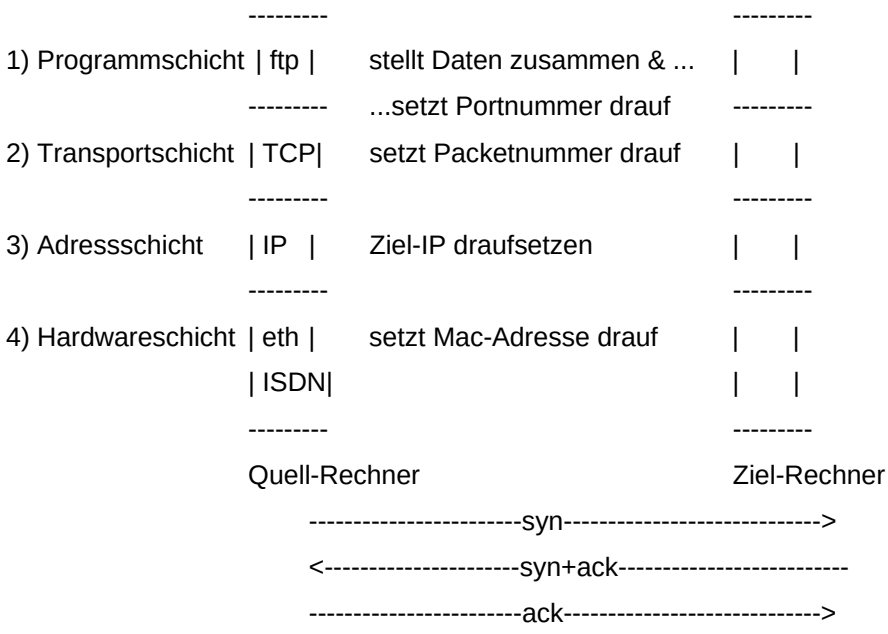
```
-------------------------------------------------------------------------------
|ANMERKUNG Startskripte:                                                      |
|     - /etc/init.d # ./syslog                                                |
|     - rcsyslog     Links auf Startskripte in /usr/sbin                      |
|                 können von allen Verzeichnissen erreicht werden             |
-------------------------------------------------------------------------------
```

6. CronTab:
   - crond:
     - /etc/crontab => wann was gemacht werden soll (z.B. Backup)
     - Inhalt:

```
Min  Std  Tag Monat    WTag     Job (der gemacht werden soll)
-------------------------------------------------------------------
10   |*    |*    |*          |*          |
--> Job soll 10 Min nach jeder bel. Std, jedem bel. Tag, Monat, WTag gemacht
werden
*/15 |     |     |           |           |
--> alle 10 Min ausführen
     |     |     |           |4          |
--> immer mittwochs
```

     - nicht über syslog protokollieren

7. Netzwerk:
   1. Protokolle:
      - TCP/IP: transfer control protocol / internet protocol
      - ICMP: internet control message protocol (verwendet von PING, ...)
      - UDP: user datagram protocol (verwendet von nfs, dns, ...)
   2. Schichten:



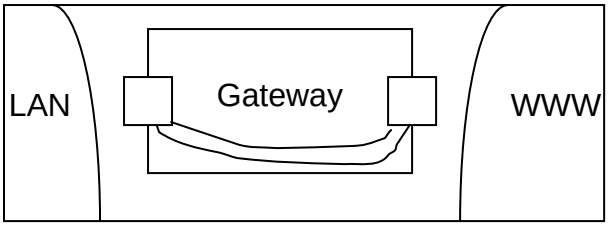
3. wichtige Pfade:
   - /etc/sysconfig/network/ifcfg-eth0 => Netzwerkkarte
   - /etc/HOSTNAME => enthält Hostname des Rechners
   - /etc/sysconfig/network/routes => Wegewahltabelle
   - /etc/host.conf:
     Zeile: "order hosts, bind"
     --> falls der Rechnername über /etc/hosts aufzulösen ist
     --> sonst in der /etc/resolv.conf suchen

4. Routing:
   - Wegewahltabelle:
     - in /etc/sysconfig/network/routes ODER Kommando "# route"
     - Inhalt:
       Destination Gateway Genmask Flags Metric Ref Use Iface
     - Eintrag löschen ("del"):
       - "# route del -net 0.0.0.0" --> löscht Route ins Internet (default)
       - "# route del -net ZIEL-IP netmask MASKE" --> best. Eintrag lö.
     - Eintrag einfügen ("add"):
       - "# route add -net ZIEL-IP netmask MASKE eth0"
       - "# route add -net 0.0.0.0 gw GATEWAY eth0" --> Route ins Internet (def)

5. Server und Clients:
   1) Dienstleistung | Server

Fileserver	nfs: Network File Server
	samba: zwischen Windows-Linux (meist W-Server & L-Clients)
Webserver	apache
DB-Server	mysql
Mailserver	sendmail, postfix
FTP-Server	inftp, wuftp
Proxy-Server	squid
Packetfilter	im Kernel integriert
startet Dienste	inetd

2) Gateway, IP-Forwarding, Masquerading



=> IP-Forwarding: IP-Pakete werden direkt weitergeleitet

/proc/sys/net/ipv4/ip_forward

Masquerading: wenn Pakete aus dem lok. Netz ins WWW weitergeleitet werden, dann ersetzt er die IP durch seine eigene IP

3) DHCP: dynamic host configuratio protocol
- dhcpd: dhcp-Deamon
  - Konfigurationsdatei: /etc/dhcpd.conf
  - liefert IP d. Gateways, von Nameservern
  - Nachteile: IP wird dyn. zugewiesen

4) DNS: domain name server
- named
  - Konfigurationsdatei: /etc/named.conf
  - Zone-Dateien: /var/named
  - Zeile:"notify no" --> nach aussen nicht sichtbar
    "zone localhost ... "localhost.zone"" --> Datei /var/named/localhost.zone
    "type master" --> alle Anfragen von localhost werden von diesem Nameserver bearbeitet
    "zone 0.0.127.in-addr-arpa" --> Datei /var/named/127.0.0.zone