Netzboot mit PXE

Sicherheitstage SS 2007

Hergen Harnisch

harnisch@rrzn.uni-hannover.de

21.06.2007

Netzboot allgemein:

- Entwicklung
- Anwendungen
- Novell (Rückblick)
- Probleme

PXE-Bootvorgang:

- Ablauf
- Client-Rom

Server-Konfiguration

- `DHCPD`
- `TFTPD`
- PXELinux

PXE als Environment

- PXELinux
- Alternativen

Vorbemerkung

Sicherheit?

- Disaster Recovery & Verfügbarkeit
- Thin-Client („Netz-PC“)
- regelmäßiges Neuaufsetzen entfernt Root-Kits etc.
- schnellere Updates möglich
- schnell zur Hand: Update-Tools & sauberes Scannen

Beschränkung auf PCs, nicht auf Linux

Trotz des Namens ist das u.A. vorgestellte Paket Syslinux und das enthaltene PXELinux nicht auf Linux beschränkt, es war nur ursprünglich ein Bootloader für Linux.

R|R|Z|N

Unix etc.

- bei Workstations schon lange mit `RARP` & `TFTP`
- X-Terminals ohne Festplatte
- später statt `RARP` eher `BootP` und nun `DHCP`
- Macs können seit MacOS-X / OpenFirmware via `TFTP` booten

Zweck

- Installation (insb. als es noch keine CDs gab)
- Diskless Clients
- zentrale OS-Konfiguration,
  insbesondere Cluster

Ablauf

1. Netzwerkkonfiguration (`RARP`, `BOOTP`, `DHCP`)
2. Image laden (`TFTP`) & starten

PC

- üblich zu DOS-Zeiten (Clients ohne Festplatte)
- mit Windows $\geq$95 schwierig, da Festplatte fast nötig,
  mit Windows NT4.0 & $\geq$2000 praktisch unmöglich
- Linux-Clients unproblematisch

Implementationen

- IBM RPL (LAN-Manager, Dos, OS/2, Novell)
- Novell-Netware NCP/IPX ⟵ kurze Erinnerung
- DHCP/BootP & TFTP ⟵ auch kurz
- etherboot (Open-Source)
- Intel PXE (Preboot Execution Environment)
  - anfänglich Inkompatibilitäten, extra PXE-Daemon
  - heute normaler DHCP-Daemon ausreichend ⟵ Hauptfokus

Netzboot allgemein: Anwendungen

- Installation:
  - interaktiv, aber ohne CD
  - automatisiert (z.B. mit Preseed bei Debian, RIS bei Windows)
- Thin-Client:
  - Linux (Knoppix, Ubuntu)
  - Terminal (X11, RDP, Citrix)
- Administrations-Hilfen:
  - Festplatten-Images sichern & einspielen
  - DOS booten für BIOS-Update
  - Speichertest
  - Virenscanner, forensische Tools
  - Datenrettung bei defekter lokaler OS-Installation
- Thin-Server:
  - Print-Server
  - Messrechner im Labor
  - Server mit NAS- / SAN-Anschluss
  - Firewall, Proxy

NCP/IPX-Boot

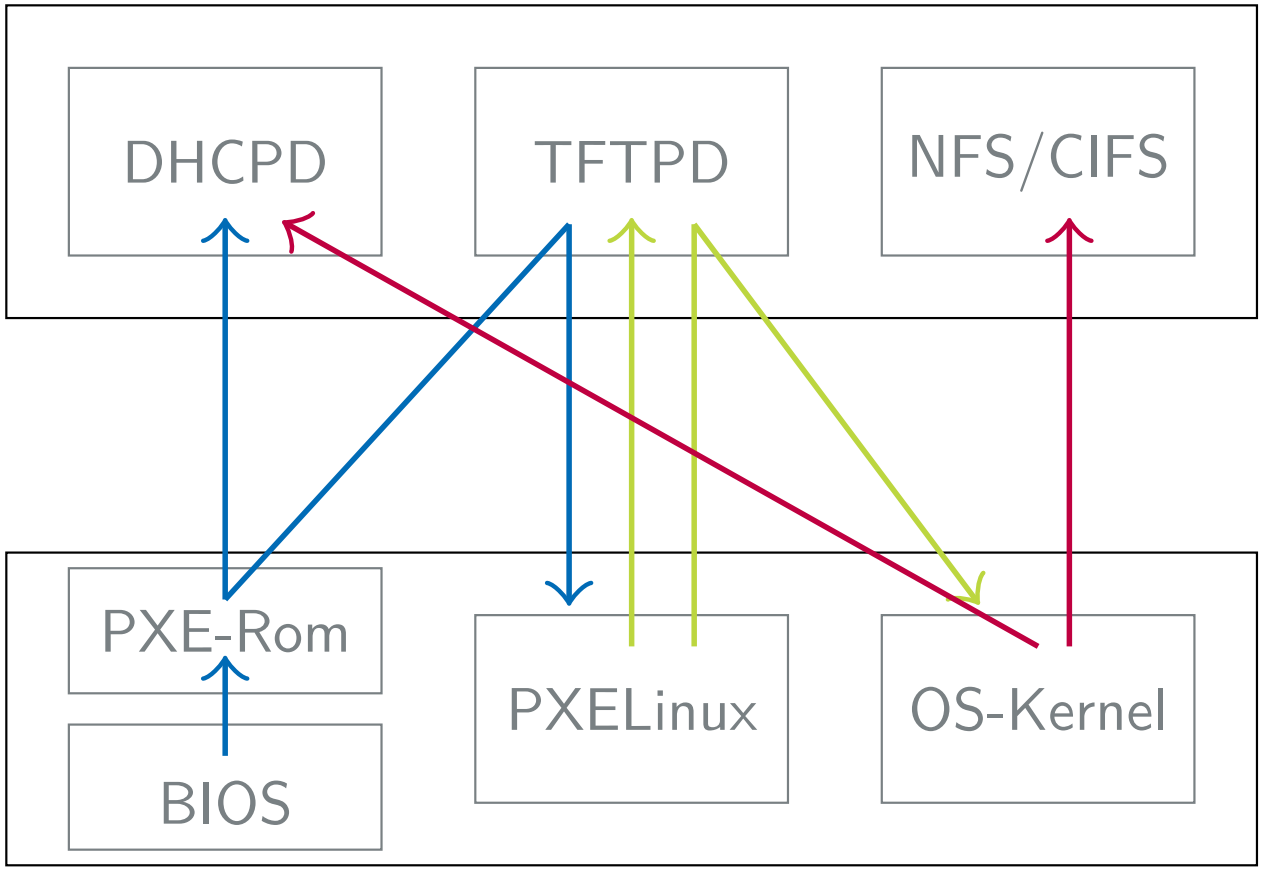
- ROM auf Netzwerkkarte biegt BIOS-Int 19h oder 18h um
- Netzwerkkonfiguration leichter als bei IP
  (kein Gateway, MAC-Adresse reicht, Server via Broadcast)
- Dateien vom Server aus immer lesbarem `SYS:\LOGIN`
- `SYS:\LOGIN\BOOTCONF.SYS` definiert zu ladendes Image
  (je nach MAC-Adresse; Default ist `NET$LOG.SYS`)
- Disketten-Image wird aus `SYS:\LOGIN` geladen
- Image ersetzt Floppy-Laufwerk `A:` (BIOS Int 13h umgebogen)
- Image wird vergessen bei Laden des Novell-Clients `NETX.EXE`,
  Floppy-Laufwerk wieder ansprechbar als `A:`

Netzboot allgemein: Probleme

- Image-Formate
  - Disketten-Image
  - Kernel-Image (z.B. elf,nbi)
  - OS-abhängiger Bootloader (DOS-Bootsektor, ntldr)
- Betriebssysteme eher auf lokale Medien (Festplatte) ausgelegt
- Disketten-Simulation:
  - Simulation nur bei Nutzung BIOS Int 13h, keine Hardware-Simulation
  - Kopie im RAM, darf nicht überschrieben werden
  - irgendwann muss Simulation/RAM augegeben werden
- Boot-Images zu klein, meist extra Dateisystem nötig
  - lokale Platte (als Option oder für Applikationen)
  - Netzlaufwerk
  - RAM-Disk
- Image-/OS-Auswahl, rechnerindividuell oder per Boot-Menü

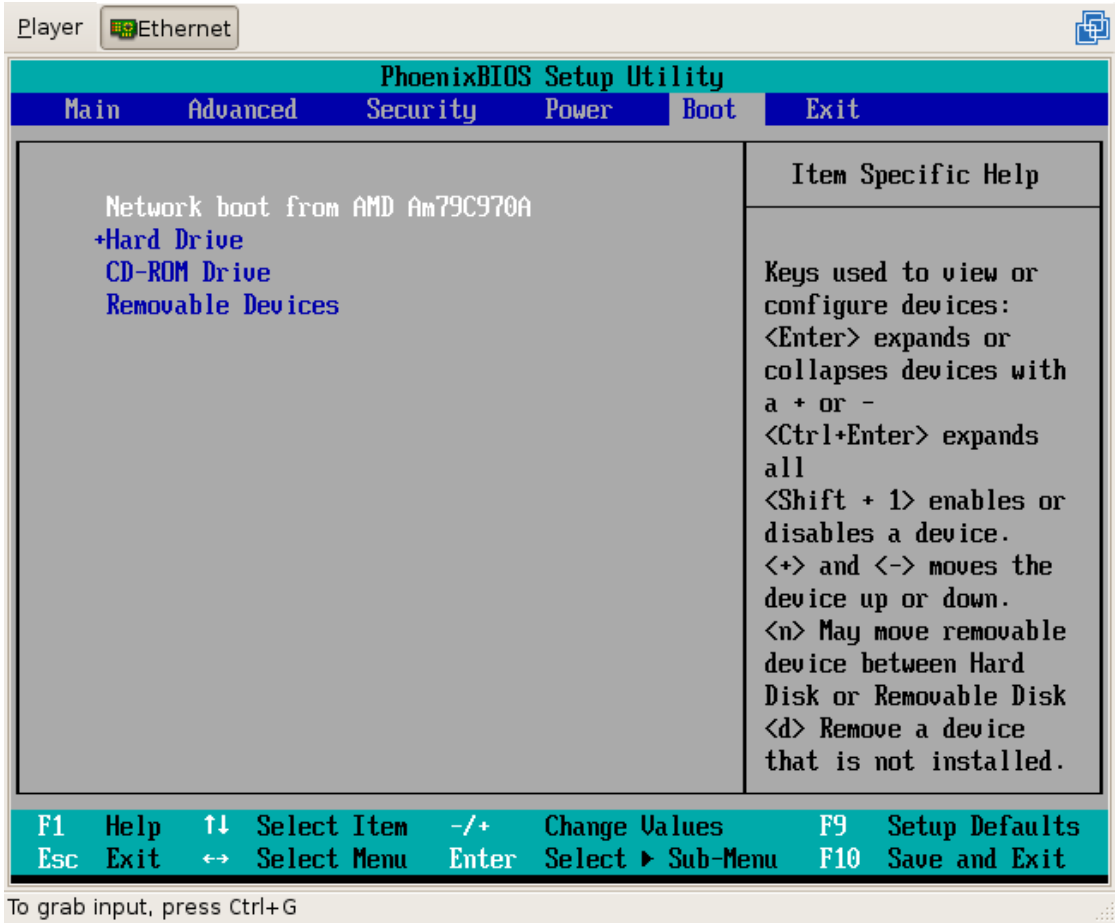
R|R|Z|N

Schema


DHCPD
TFTPD
NFS/CIFS
Server
3. OS
2. pxelinux.0
1. Firmware
PXE-Rom
BIOS
PXELinux
OS-Kernel
Client

R|R|Z|N

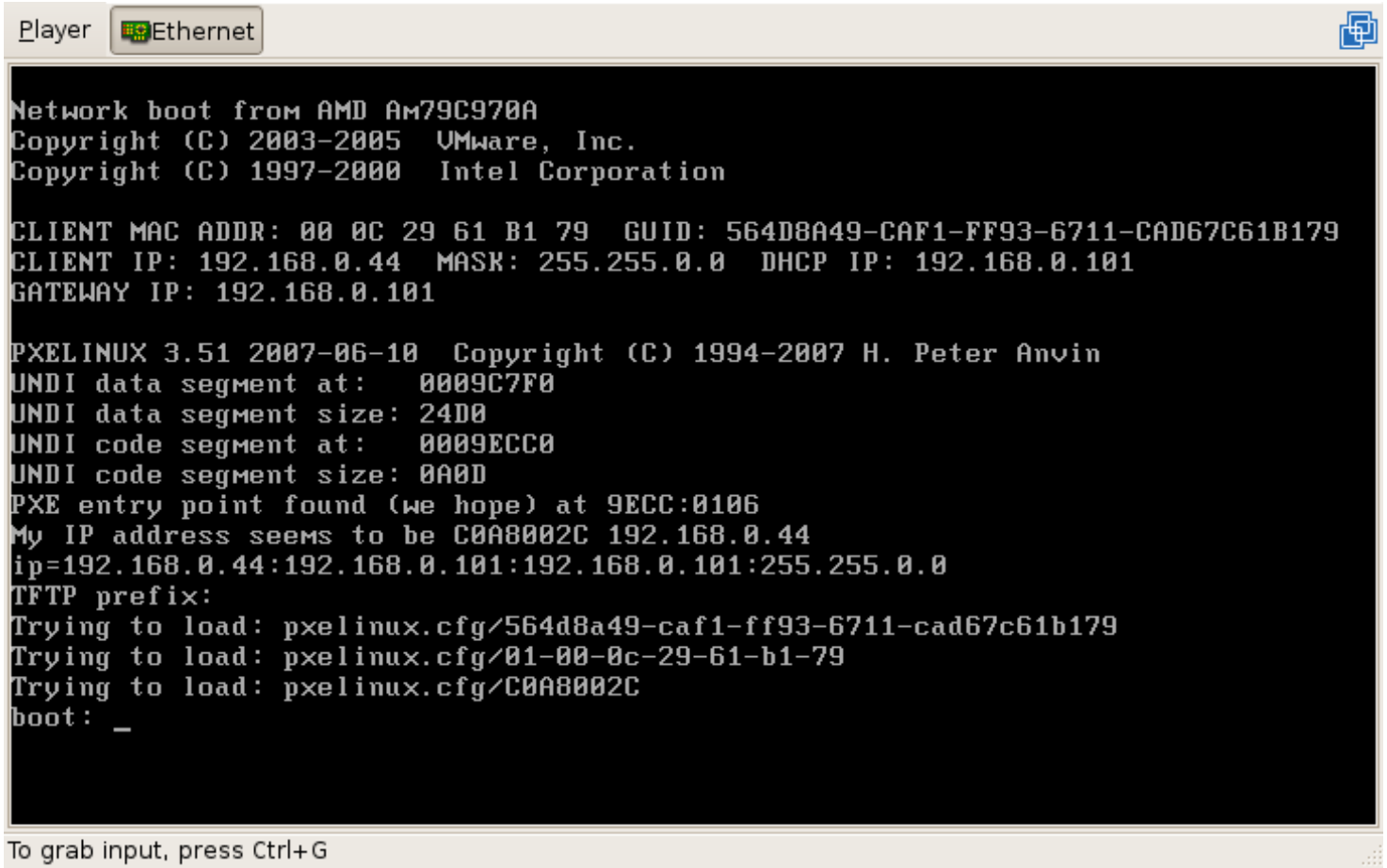
Bios-Einstellung



Bootreihenfolge oder per BIOS-Bootmenu: PXE/MBA; Int19/18h

R|R|Z|N

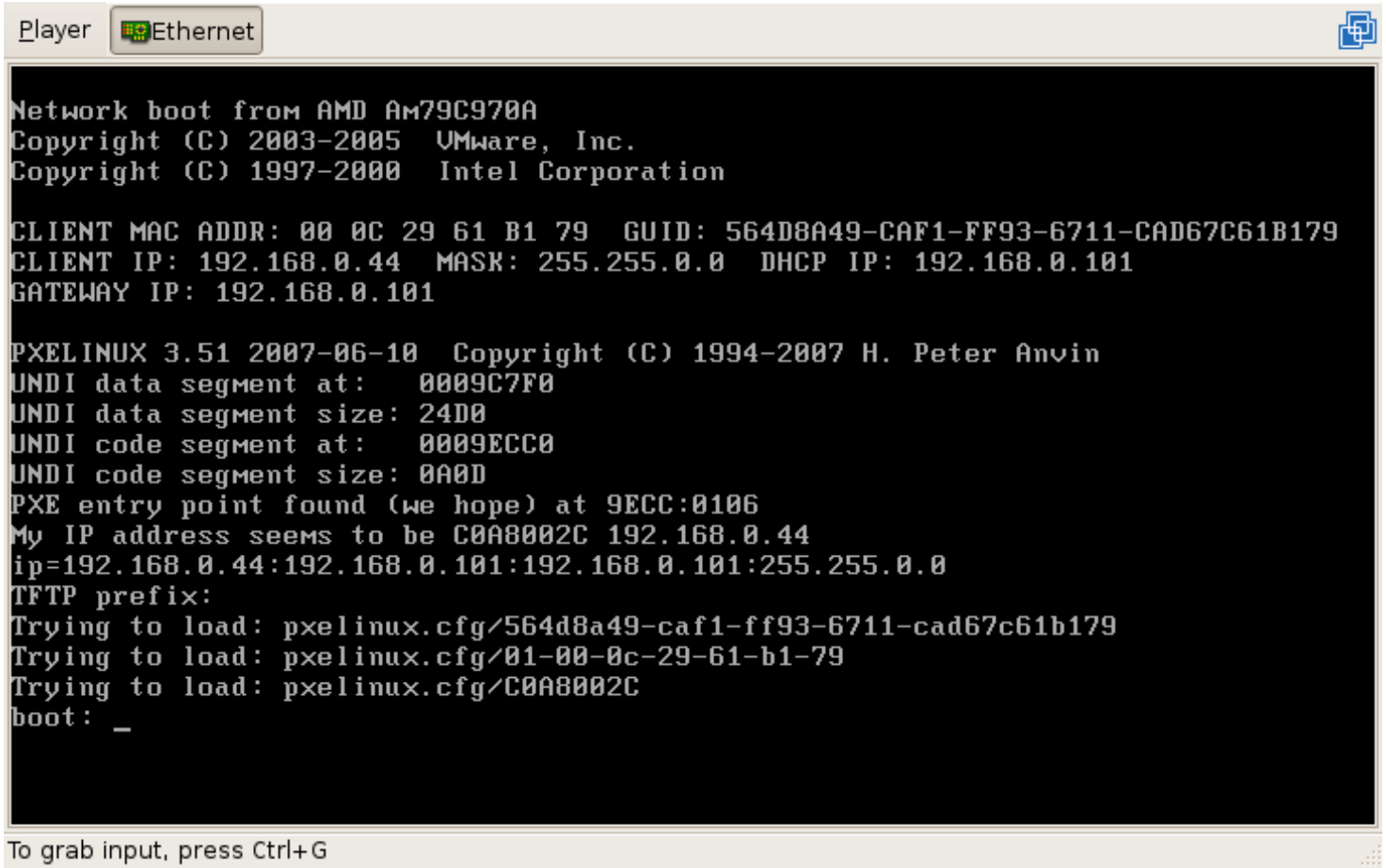
PXE-Rom



Netzwerkkarte initialisieren, IP-Stack, DHCP, 1. TFTP-Image

R|R|Z|N

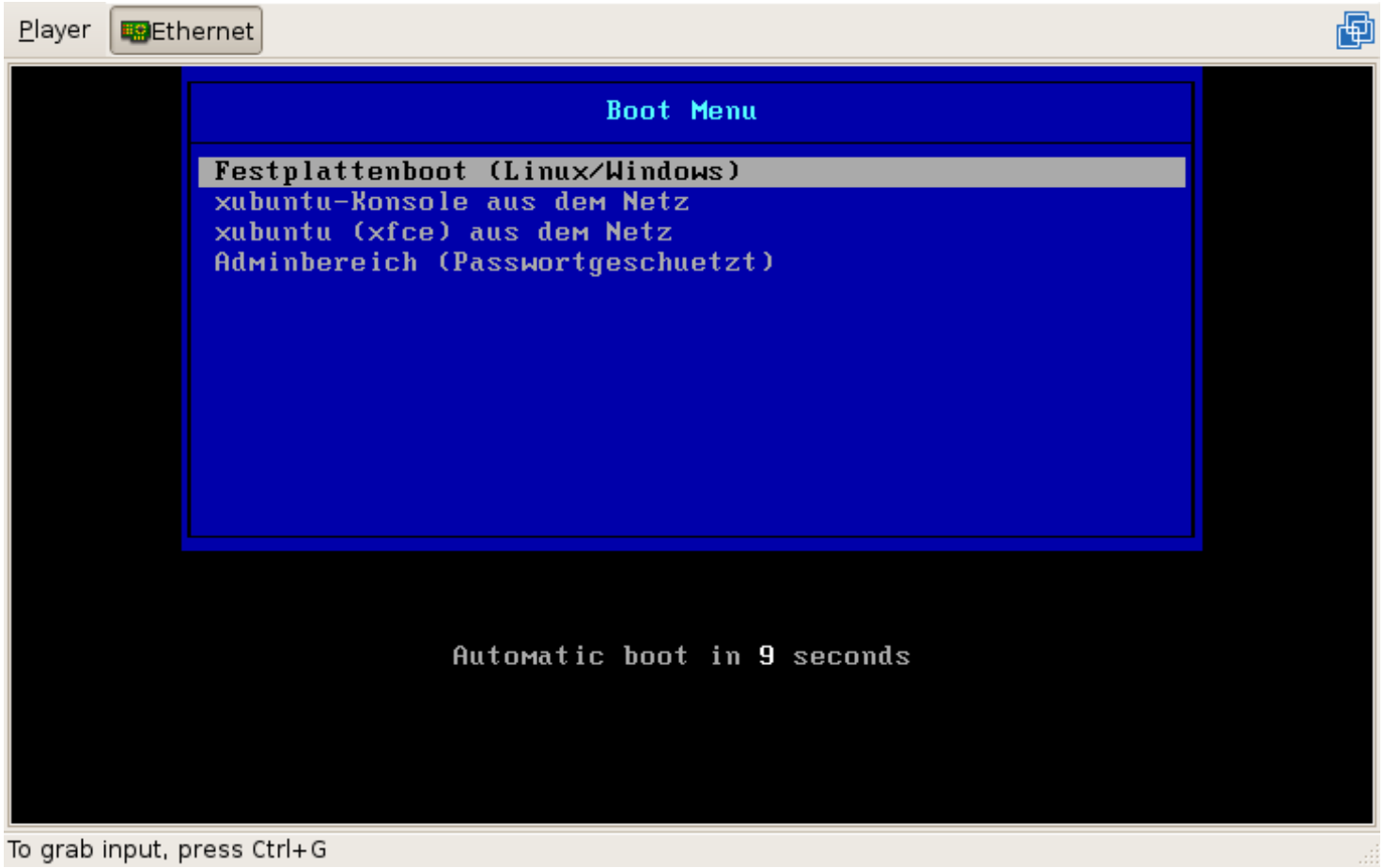
PXELinux



PXELinux-Start, -Konfig suchen/laden, -Prompt

R|R|Z|N

PXELinux - Menü



PXELinux-Start, -Konfig suchen/laden, -Prompt...

PXE-Rom im Client

- häufig im BIOS für motherboard-integrierte Ethernet-Schnittstellen
- evt. im Flash/Eprom einer Netzwerkkarte (nachrrüstbar)
- ROM eigentlich auf bel. Karte oder im BIOS nachrüstbar[1]
- ROM von Floppy, CD, USB-Stick oder Flash-Drive
  $\longrightarrow$ gut für erste Tests, Medien nur einmal zu erstellen
- kommerzielle ROM-Implementationen nachkaufbar
- oder mit etherboot als Open-Source,
  Online-Generierung mit PXE: `http://rom-o-matic.net/`
- *zum Testen:* VMWare, Virtualbox haben PXE im Gast-BIOS
- PCMCIA-/Cardbus-, USB- oder WLan-Adapter gehen nicht

[1] im Internet beschriebene Bastelei, lieber nicht!

R|R|Z|N

„Zutaten“

nötige Serverdienste

- DHCP
- TFTP
- ggf. NFS, CIFS/SMB
- bei privaten IPs: ggf. Natting, DNS für private

für Dateien im TFTP

- Paket Syslinux (enthält PXELinux)
- Dateien für Client-OS

. . . folgend für Debian-Etch

Server-Konfiguration DHCPD

1. ISC-DHCP-Server 3 installieren mit
   `aptitude install dhcp3-server`
2. Konfiguration für alle Clients
   - Netzmaske, Gateway, DNS-Server
   - TFTP-Server (wenn abweichend)
   - initiales Boot-Image
3. für jeden Host: MAC-Adresse – Hostname/IP

/etc/hosts (optional)

```
130.75.8.15    demopc.rrzn.uni-hannover.de demopc
```

/etc/dhcp3/dhcpd.conf

```
option domain-name-server 130.75.1.32, 130.75.1.40;
subnet 130.75.8.0 netmask 255.255.255.0 {
  option broadcast-address 130.75.8.255;
  option routers 130.75.8.250;
  option domain-name "rrzn.uni-hannover.de";
  next-server "tftp.rrzn.uni-hannover.de";
  filename "pxelinux.0";
  use-host-decl-names on;
  host demopc {
    hardware ethernet 00:00:00:52:52:5A:4E;
    fixed-address demopc.rrzn.uni-hannover.de;
  }
}
```

1. TFTP-Server installieren:
   `aptitude install atftpd`
   (Daemon muss `tsize`-Option unterstützen, Debian-Paket tftpd ungeeignet, atftpd und tftpd-hpa gehen)
2. egal: über `inetd` oder standalone
3. Multicast nicht von PXELinux unterstützt, Images sowieso klein
4. statt `/tftpboot` lieber `/srv/tftpboot` (wg. LFH)
5. Rechte für Dateien in `/srv/tftpboot`:
   - lesbar für `nogroup.nobody`
   - Schreibrechte gefährlich, da TFTP unauthentifiziert

- Syslinux-Paket installieren (oder direkt `.tar.gz` holen):
  `aptitude install syslinux`
- Dateien umkopieren (oder linken):
```
cp /usr/lib/syslinux/pxelinux.0 /srv/tftpboot
cp /usr/lib/syslinux/{memdisk,menu.c32} \
                                /srv/tftpboot/pxelinux.msc
```
- Client-Boot-Konfiguration:
```
# /srv/tftpboot/pxelinux.cfg/default
LABEL harddisk
  LOCALBOOT 0
LABEL linux
  KERNEL vmlinuz.knl
  APPEND initrd=initrd.ird
```

Bemerkung: Boot mit Syslinux ähnlich von USB-Stick, mit Isolinux von CD/DVD konfigurierbar, trotz der Namen für alle Betriebssysteme.

Server-Konfiguration PXELinux

R|R|Z|N

ls -l /srv/tftpboot

```
drwxr-xr-x 2 root root ... knoppix
-rw-r--r-- 1 root root ... pxelinux.0      ⟵ PXE-Bootloader
drwxr-xr-x 2 root root ... pxelinux.cfg    ⟵ Boot-Konfig.
drwxr-xr-x 2 root root ... pxelinux.msc    ⟵ Addons
drwxr-xr-x 3 root root ... xubuntu
```

ls -l /srv/tftpboot/pxelinux.msc

```
-rw-r--r-- 1 root root ... german.kbd      ⟵ dt. Tastatur
-rw-r--r-- 1 root root ... memdisk         ⟵ Floppy-Emulation
-rw-r--r-- 1 root root ... menu.c32        ⟵ Menu-Prg.
```

ls -l /srv/tftpboot/pxelinux.cfg

```
lrwxrwxrwx 1 root root ... 824B080F -> service  ⟵ 130.75.8.15
lrwxrwxrwx 1 root root ... default -> standard ⟵ Standard
-rw-r--r-- 1 root root ... service
-rw-r--r-- 1 root root ... standard
```

PXE als Environment PXELinux

- PXE-Rom bietet eine PXE-API, die `pxelinux.0` nutzt
- `pxelinux.0` bietet selbst API
- `*.c32`-Programme von PXELinux nutzen diese, z.B. `chain.c32`, `menu.c32`
- `memdisk` ist spezieller „Kernel“, der Floppy-Image als „InitRD“ erhält
- Direktiven in PXELinux-Konfig für:
  - Starten von `*.c32`-Anwendungen
  - Booten von Festplatte / lokalen Laufwerken
  - (Linux-) Kernel
  - Textausgabe, Prompt

PXE als Environment Alternativen

R|R|Z|N

Es gibt auch andere PXE-Bootloader als PXELinux:

- grub (noch nicht lange)
- BSD hat PXE-Bootloader
- bpbatch: integriertes Tool zum Partitionieren, Formatieren, Image erstellen/einspielen
  (früher kostenlose Privatnutzung und kleines Tool, heute Bestandteil von IBM-Tivoli)
- Novell Zenworks
- Microsoft Remote-Installation-Service (RIS)
- Symantic Norton Ghost

Mit PXELinux immer Chaining in anderen PXE-Bootloader möglich.

R|R|Z|N

Sicherheit

Vorteile

- „Read-Only-OS“ vom Server umgeht Malware auf Client
- einfaches verlässliches Scannen nach Malware
- Disaster-Recovery:
  - einfacher Hardware-Wechsel
  - schnelles Wiederaufsetzen
- regelmäßiges Wiederaufsetzen
  - vernichtet Malware auf Client,
  - ermöglicht einfache Updates

R|R|Z|N

Sicherheit

Nachteile / Probleme

- SPoF: ohne `DHCPD` & `TFTPD` kein Netzboot
- `DHCP` per Broadcast:
  wilde `DHCP`-Server können bootenden PC übernehmen
- MitM: keine Serverauthentifizierung bei `DHCP` & `TFTP`
- keine Clientauthentifizierung,
  (höchstens Userberechtigung im Client per Hash)

Probleme ließen sich höchstens mit TPM lösen ...

R|R|Z|N

an der Uni

Anwendungsbereich

- unbedingt empfehlenswert für (CIP-) Pools,
- evt. für gleichartige Desktops und
- als Administrationshilfe bei Servern / Arbeitsplätzen im LAN

Hinweise

- `DHCPD` sollte statisch IPs zuweisen
- RRZN-Beispiel-Images & -Skripte
- Tests mit VMWare od. Virtualbox möglich, Konfiguration PXELinux auch lokal mit Syslinux auf USB-Stick testbar

Links

- etherboot (PXE-Rom für Client):
  `http://www.etherboot.org/`, `http://rom-o-matic.net/`
- syslinux (pxelinux, auch für CD-Rom / HD / USB-Stick):
  `http://syslinux.zytor.com/`