Linux im Netzwerk

Martin Steigerwald
<ms@teamix.de>

Linux User Schwabach (LUSC)
mit freundlicher Unterstützung der team(ix) GmbH

16. April 2005

Inhalt I

1. Netzwerk-Grundlagen
   - Was ist ein Netzwerk?
   - Übertragungsmedien und Netzwerk-Topologien
   - Protokolle und Schichten
   - Netzwerk-Hardware
   - Adressen und Hostnamen
   - Netzwerke und andere Dinge
   - Routing
2. Mit Linux ins Netz
   - Treiber laden
   - Netzwerk konfigurieren
   - Routing oder: Ich will Internet

Inhalt II

- DNS oder: Ich will Namen tippen
- Alles ganz automatisch mit DHCP
- Geht alles?

3 Tausend Möglichkeiten

- Konfiguration und Analyse von Netzen
- Dateien tauschen
- WWW
- Sicherheit
- Linux als Router
- Auf entfernten Systemen arbeiten
- Was geht sonst noch so?

4 Infos

Was ist ein Netzwerk?
Übertragungsmedien und Netzwerk-Topologien
Protokolle und Schichten
Netzwerk-Hardware
Adressen und Hostnamen
Netzwerke und andere Dinge
Routing

Was ist ein Netzwerk?

- mehrere Computer ...
- die miteinander kommunizieren (Datenaustausch)
- Verbindungen zwischen Computern über einen Kommunikationsweg (Medium)
- gemeinsame Spache nötig (Protokoll)
- Anwendungen, die Daten austauschen (Server und Client)

Übertragungsmedien

- Kabelgebunden
  - Elektronenleiter: Kupferkabel
  - Lichtwellenleiter: Glasfaser
- Drahtlos
  - Funkwellen: WLAN, Bluetooth
  - Lichtwellen: Laser

Übertragungsmedien

Gebräuchlich im Heimbereich

- Kupferkabel
- WLAN

Netzwerk-Topologien

- Bus-Struktur, z.B.: 10Base-2
- Ring-Stuktur, z.B.: Token Ring
- Stern-Struktur, z.B.: 10Base-T, 100Base-T, 1000Base-T
- Punkt-zu-Punkt, z.B.: Modem und ISDN (PPP), diverse Standleitungen, VPN-Verbindungen

Netzwerk-Topologien

Gebräuchlich im Heimbereich

- Stern-Struktur
- früher auch Bus-Struktur

Protokolle - Sprachen des Netzes

Computer im Netz brauchen zur Kommunikation eine gemeinsame Sprache, damit sie sich verstehen

- Unterschiedliche Sprachen für verschiedene Anwendungsfälle:
  - HTTP u.a. fürs Web
  - SMTP, POP3, IMAP für E-Mail
  - Ethernet für Netzwerkkarten
- Standardisierte Sprachen:
  - IETF erstellt RFCs (Request for Comment)
  - RFCs definieren oft nur Teile einer Sprache (z.B. RFC 1918: IP-Adreßbereiche für private Netze)

Schichten-Modell

Netze sind etwas komplexes: Daher Aufteilung in Schichten

- Standardisierte Schnittstellen: Austauschbarkeit einer einzelnen Schicht, ohne den Rest zu berühren
- Vom Speziellen (Hardware) zum Allgemeinen (Anwendungen): Hardware-Unabhängigkeit
- ISO/OSI-Schichtmodell (7 Schichten) eher akademisch
- TCP/IP-Schichtmodell (4 Schichten) heutige Praxis

TCP/IP-Schichtenmodell

- Schicht 1: Netzzugangs-Schicht (Ethernet)
- Schicht 2: Internet-Schicht (IP)
- Schicht 3: Transportschicht (TCP, UDP, ICMP)
- Schicht 4: Anwendungsschicht (HTTP, FTP, SMTP, SSH)

Netzwerk-Hardware am Beispiel von Ethernet

- Computer (mit Netzwerk-Software)
- Ethernet-Netzwerkkarte (von Linux unterstützt, gut geeignet z.B.: Intel E100)
- Kabel (gebräuchliches Cat5-Kabel, “Twisted Pair”-Kabel)
- Switch (Schaltzentrale, in der alle Kabel zusammenlaufen)
  - Leitet typischerweise Ethernet-Pakete anhand Ihrer MAC-Adresse weiter

MAC-Adressen

- Für jede Netzwerk-Karte eine MAC-Adresse
- Weltweit eindeutig
- Hardwarenahe Ebene: Netzzugangsschicht
- Ethernet
- 48 Bit oder 6 Byte groß
- Beispiel: 00:02:8A:4F:56:2A

IP-Adressen

- Für jeden Computer und jeden Switch eine IP-Adresse
- Internet-Schicht
- Zuordnung zu MAC-Adressen durch ARP
- 32 Bit oder 4 Byte groß
- Beispiel: 192.168.1.1

Hostnamen

- Für jeden Computer einen oder mehrere Hostnamen
- Anwendungsschicht
- Zuordnung zu IP-Adressen durch DNS
- Beispiel: mango, deepdance, felix
- Mit Domainnamen: teamix.de, heise.de

Netzwerke und andere Dinge

- Netzwerk-Adresse
  - Die erste IP-Adresse eines Netz-Bereiches
  - Beispiel: 192.168.1.0
- Broadcast-Adresse: Nachricht an Alle
  - Die letzte IP-Adresse eines Netzes
  - Beispiel: 192.168.1.255

Netzmaske

- Definiert, welche IP-Adressen zum lokalen Netzwerk gehören
- Spaltet IP-Adresse bitweise in Netzwerk- und Host-Adresse
- Beispiel: 11111111.11111111.11111111.0000000 oder 255.255.255.0
  - Die ersten 3 Bytes für Netze, das letzte Byte für Hosts
  - Zusammen mit Netzwerk auch: 192.168.1.0/24
  - Netze: 192.168.1.0, 192.168.2.0, 192.168.3.0 ...
  - Hosts: 192.168.1.1, 192.168.1.2, ..., 192.168.2.1, ...

Wie finden Netzwerk-Pakete ihren Weg?

- Gleiches Netz-Segment: Kein Routing erforderlich
- Andere Netz-Segmente: Routing-Tabelle mit Zielnetzen und Wegen dorthin
- Das Internet ist groß: Daher Standard-Route (0.0.0.0) für alles, worum sich jemand anders kümmert
  - Router (Standard-Gateway), z.B.: DSL-Router, Router beim Internet-Provider

Wie finden Netzwerk-Pakete ihren Weg?

Gebräuchlich im Heimbereich

- Gleiches Netz-Segment
- Alles Andere via Standard-Route

Private Netze

- Private Netze werden nicht ins Internet geroutet.
  - 10/8: 10.0.0.0 - 10.255.255.255
  - 172.16/12: 172.16.0.0 - 172.31.255.255
  - 192.168/16: 192.168.0.0 - 192.168.255.255
- Gut geeignet für Heim-Netzwerke
- Für automatische IP-Adreßvergabe, wenn DHCP-Server fehlt (link local)
  - 169.254/16: 169.254.0.0 - 169.254.255.255
- Internet-Standard RFC 1918 und RFC 3330

Treiber laden

- Treiber für die Netzwerk-Karte bei den meisten Distributionen automatisch geladen
  - Unter Debian via hotplug (Installieren mit: apt-get install hotplug)
  - Falls nicht, Treibermodul mit modprobe von Hand laden
  - Unter Debian auch menü-gesteuert via modconf

Netzwerk-Schnittstelle konfigurieren

- ifconfig eth0 <IP-Adresse> netmask <Netzmaske> up
  - Beispiel: ifconfig eth0 192.168.1.2 netmask 255.255.255.0 up
- Anzeigen mit: ifconfig eth0 oder einfach nur ifconfig für alle Netzwerk-Schnittstellen
- Mit jedem Neustart:
  - Debian: In Datei /etc/network/interfaces
  - SuSE: Mit YaST konfigurieren (Unter /etc/sysconfig/network)

Ran ans Netz

- Standard-Route zum Standard-Gateway eintragen: route add default gw <IP-Adresse des Routers>
  - Beispiel: route add default gw 192.168.1.1
- Anzeigen mit: route
- Anzeigen ohne Namensauflösung mit: route -n

Ich will Namen tippen

- DNS-Server in die Datei /etc/resolv.conf eintragen, z.B.:
  - search of.teamix.net teamix.net n-ix.net
  - nameserver 172.21.254.1
  - nameserver 172.21.254.254
- Domains in “search” werden probiert, wenn kein Domain-Name angegeben wird

Alles ganz automatisch mit DHCP

- Oder alles ganz automatisch mit DHCP: dhclient <Netzwerk-Schnittstelle>
  - Beispiel: dhclient eth0
- dhclient ohne Argument probiert alle Schnittstellen
- Alternativ auch mit: pump -i <Netzwerk-Schnittstelle

Geht alles?

- Das lokale Netz: ping <IP-Adresse des lokalen Netzes>
  - Zum Beispiel das Standard-Gateway: ping 192.168.1.1
- Das Internet: ping <Name von bekanntem Host>
  - Zum Beispiel: ping teamix.de
- Wenn die Namensauflösung nicht geht:
  - Sind die DNS-Server erreichbar?

Netzwerk-Konfiguration

- ifconfig und route
- Der Nachfolger: ip(route) (Debian-Paket: iproute)
- Halb-Automatisch via ifplugd und guessnet
- Im Kommen: Voll-Automatisch via zeroconf
- Grafische Einsteller für Desktop-Umgebungen
  - GNOME: gnome-system-tools
  - KDE unter Debian: knetworkconf
  - KDE 3.4: Zeroconf
- Grafische Einsteller der Distributionen
  - SuSE's YaST

Netzwerk-Analyse

- “Hallo Du?” mit ping <IP-Adresse>
- “Jemand da?” mit ping <Broadcast-Adresse> (Vorsicht bei großen Netz-Segmenten!)
- Wer hat welche MAC-Adresse mit arp -a
- Netzwerk-Routen verfolgen mit traceroute oder mtr
- Schnüffeln mit tethereal oder ethereal
- Datendurchsatz mit iptraf

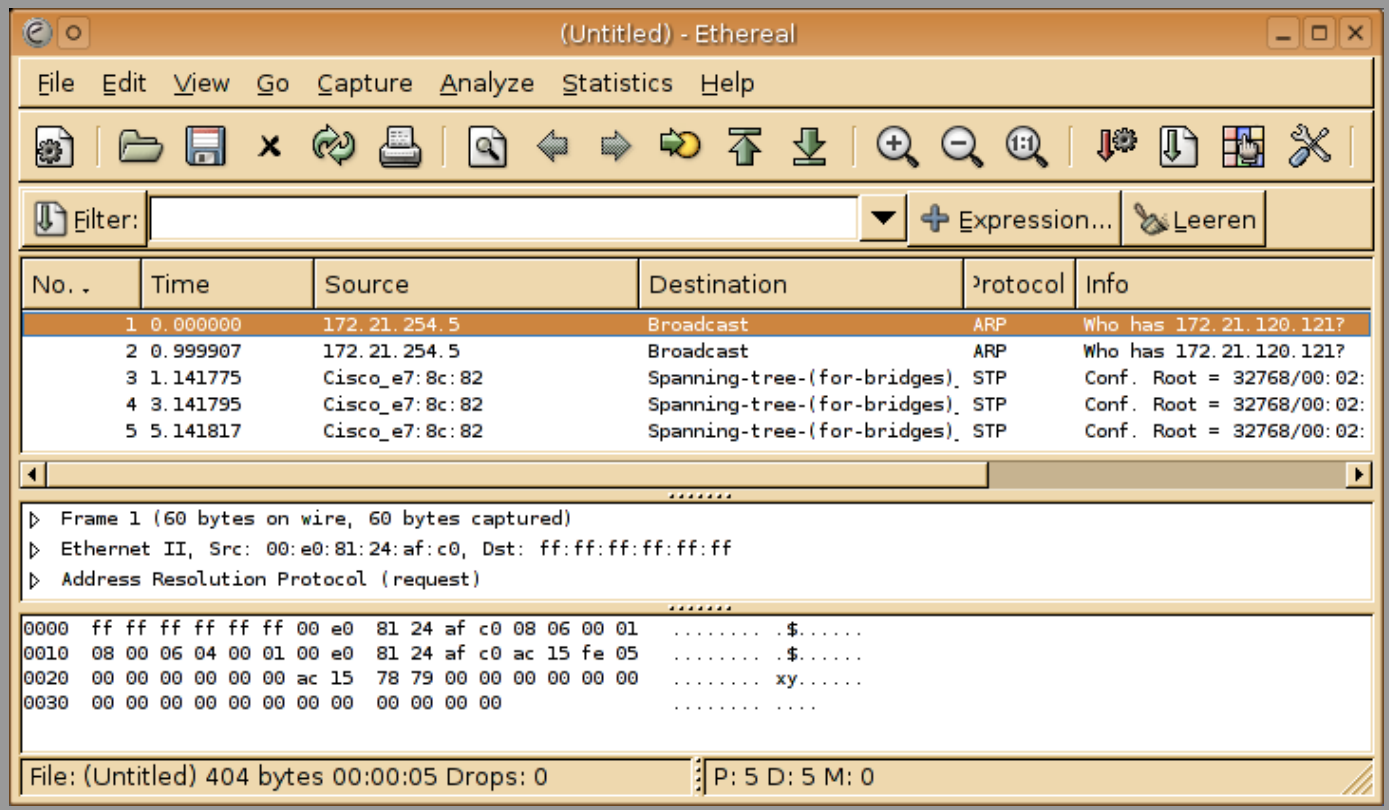
Netzwerk-Routen mit mtr

My traceroute [v0.67]

Hostname: www.heise.de | 1,00 | Pause | Restart | Quit

Hostname	Loss	Rcv	Snt	Last	Best	Avg	Worst	StDev
blackhole.of.teamix.net	0%	16	16	16	3	12	20	5,35
ge0-0-ct.nue.teamix.net	0%	16	16	12	2	11	16	4,57
nub1ip5.versatel.de	0%	16	16	20	3	12	20	4,90
fra20ip5.versatel.de	0%	16	16	21	5	13	23	4,68
de-cix.ffm.plusline.net	0%	16	16	54	6	40	216	65,62
heise1.f.de.plusline.net	0%	16	16	16	9	15	21	3,62
heise3.f.de.plusline.net	0%	16	16	17	6	13	21	4,12
www.heise.de	0%	16	16	14	6	13	21	3,94

Schnüffeln mit ethereal



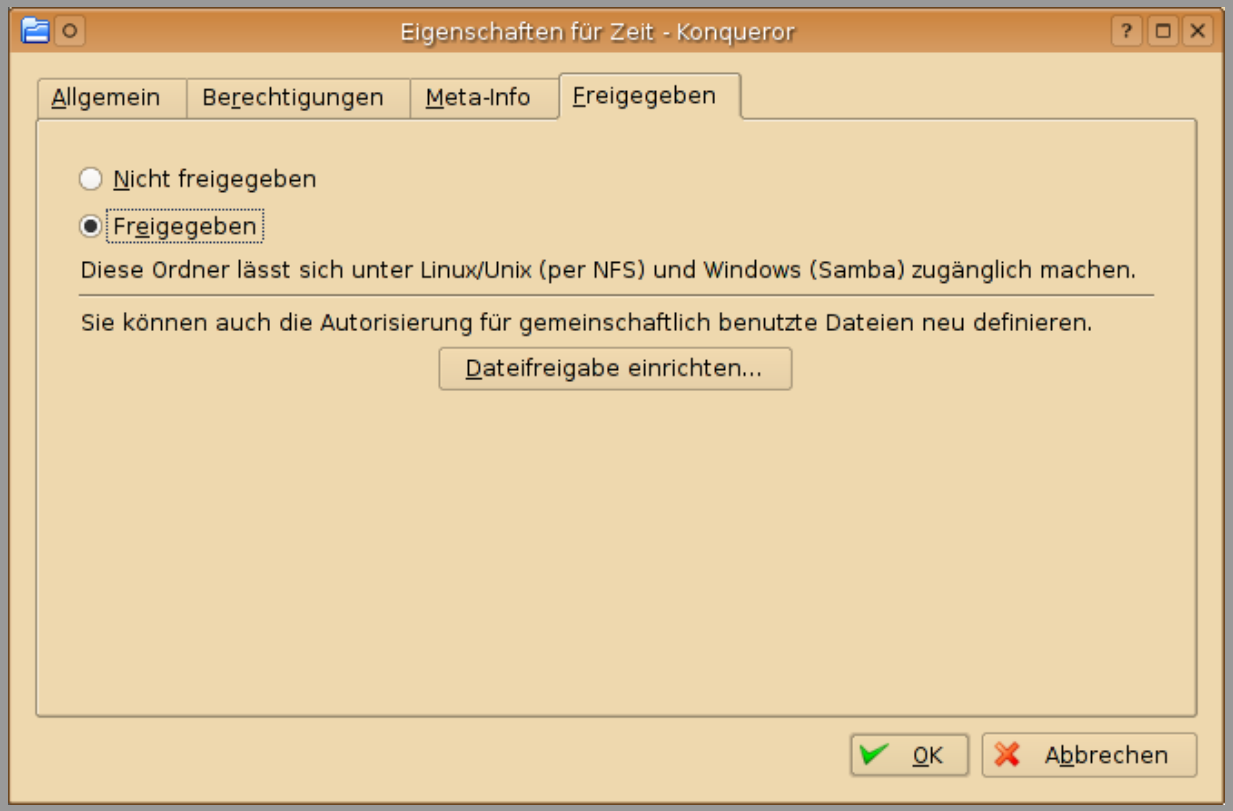
NFS - Network Filesystem

- Unter Unix-artigen Systemen weit verbreitet
- Zugangskontrolle nur über IP-Adresse
- Unverschlüsselt
- Client und Server verfügbar
- Mit KDE: Verzeichnisfreigabe möglich

Das Tor zur Windows-Welt - Samba

- Implementiert SMB-Protokoll von Windows
- Client und Server verfügbar
- Eigenes Dateisystem (smbfs oder cifs)
- Mit KDE: smb://hostname/freigabe/
- Mit GNOME
- Mit Dateisystem smbfs oder cifs

Samba- und NFS-Freigaben mit KDE

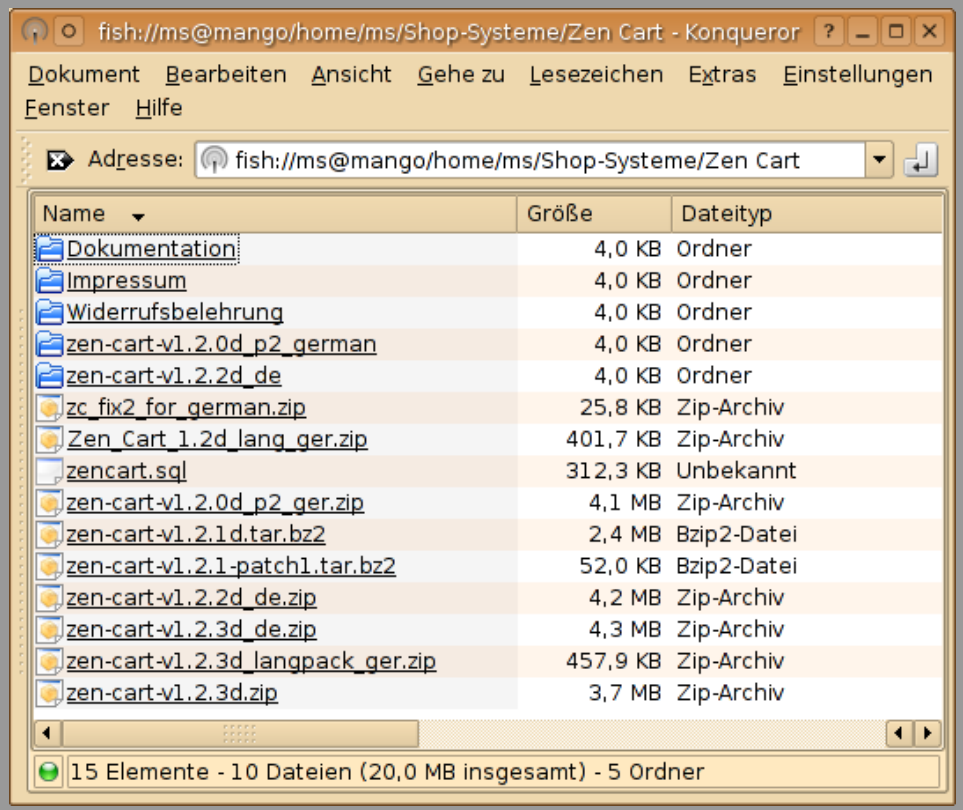


Sicher ist sicher - SSH

Mit SSH (Secure Shell)

- scp
- rsync zum Spiegeln ganzer Verzeichnisbäume
- Mit KDE: fish://benutzer@hostname/verzeichnis/
- Mit GNOME
- Mit dem Dateisystem shfs

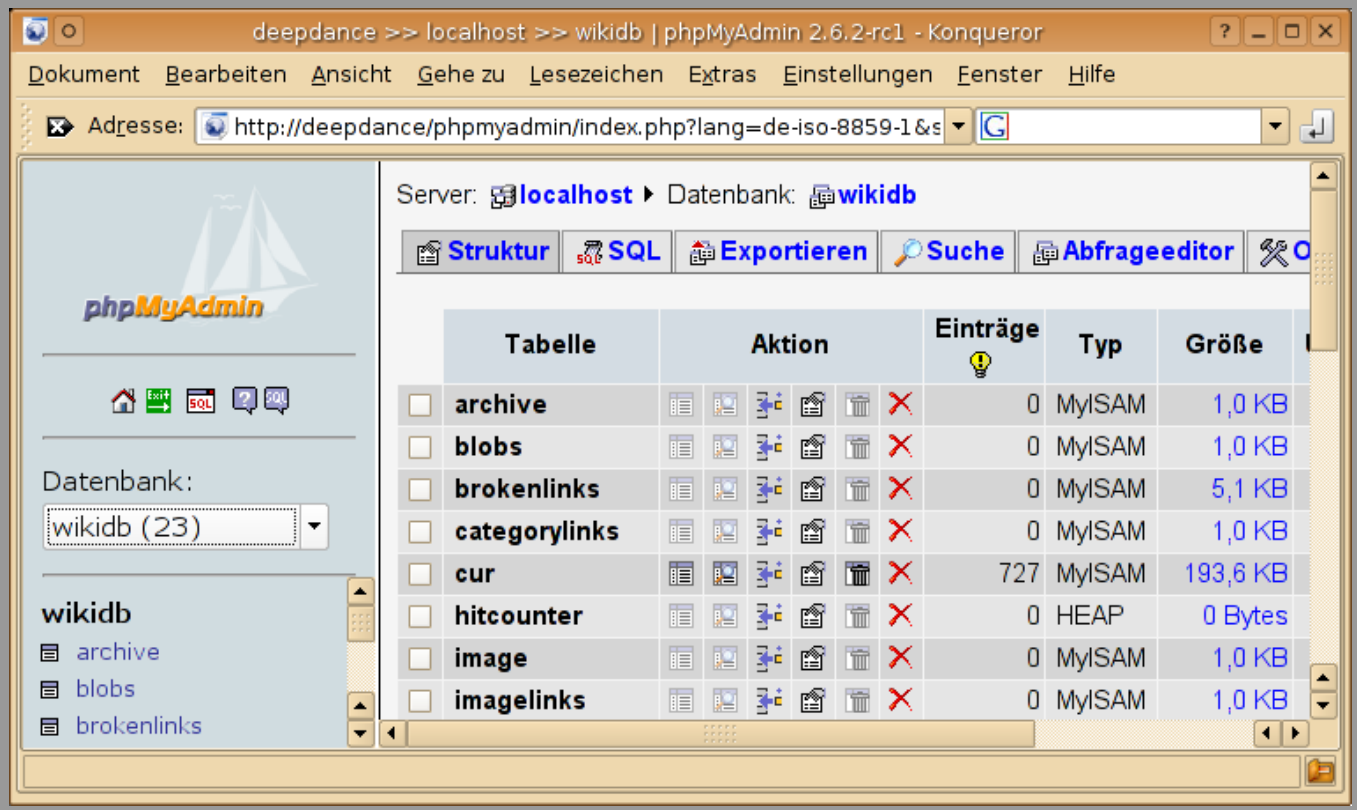
KDE und SSH


fish://ms@mango/home/ms/Shop-Systeme/Zen Cart - Konqueror
Dokument Bearbeiten Ansicht Gehe zu Lesezeichen Extras Einstellungen
Fenster Hilfe
Adresse: fish://ms@mango/home/ms/Shop-Systeme/Zen Cart
Name Größe Dateityp
Dokumentation 4,0 KB Ordner
Impressum 4,0 KB Ordner
Widerrufsbelehrung 4,0 KB Ordner
zen-cart-v1.2.0d_p2_german 4,0 KB Ordner
zen-cart-v1.2.2d_de 4,0 KB Ordner
zc_fix2_for_german.zip 25,8 KB Zip-Archiv
Zen_Cart_1.2d_lang_ger.zip 401,7 KB Zip-Archiv
zencart.sql 312,3 KB Unbekannt
zen-cart-v1.2.0d_p2_ger.zip 4,1 MB Zip-Archiv
zen-cart-v1.2.1d.tar.bz2 2,4 MB Bzip2-Datei
zen-cart-v1.2.1-patch1.tar.bz2 52,0 KB Bzip2-Datei
zen-cart-v1.2.2d_de.zip 4,2 MB Zip-Archiv
zen-cart-v1.2.3d_de.zip 4,3 MB Zip-Archiv
zen-cart-v1.2.3d_langpack_ger.zip 457,9 KB Zip-Archiv
zen-cart-v1.2.3d.zip 3,7 MB Zip-Archiv
15 Elemente - 10 Dateien (20,0 MB insgesamt) - 5 Ordner

WWW

- Client-seitig mit Mozilla Firefox, Galeon (GNOME), Konqueror (KDE), Opera
- Mit JavaScript, Java, Flash-Plugin möglich
- Server-seitig mit Apache
  - Alles inklusive: LAMP - Linux Apache MySQL PHP

LAMP - Linux, Apache, MySQL und PHP



Sicherheit

- Vorteil: Gängige Viren, Würmer, Spyware usw. laufen nicht unter Linux
- Primär: Nur die nötigen Dienste von außen zugänglich machen
  - nmap - Scannt nach offenen Ports
  - nessus - Sucht nach bekannten Sicherheitslücken
  - inetd-Superserver
  - Einzelne Serverdienste (Apache, Samba)

Sicherheit

- Sekundär: Firewall mit IP-Filter (IP-Tables)
  - Grundprinzip: Zuerst alles verbieten und dann das nötige erlauben
  - Für Desktops: Ausgehende Verbindungen JA, eingehende nur wenn nötig
  - Grafische Konfiguration via firestarter, guarddog, kmyfirewall, knetfilter, YaST ...
    - Mitunter suboptimal.
    - Kann Verständnis des Grundprinzip nicht ersetzen.

Linux als Router

- Routen für bekannte Netzwerk-Segmente hinzufügen
- Evtl. eine Standard-Route für Internet-Zugang
- Weiterleiten von IP-Paketen aktivieren
  - cat 1 >/proc/sys/net/ipv4/ip_forward
  - Permanent unter Debian “ip_forward=yes” in /etc/network/options

Mehrere Rechner ins Internet?

- Kein Problem: Doch was ist mit den IP-Adressen?
  - In der Regel nur eine IP-Adresse pro Internet-Zugang
  - Aber mehrere IP-Adressen im lokalen Netz
  - Lokale IP-Adressen nicht ins Internet geroutet
- Lösung: NAT - Network Address Translation
  - Umschreiben der IP-Adressen auf dem Router
  - Router merkt sich umgeschriebene IP-Adressen umgeschrieben hat
  - Antwort-Paket aus dem Netz wieder an entsprechenden internen Computer
  - Einschalten mit: iptables -t nat -A POSTROUTING -o <Internet-Schnittstelle> -j MASQUERADE

Auf entfernten Systemen arbeiten

- Mit SSH: ssh <benutzername>@<hostname>
  - Auch mit X11: ssh -X <benutzername>@<hostname>
- Plattform-übergreifend mit VNC
  - Server und Client
  - Mit xvncviewer
  - Mit KDE's Desktop-Freigabe: vnc://<benutzername>@<host>
  - Mit GNOME's integrierten VNC-Server vino
  - Windows-Client unter http://www.realvnc.com
- Effizient mit FreeNX

Was geht sonst noch so?

Viel ;-). Eine kleine Auswahl:

- E-Mail: Reichhaltige Auswahl an Clients und Servern
- Chatten: IRC, SILC, Instant Messenger Protokoll, Talk
- VPN (Virtual Private Network): Mit OpenVPN oder IPSec Netzwerke tunneln
- Drucken: Via CUPS (Common Unix Printing System) und IPP (Internet Printing Protocol)
- Routing-Protokolle: Internet-Routing

Ich will noch mehr wissen

- Wikipedia: http://de.wikipedia.org
- IETF (Internet Engineering Taskforce): http://www.ietf.org