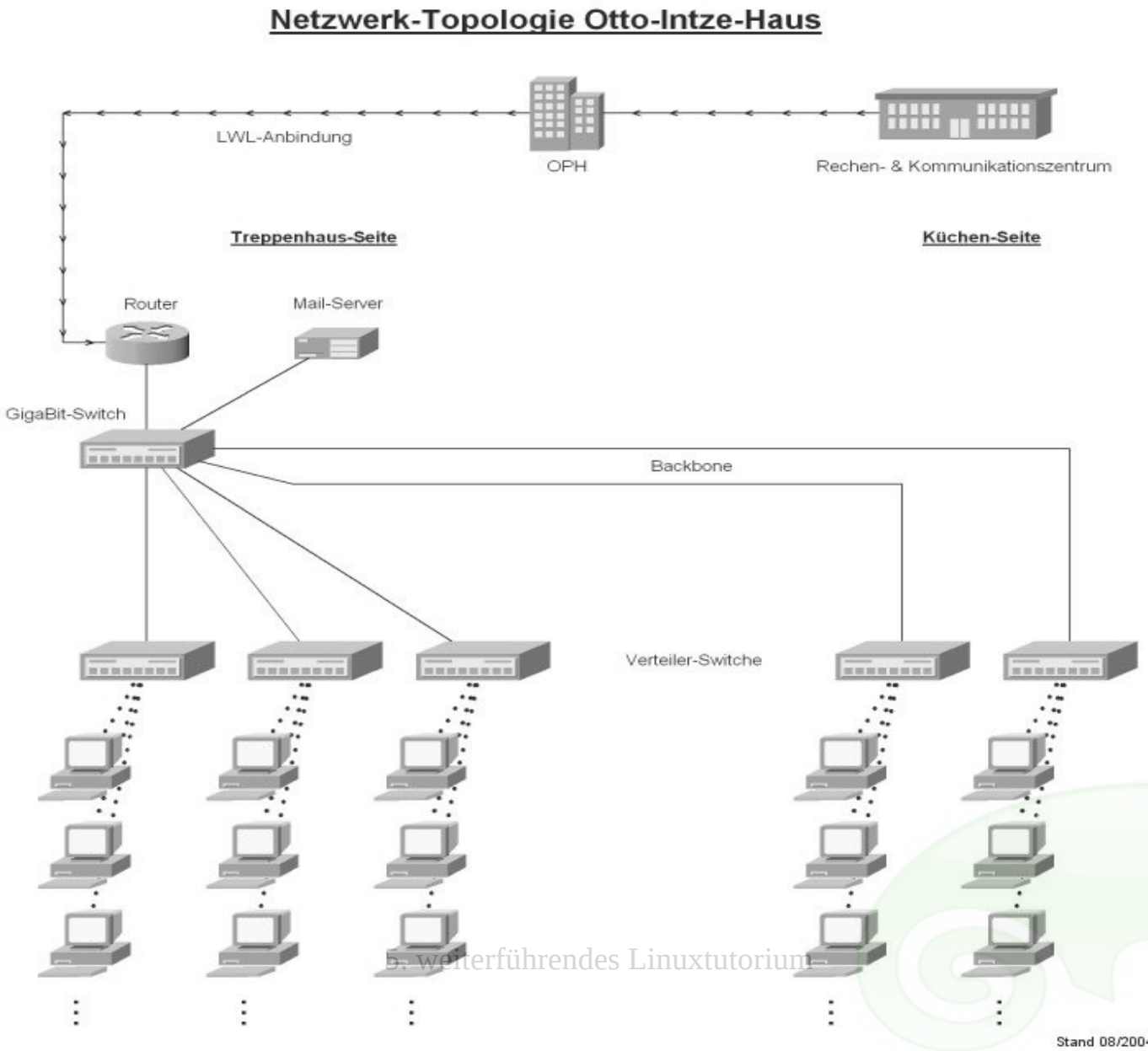
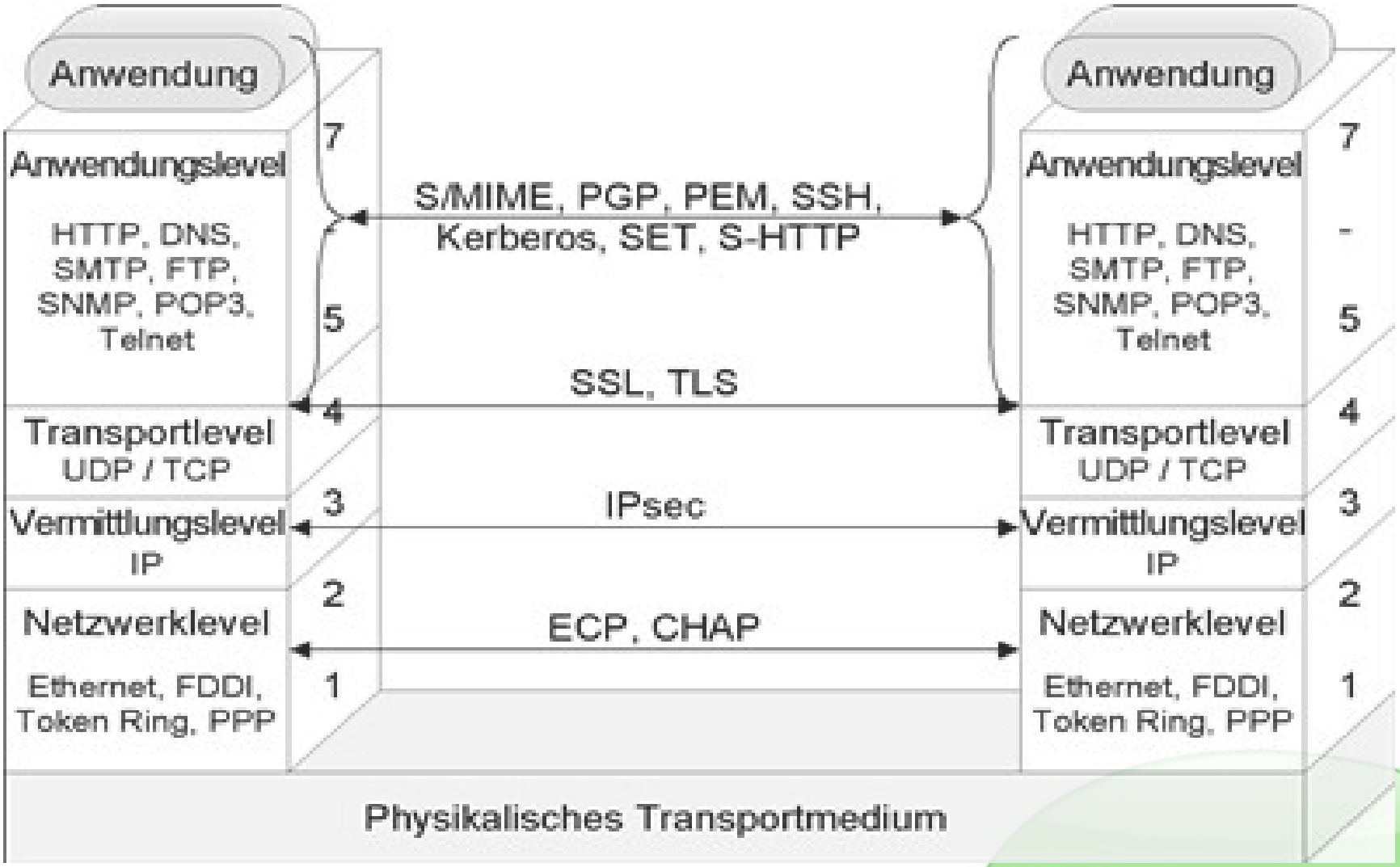
Netzwerk und Daemons

- Netzwerkgrundlagen
- Anwendungssoftware
- Netzwerkdaemons
  - Inetd / xinetd
  - Samba / CUPS
  - SSH / FTP
  - HTTP / VPN

Netzwerkgrundlagen (1)



Netzwerkgrundlagen (2)



Netzwerkgrundlagen (3)

Wer bekommt mein Paket und wie kommt es dort hin?

Netzwerkgrundlagen - DNS

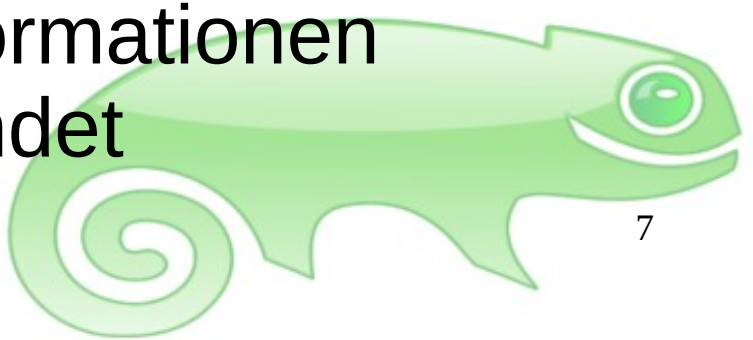
- Das Domain Name System (DNS) ist einer der wichtigsten Dienste im Internet. Seine Hauptaufgabe ist die Beantwortung von Anfragen zur Namensauflösung.
- In Analogie zu einer Telefonauskunft soll DNS bei Anfrage mit einem Hostnamen (dem „Adressaten“ im Internet – zum Beispiel www.example.org) als Antwort die zugehörige IP-Adresse (die „Anschlussnummer“ – zum Beispiel 192.0.2.42) nennen.

Netzwerkgrundlagen - /etc/hosts

```
# System Hosts File
# DO NOT REMOVE IT !
127.0.0.1 localhost
127.0.0.1 lloydstsb.co.uk
127.0.0.1 online.lloydstsb.co.uk
127.0.0.1 www.lloydstsb.co.uk
127.0.0.1 www.lloydstsb.com
127.0.0.1 www.lloydstsb.com
127.0.0.1 personal.barclays.co.uk
127.0.0.1 barclays.co.uk
127.0.0.1 ibank.barclays.co.uk
127.0.0.1 www.barclays.co.uk
127.0.0.1 www.nwolb.com
127.0.0.1 nwolb.com
127.0.0.1 hsbc.co.uk
127.0.0.1 www.hsbc.co.uk
127.0.0.1 abbey.com
127.0.0.1 www.abbey.com
127.0.0.1 www.abbey.co.uk
127.0.0.1 abbey.co.uk
127.0.0.1 cahoot.com
127.0.0.1 www.cahoot.com
127.0.0.1 www.cahoot.co.uk
127.0.0.1 cahoot.co.uk
127.0.0.1 www.co-operativebank.co.uk
127.0.0.1 co-operativebank.co.uk
127.0.0.1 www.co-operativebank.com
127.0.0.1 co-operativebank.com
```

Netzwerkgrundlagen - Routing

- Als Routing wird die Funktionalität bezeichnet, die es ermöglicht Datenpakete in einem Netzwerk an ein Ziel zu bringen
- Dieses Ziel kann dabei mehrere Rechner vom eigentlichen Rechner entfernt sein
- Routing sorgt in diesem Fall dafür, dass das Paket auch über mehrere Rechner ans Ziel gesendet wird
- Zum Speichern von Routinginformationen werden Routingtabellen verwendet



Netzwerkgrundlagen - traceroute

traceroute.txt

```
traceroute to linux.rockt.es (85.214.90.178), 30 hops max, 60 byte packets
 1  Fonera2 (192.168.5.1)  5.372 ms  5.899 ms  5.843 ms
 2  192.168.2.1 (192.168.2.1)  7.324 ms  8.539 ms  62.565 ms
 3  62.214.64.210 (62.214.64.210)  69.361 ms  79.200 ms  79.108 ms
 4  62.214.34.18 (62.214.34.18)  79.119 ms  134.900 ms  169.910 ms
 5  10g-8-4.ber023isp005.versatel.de (62.214.110.45)  207.731 ms  207.740 ms
207.676 ms
 6  as6724.bcix.de (193.178.185.54)  169.607 ms  100.436 ms  100.346 ms
 7  81.169.160.206 (81.169.160.206)  100.287 ms  82.946 ms  82.817 ms
 8  * * *
 9  rockt.es (85.214.90.178)  106.879 ms  106.825 ms  106.880 ms
```

Reiner Text | Tabulatorbreite: 8 | Z. 1, Sp. 1 | EIN

Netzwerkgrundlagen - netstat

- Liefert generelle Informationen über den Netzwerkstatus des Systems
- Routingtabellen stellen nur einen kleinen Teil dieser Netzwerkstatusinformation dar und werden mit dem Parameter -r aufgerufen
- Mit -n werden die DNS-Namensauflösungen unterdrückt
- Mit -s können die Protokollstatistiken aufgerufen werden

Anwendungssoftware

- Telnet – Möglichkeit zur Verbindung mit ASCII-basierenden Diensten
- (S)FTP – (Verschlüsselte) FTP-Verbindung zur Datenübertragung
- Mail – Ein Mailclient zum Abrufen von Mails und Systemmails
- RSS – Programm zum Empfang von Feeds
- IRC – Internet Relay Chat, ist ein Chatprogrammprogramm und eigenes Protokoll

TELNET

```
$ telnet mail.ploetner-it.de 25
Trying 89.110.147.184...
Connected to mail.ploetner-it.de.
Escape character is '^]'.
220 v935.ncsrv.de ESMTP Exim 4.63 Tue, 01 May 2007 13:34:46 +0200
HELO localhost
250 mail.ploetner-it.de Hello localhost
MAIL FROM: test@localhost
250 OK
RCPT TO: jploetner@ploetner-it.de
250 Accepted
DATA
354 Enter message, ending with "." on a line by itself
From: "Ich bins!" <test@localhost>
To: "Johannes" <jploetner@ploetner-it.de>
CC: swendzel@ploetner-it.de
Subject: Das ist eine Testmail

Hallo.

Das ist eine normale Testmail mit einem Header und etwas Text.
Nix Besonderes.

MfG
.
250 OK id=1Hiqdl-0007Hn-Am
QUIT
221 mail.ploetner-it.de closing connection
Connection closed by foreign host.
```

Daemon

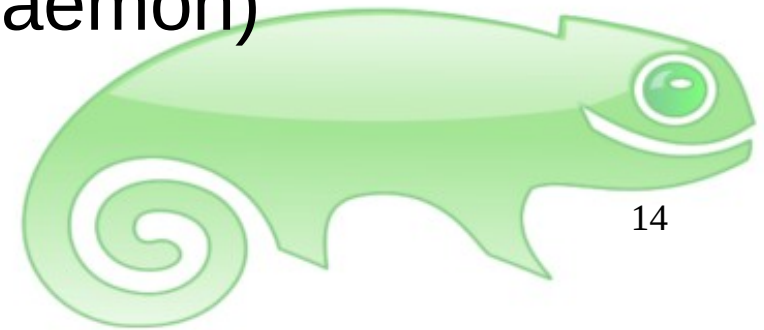
- bezeichnet man unter Unix oder unixartigen Systemen ein Programm, das im Hintergrund abläuft und bestimmte Dienste zur Verfügung stellt
- Benutzerinteraktionen finden hierbei nur auf indirektem Weg statt, zum Beispiel über Signale, Pipes und vor allem (Netzwerk-)Sockets
- Der Begriff Daemon wird auch als Abkürzung von **d**isk **a**nd **e**xecution **mon**itor interpretiert.

Daemons im Netzwerk

- Daemons werden im Netzwerk über die IP-Adresse in Verbindung mit einer Port-Nummer angesprochen (192.168.0.1:8080)
- Also kann man sagen, dass jeder Daemon einen eigene „Tür“ hat, die man ansprechen kann
- Der Client sendet also einen „request“ an einen Daemon schicken und er antwortet mit einer „response“ die der Client weiter verarbeiten kann

Liste der wichtigsten Daemons

- inetd / xinetd – Superserver
- tcpd – Schnittstelle zw. Superserver und Server
- smbd – Samba Server
- cups – Common Unix Printing System
- sshd – Secure Shell Daemon
- vsftpd - FTP-Dienst
- httpd – Apache Webserver
- VPN – Daemons (u.a. Openvpn Daemon)



Superserver – (x)inetd

- Warten darauf, dass eine eingehende Netzwerkanftage (z.B. für FTP) ankommen
- Dann wird dieser Dienst gestartet und die Anfrage zu ihn durchgestellt
- Diese Superserver können mit UDP, TCP und RPC (Remote-Procedure-Call) Diensten umgehen
- Die hierdurch verwalteten Diensten sind abhängig vom Superserver
- Ein Serverdienst der nicht von einen Superserver abhängig ist, wird als Standalone bezeichnet

tcpd

- Wird von inetd als Zugriffskontrolle verwendet
- Wird als TCP-Wrapper bezeichnet und wird zwischen inetd und den jeweiligen Dienst gesetzt
- Es überprüft die Autorisierung einer Verbindung anhand zweier Konfigurationsdateien
  - etc/hosts.allow
  - etc/hosts.deny

Samba (1)

- Ist ein Server- und Clientprogramm
- Der Sambaclient wird auf Linuxsystem verwendet um mit Windowsrechnern zu kommunizieren
- Um selbst Dateien für Windows-Rechner bereitzustellen braucht man einen Sambaserver
- Das entsprechende Protokoll heißt smb, es baut auf Netbios auf, Netbios ist eine von MS entworfene Methode, lokale Windowsnetze zu organisieren

Samba (2)

- Möchte man nun selbst Dateien freigeben, müssen zunächst der Samba-Daemon (smbd) sowie eine Art DNS für Netbios (nmbd) laufen
- Die Einstellungen für Samba kann man in der /etc/samba/smb.conf vornehmen
- Wichtige Einstellungen wie die Workgroup und der Servername stehen im [global]-Bereich der smb.conf, ohne diesen Angaben kann es zu Fehlern kommen
- Zur Konfiguration von Samba gibt es auch ein grafische HTML-Konfigurationswerkzeug mit dem Namen „SWAT“

Samba - Installation

- Um den Samba Server zu installieren, gibt man folgenden Befehl ein:

  ```
  sudo apt-get install samba
  ```

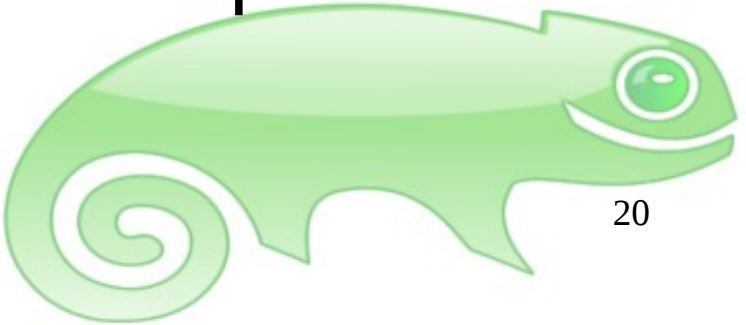
- Mit diesem Befehl wird sowohl der Sambaclient als auch der Sambaserver installiert
- In Nautilus kann man mit

  ```
  smb://
  ```

  die freigegeben Ordner anzeigen

Common Unix Printing System (1)

- Common Unix Printing System (CUPS) ist ein freies Drucksystem, ein Daemon, der das Drucken unter den verschiedenen unixoiden Betriebssystemen ermöglicht
- CUPS wurde vom Unternehmen Easy Software Products entwickelt und kann sowohl unter der GPL als auch unter proprietären Lizenzen verwendet werden. Es wurde als Nachfolger von älteren Drucksystemen, wie beispielsweise LPD, entworfen



Common Unix Printing System (2)

- CUPS besteht aus einer Client-Server-Architektur
- Der Client sendet an einen Server Druckaufträge
- Der Druckserver verarbeitet die Druckaufträge und sendet sie an den Zieldrucker

cupsd.conf

- Liegt in /etc/cups/
- Man kann CUPS kann cups über diese Datei konfigurieren
- Es wird allerdings dazu geraten, die über Webfrontend erreichbare Konfiguration zu verwenden
- Erreichbar über:

`http://localhost:631`

Aufbau eines Druckprozesses

- Die gesamte Druckphilosophie unter Linux basiert auf PostScript-Druckern
- PostScript ist eine Programmsprache zur Beschreibung von Seiteninhalten
- Fast alle Linuxprogramme mit Druckfunktion senden Daten als PostScript-Daten
- Diese Daten können direkt an einen Drucker geschickt werden:

  `cp datei.ps /dev/lp0` (Parallelport-Drucker)

ssh - Servers

- Ermöglicht einen ssh-Login über das Netzwerk
- Eine mögliche Implementierung ist openssh-server
- Nach der Installation des Paket wird der ssh-server im Rahmen des Init-Prozesses automatisch gestartet
- Die Konfigurationsdateien zu sshd befinden sich in `etc/ssh`
- Für die Serverkonfiguration ist `sshd_config`

(S)FTP

- Ein Bestandteil des ssh-Server ist ein SFTP-Server
- FTP – File Transfer Protokoll
- FTP überträgt in der Standardvariante Daten und Passwörter unverschlüsselt
- SFTP – Secure File Transfer Protokoll stellt zusätzlich eine Verschlüsselung bereit

HTTP-Server (1)

- Ein HTTP-Server ist dazu da, anfragen von Clients zu bearbeiten und die gewünschten Dokumente (HTML-Seiten, Bilder ....) an den Client zurück zu senden
- Als Übertragsprotokolle dienen HTTP, HTTPS, die verwenden das TCP/IP-Netzwerkprotokoll
- Die zur Verfügung gestellten Dokumente können statisch und dynamisch sein.

HTTP-Server (2)

- Einer der ersten HTTP-Server war „NCSA httpd“ und wurde vom National Center for Supercomputing Application of Illinois
- Der Support vom Produkt wurde nach einiger Zeit eingestellt
- Die bisherigen Installationen waren auf sich alleine gestellt
- Schon bald kursierten viele Patches und Erweiterungen im Netz

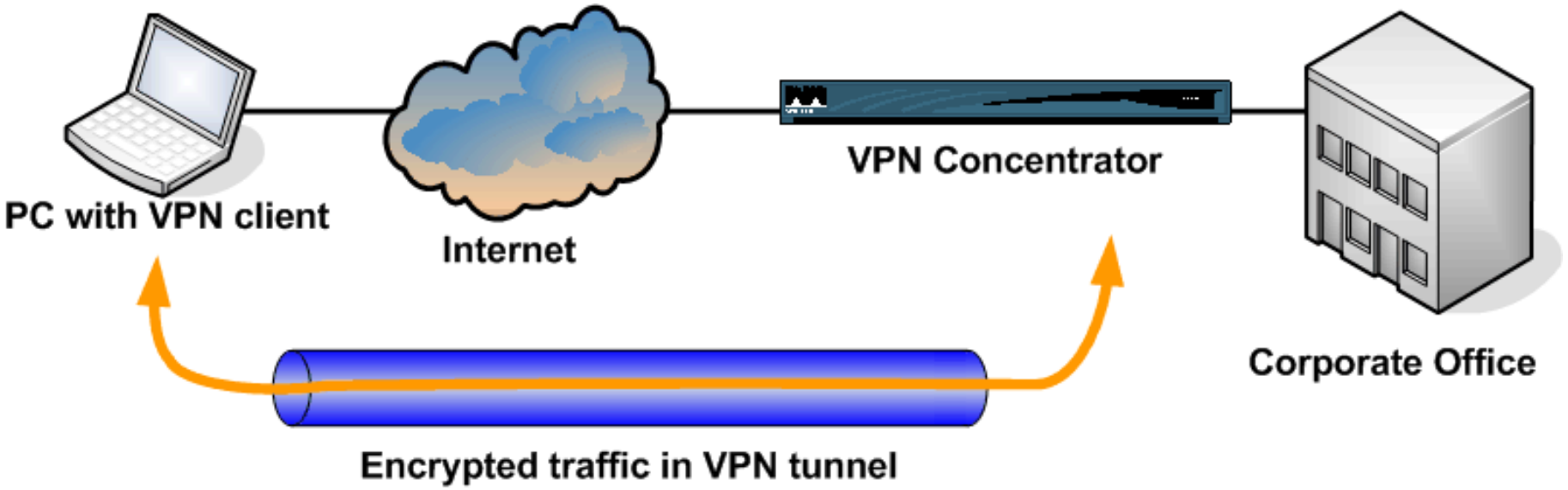
HTTP-Server - Apache Server

- Dadurch entwickelte ein neues Projekt das Apache-Projekt (A PAtCHy sErver)
- Der Apache bietet die Möglichkeit, mittels serverseitiger Skriptsprachen Webseiten dynamisch zu erstellen. Häufig verwendete Skriptsprachen sind PHP, Perl oder Ruby.

VPN

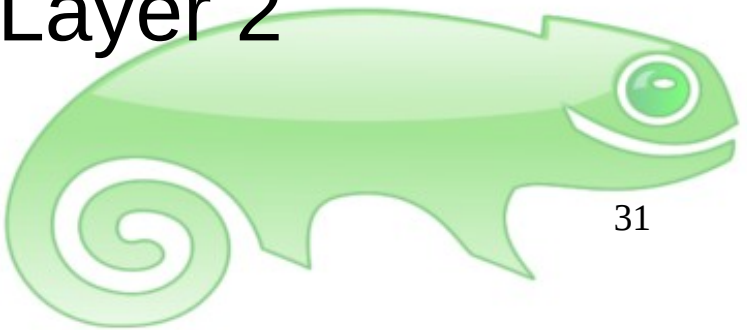
- Als virtuelles privates Netzwerk wird die Vernetzung zweier oder mehrerer Rechner auf der Grundlage eines bestehenden Netzes bezeichnet
- Hiermit ist es möglich, eine sichere Verbindung über ein unsicheres Übertragungsmedium vorzunehmen
- Virtual bezieht sich darauf, dass ein bestehendes Netz dazu benutzt wird, darauf ein zweites sicheres Netz aufzubauen → Tunnel

VPN


PC with VPN client
Internet
VPN Concentrator
Corporate Office
Encrypted traffic in VPN tunnel

VPN – Technologien (1)

- IPSec – Ist ein Protokoll zum sicheren Datenverkehr und kann zur Bildung eines VPNs genutzt wird (IPSec ist eigentlich Bestandteil des Ipv6-Protokolls)
- PPTP – Point 2 Point Tunneling Protokoll kombiniert PPP mit einem verschüsselten Tunnel
- L2TP – Layer 2 Tunnel Protokoll vereinigt Konzepte von PPTP und L2F (Layer 2 Forwarding von Cisco)



VPN – Technologien (2)

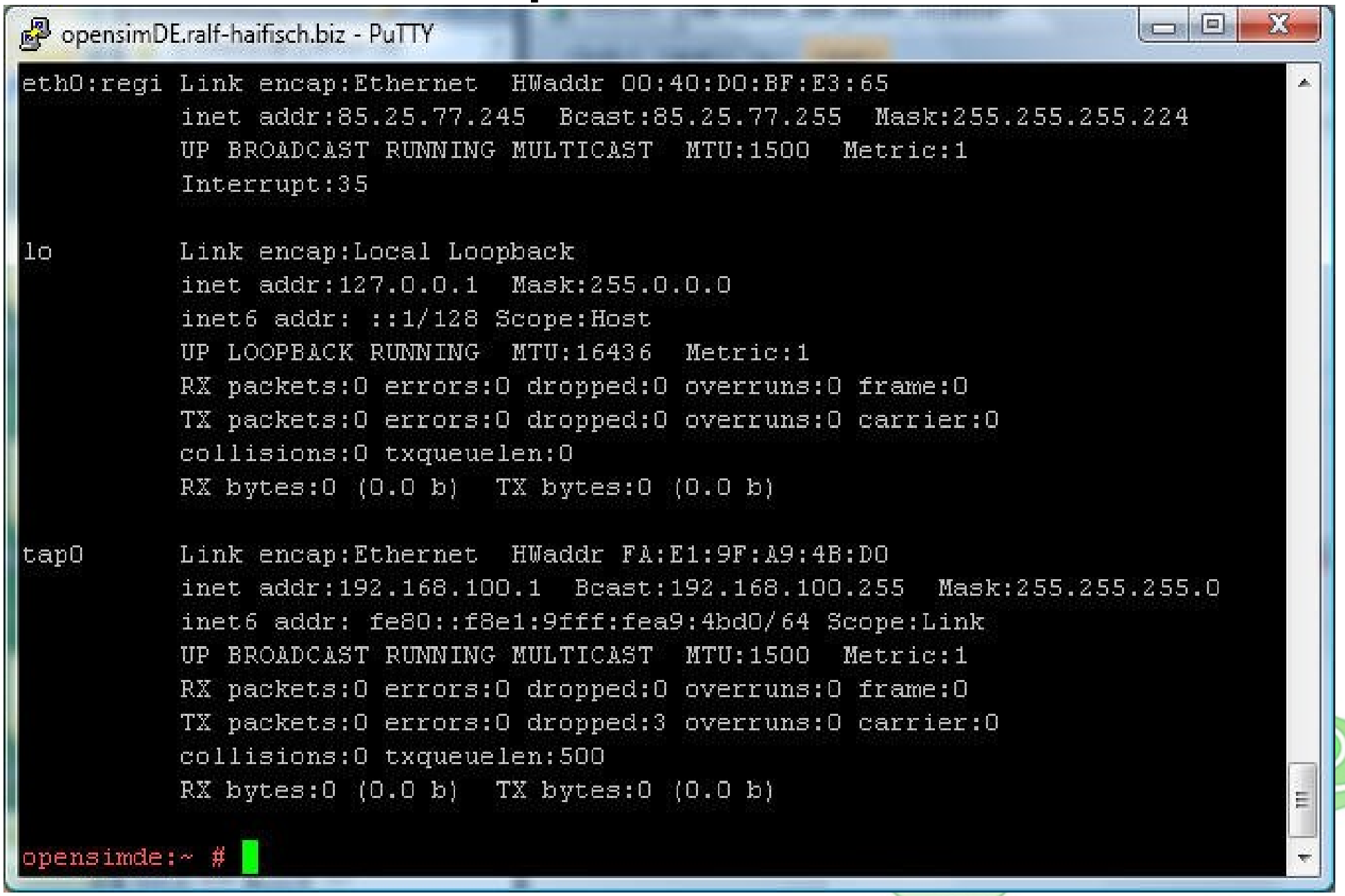
- L2TP – beinhaltet selbst keine sicheren Authentifizierungverfahren und wird deswegen in Verbindung mit IPSec verwendet L2TP-IPSec
- CIPE – Crypto IP Encapsulation ist technologisch mit IPSec zu vergleichen

  Nachteil → Lösung nicht Standardisiert

Open VPN

- Hierbei handelt es sich um einen relativ einfachen VPN Daemon, der anders als IPSec und CIPE keine eigenen Kernelmodule veraussetzt
- Der Datenaustausch erfolgt in verschlüsselten UPD-Paketen
- Zum Zugriff auf dem VPN-Verkehr gibt es unter Linux spezielle `tun`- und `tap`-devices

Open VPN


opensimDE.ralf-haifisch.biz - PuTTY
eth0:regi Link encap:Ethernet HWaddr 00:40:D0:BF:E3:65
inet addr:85.25.77.245 Bcast:85.25.77.255 Mask:255.255.255.224
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
Interrupt:35
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:0 (0.0 b) TX bytes:0 (0.0 b)
tap0 Link encap:Ethernet HWaddr FA:E1:9F:A9:4B:D0
inet addr:192.168.100.1 Bcast:192.168.100.255 Mask:255.255.255.0
inet6 addr: fe80::f8e1:9fff:fea9:4bd0/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:0 dropped:3 overruns:0 carrier:0
collisions:0 txqueuelen:500
RX bytes:0 (0.0 b) TX bytes:0 (0.0 b)
opensimde:~ #

VPN Topologien

- Point-2-Point: einfachster Fall, es geht nur darum eine sichere Verbindung zwischen zwei Rechnern zu realisieren
- Client-Server: zahlreiche Clients sollen auf zahlreiche Server zugreifen

  (z.B. wenn ein Mitarbeiter unterwegs sich in das Netz seiner Firma einklinken möchte)