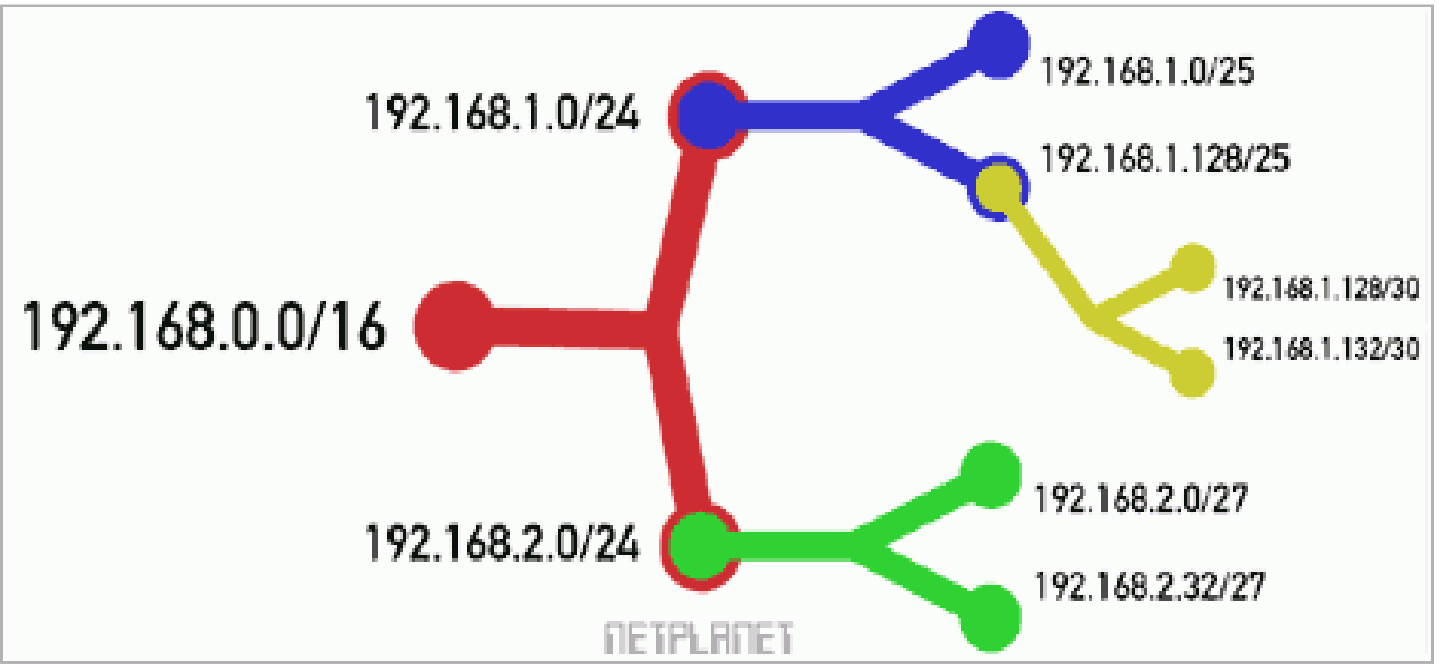
VLSM
Variable Length Subnet Masks
(variabel lange Subnetzmasken)



Problem des herkömmlichen Subnetting : innerhalb eines Netzes kann nur eine Subnetzmaske verwendet werden.

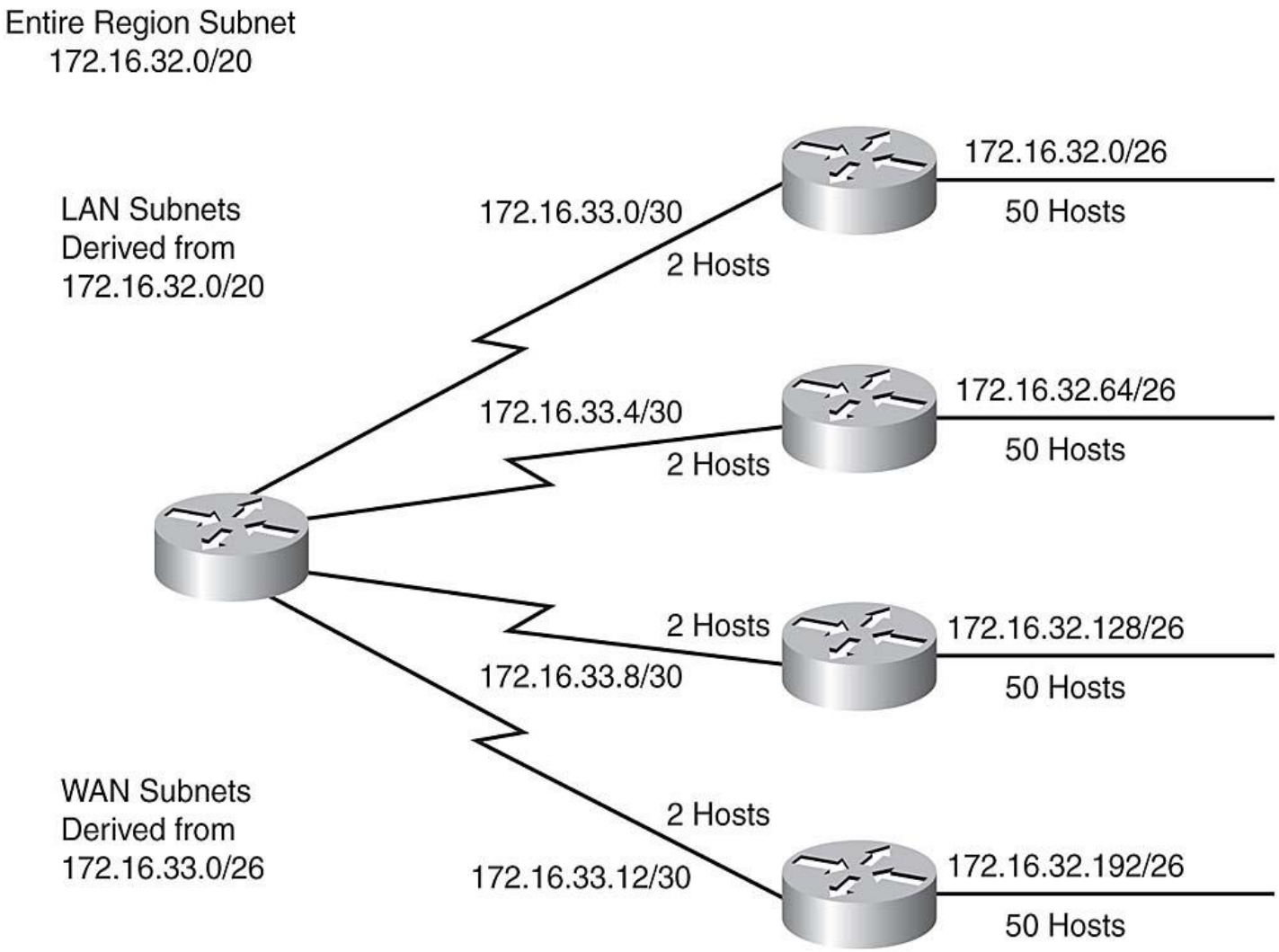
Lösung : VLSM ermöglicht die individuelle Aufteilung von zugeteilten Netzen.

VLSM erleichtert und verbessert die Nutzung des zugeteilten Adressbereichs innerhalb eines Unternehmens.

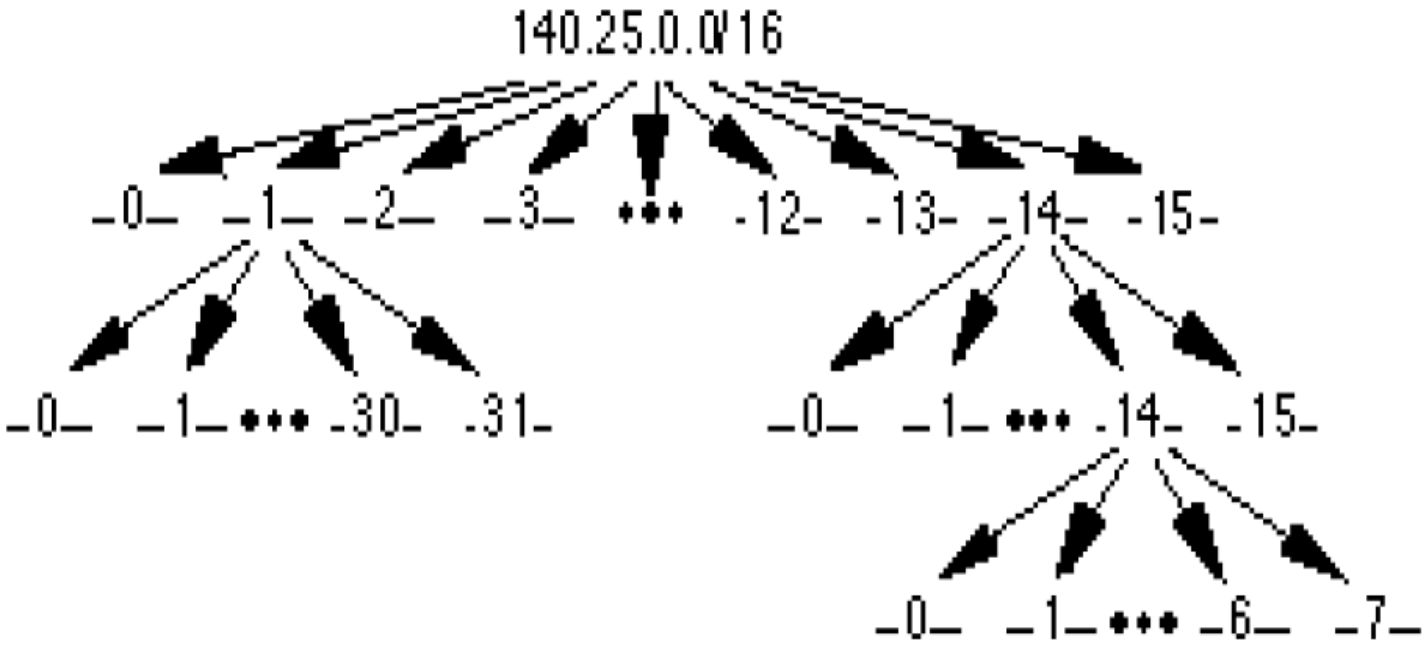
Zusammenfassen von Routen
(-> Route Aggregation)
VLSM erlaubt auch die rekursive Aufteilung des Adressraumes einer Organisation, so dass er wieder zusammengefasst werden kann, damit die Menge an Routinginformation auf der obersten Ebene reduziert werden kann.

Moderne Routing-Protokolle wie **OSPF** und **RIP-v2** erlauben den Einsatz von VLSM.

Beispiel für VLSM :

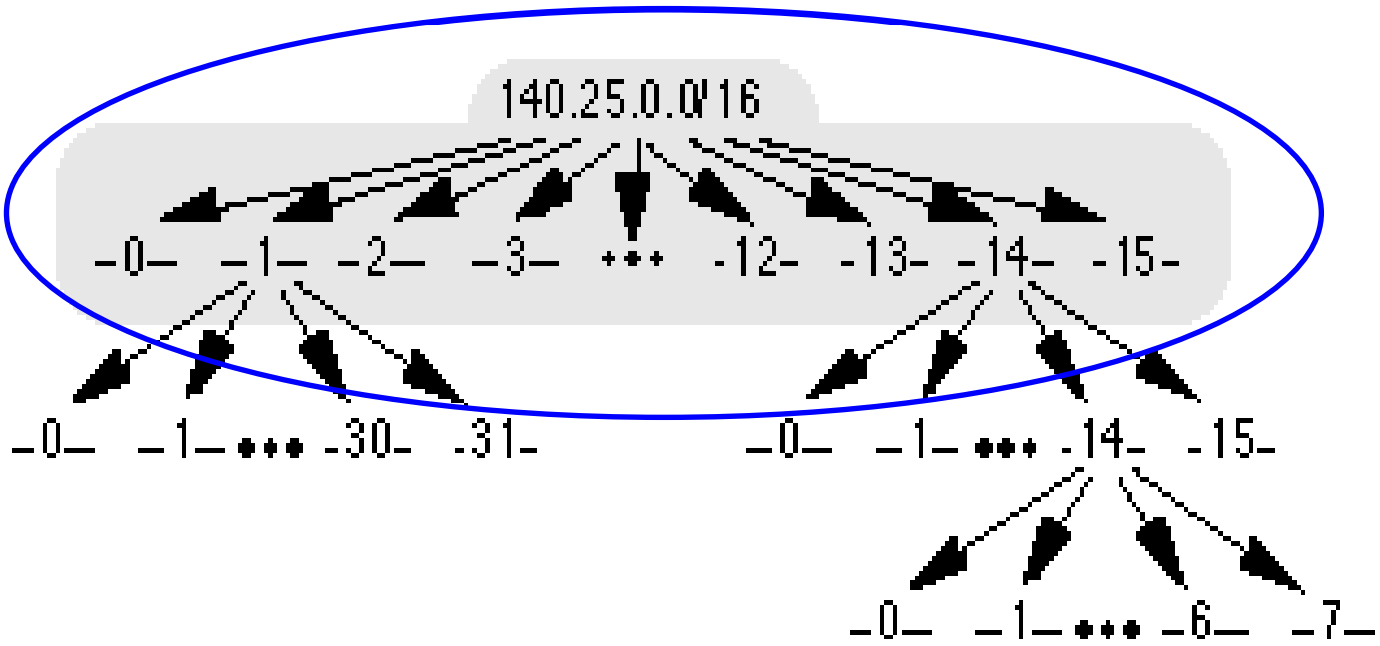


VLSM-Beispiel : Einer Organisation wurde die Netzwerkadresse 140.25.0.0/16 zugewiesen und sie plant die Verwendung von VLSM.



1. die Netzwerkadresse wird in 16 gleich große Adressblöcke aufgeteilt.
2. das Subnetz Nummer 1 wird dann in 32 gleich große Blöcke aufgeteilt.
3. das Subnetz Nummer 14 in 16 gleich große Blöcke aufgeteilt wird.
4. das Subnetz Nummer 14->14 in acht gleich große Blöcke zerlegt.

1. Schritt :
die Basisnetzwerkadresse
140.25.0.0/16 wird in 16 gleich große Adressblöcke geteilt.



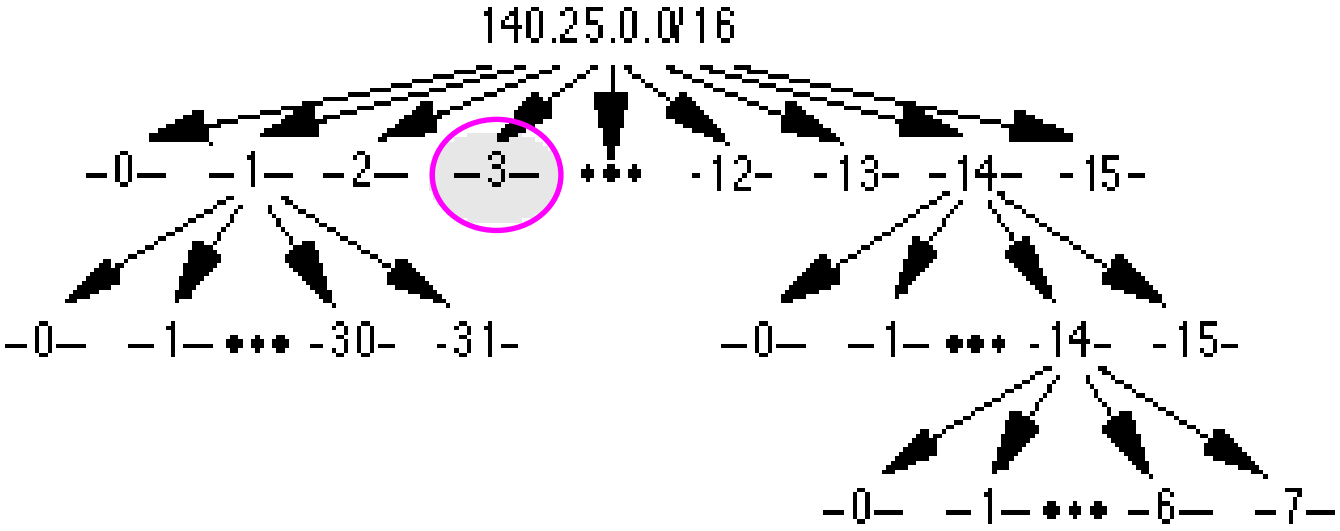
Die Subnetmask muss um vier Bits erweitert werden,
-> neuer Netzwerkpräfix /20 (-> 255.255.240.0).
Jedes dieser Subnetze hat einen fortlaufenden Block von 2^{12} (= 4096) Netzwerkadressen.

Die 16 Subnetze des Netzes 140.25.0.0/16

Basisnetzwerk:10001100.00011001.00000000.00000000 = **140.25.0.0/16**

Subnetz #0: 10001100.00011001.00000000.00000000 = **140.25.0.0/20**
Subnetz #1: 10001100.00011001.00010000.00000000 = **140.25.16.0/20**
Subnetz #2: 10001100.00011001.00100000.00000000 = **140.25.32.0/20**
Subnetz #3: 10001100.00011001.00110000.00000000 = **140.25.48.0/20**
Subnetz #4: 10001100.00011001.01000000.00000000 = **140.25.64.0/20**
:
Subnetz #13: 10001100.00011001.11010000.00000000 = **140.25.208.0/20**
Subnetz #14: 10001100.00011001.11100000.00000000 = **140.25.224.0/20**
Subnetz #15: 10001100.00011001.11110000.00000000 = **140.25.240.0/20**

Definieren der Hostadressen für das Subnetz Nummer 3 (140.25.48.0/20) :

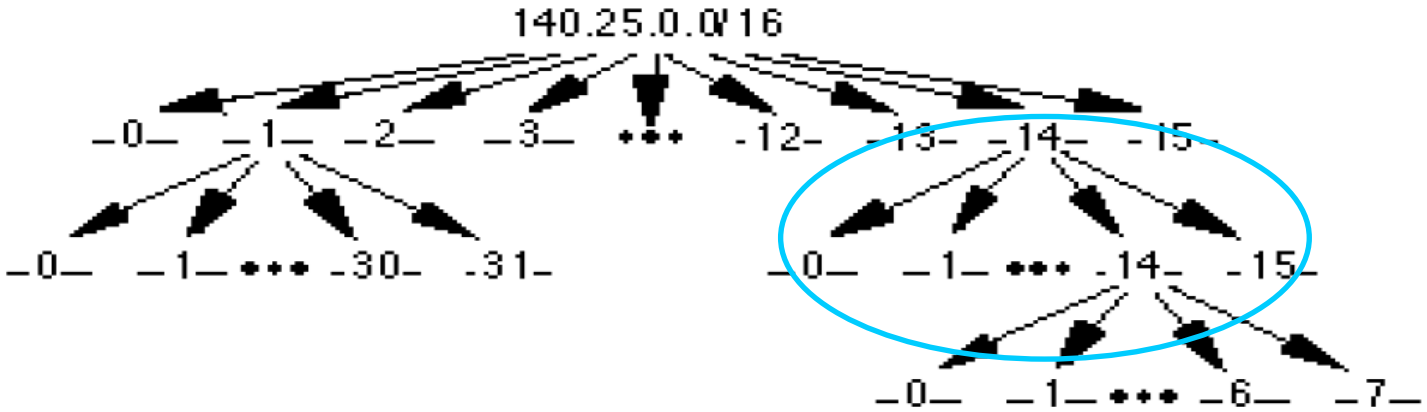


12 Bit -> 4094 (=2^{12} - 2) Hostadressen

Subnetz #3: 10001100.00011001.00110000.00000000 = **140.25.48.0/20**
Rechner #1: 10001100.00011001.00110000.00000001 = 140.25.48.1/20
Rechner #2: 10001100.00011001.00110000.00000010 = 140.25.48.2/20
:
Rechner #4093: 10001100.00011001.00111111.11111101 = 140.25.63.253/20
Rechner #4094: 10001100.00011001.00111111.11111110 = 140.25.63.254/20

Broadcast-Adresse des Subnetzes #3 -> alle Bits der Hostadresse auf eins gesetzt:
10001100.00011001.00111111.11111111 = **140.25.63.255**

Nachdem das Basisnetzwerk in 16 Subnetze unterteilt wurde, wird das Subnetz #14 (140.25.224.0/20) wiederum in 16 Subnetze unterteilt.

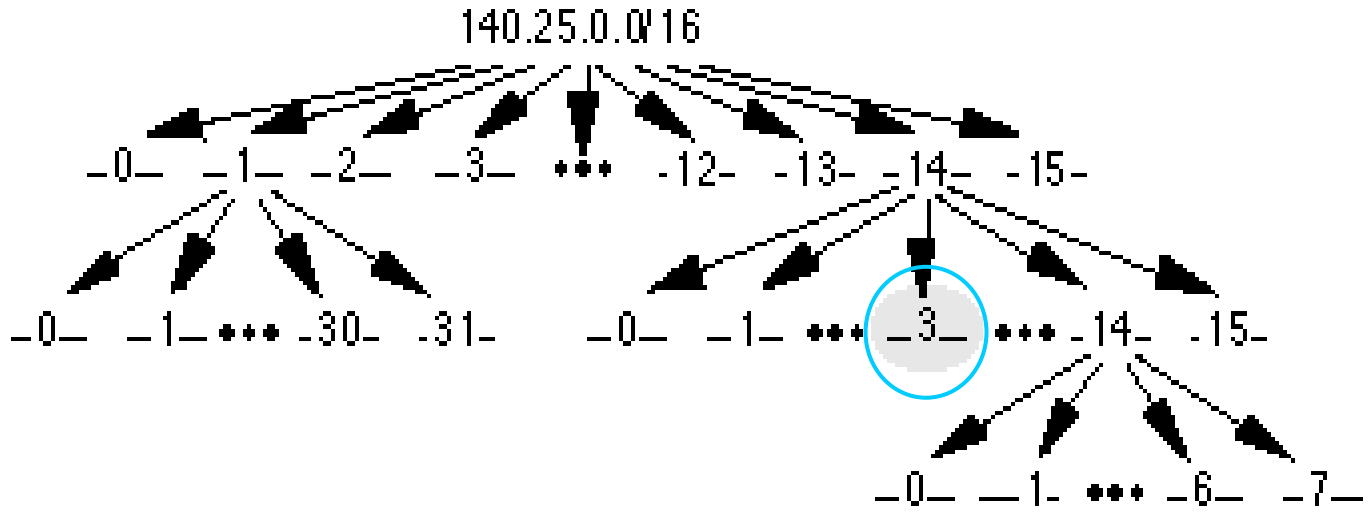


Es werden vier weitere Bits benötigt, um die erforderlichen Subnetze zu adressieren -> Netzwerkpräfix ***/24***

Die 16 Subnetze des Adressblockes 140.25.224.0/20 :

Subnetz #14: 10001100.00011001.11100000.00000000 = 140.25.224.0/20
Subnetz #14-0: 10001100.00011001.11100000.00000000 = 140.25.224.0/24
Subnetz #14-1: 10001100.00011001.11100001.00000000 = 140.25.225.0/24
Subnetz #14-2: 10001100.00011001.11100010.00000000 = 140.25.226.0/24
Subnetz #14-3: 10001100.00011001.11100011.00000000 = 140.25.227.0/24
Subnetz #14-4: 10001100.00011001.11100100.00000000 = 140.25.228.0/24
:
Subnetz #14-14: 10001100.00011001.11101110.00000000 = 140.25.238.0/24
Subnetz #14-15: 10001100.00011001.11101111.00000000 = 140.25.239.0/24

Festlegen der Hostadressen, die in Subnetz Nummer 14->3 zugewiesen werden können (140.25.227.0/24).



Jedes der Subnetze des Subnetzes 14 hat 8 Bits für die Hostadressen. Damit hat jedes Subnetz einen Block von 254 (=2^8-2) gültigen Hostadressen. Die Rechner werden von eins bis 254 durchnummeriert.

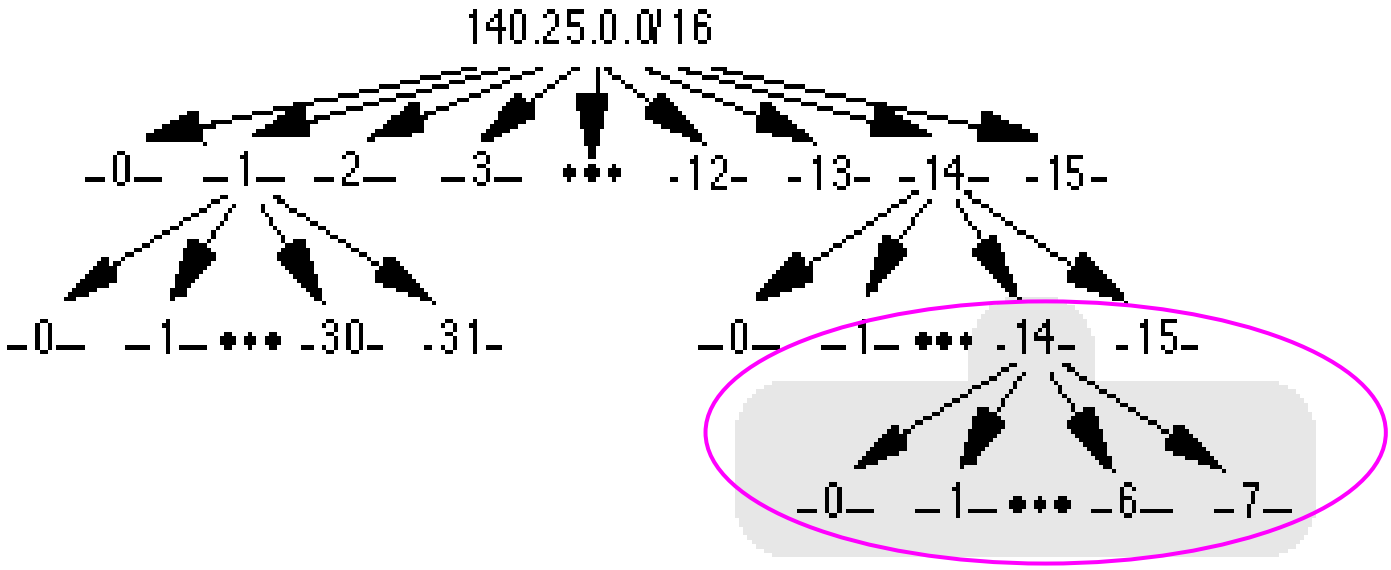
Die gültigen Hostadressen ergeben sich so zu:
Subnetz #14-3: 10001100.00011001.11100011.00000000 = 140.25.227.0/24
Rechner #1 10001100.00011001.11100011.00000001 = 140.25.227.1/24

Rechner #2 = 140.25.227.2/24
Rechner #3 = 140.25.227.3/24
Rechner #4 = 140.25.227.4/24
:
Rechner #253 = 140.25.227.253/24
Rechner #254 10001100.00011001.11100011.11111110 = 140.25.227.254/24

Broadcast-Adresse des Subnetzes #3
10001100.00011001.11100011.11111111 = **140.25.227.255**

Definieren der Subnetze des Subnetzes 14->14 (140.25.238.0/24)

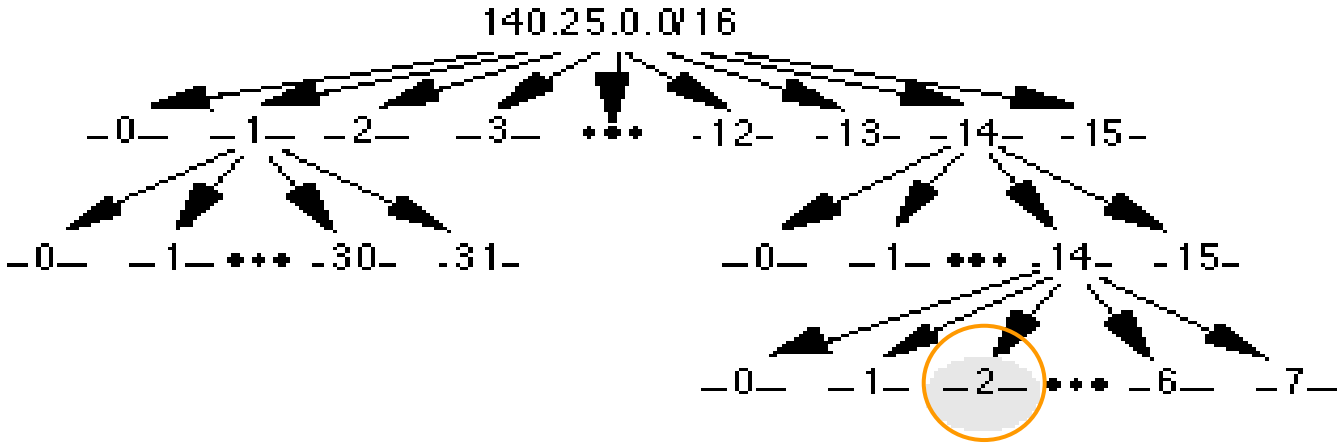
Nachdem das Subnetz 14 in 16 Subnetze unterteilt wurde, wird das Subnetz 14->14 nochmals in acht gleich große Adressblöcke unterteilt.



Es werden drei weitere Bits gebraucht, um die acht Subnetze zu adressieren; es muss daher ein Netzwerkpräfix /27 verwendet werden.

Subnet #14-14: = 140.25.238.0/24
Subnet#14-14-0: = 140.25.238.0/27
Subnet#14-14-1:10001100.00011001.11101110.00100000 = 140.25.238.32/27
Subnet#14-14-2:10001100.00011001.11101110.01000000 = 140.25.238.64/27 :
:
Subnet#14-14-6:10001100.00011001.11101110.11000000 = 140.25.238.192/27
Subnet#14-14-7:10001100.00011001.11101110.11100000 = 140.25.238.224/27

Festlegen der Hostadressen, die in Subnetz Nummer 14->14->2 zugewiesen werden können (140.25.238.64/27).



Jedes der Subnetze 14->14 hat fünf Bits in dem Feld für Hostadressen. - > Jedes Subnetz hat einen Block von 30 gültigen Adressen (2^5 -2).

Subnet#14-14-2:10001100.00011001.11101110.01000000 = 140.25.238.64/27
Rechner #1 10001100.00011001.11101110.01000001 = 140.25.238.65/27
Rechner #2 10001100.00011001.11101110.01000010 = 140.25.238.66/27
:
Rechner #29 10001100.00011001.11101110.01011101 = 140.25.238.93/27
Rechner #30 10001100.00011001.11101110.01011110 = 140.25.238.94/27

Broadcast-Adresse des Subnetzes 14->14->2 :
10001100.00011001.11011100.01011111 = 140.25.238.95

Übungsbeispiel :

Ein Administrator hat ein 192.168.1.0/24 Netzwerk.

Vier verschiedene Abteilungen mit unterschiedlicher Anzahl von Hosts werden gebraucht :

- Verkaufsabteilung: 100 Computer,
- Einkaufsabteilung: 50 Computer,
- Finanzabteilung: 25 Computer
- Management: 5 Computer.

Herkömmliches Subnetting teilt die Netze in Teilnetze mit gleicher, fester Größe -> Problem zu wenig Netze.

Aufgaben :

a) Lösen sie das Problem mit VLSM.

b) Die Werkstattabteilung würde auch noch gerne 10 Rechner im Netz unterbringen.

- Ist das möglich ?
- Wenn ja, wie ?

c) Testen sie ihre Lösung mit dem Packet Tracer.

Wichtige Kommandozeilenbefehle für die Netzwerkadministration

ping

•Standard-Diagnosewerkzeug zur Überprüfung der Netzwerkverbindung zu einem oder mehreren Remotehosts.
•Mit einem Ping sendet man eine Serie von ICMP-„Echo-Request“-Paketen ("ping") an die Zieladresse des zu überprüfenden Hosts. Der Empfänger muss, sofern er das Protokoll unterstützt und entsprechend konfiguriert ist, eine Antwort zurücksenden: ICMP „Echo-Reply“ ("pong").
•Aus der Laufzeit (Round-Trip-Delay) lässt sich die Latenzzeit (-> Qualität) einer Netzwerkverbindung abschätzen.

ipconfig

•Zeigt alle aktuellen TCP/IP-Netzwerkkonfigurationswerte an und aktualisiert all DHCP- und DNS-Einstellungen.

net

- net ist ein umfangreiches Netzwerk-Programm mit vielen Unterfunktionen.
- net /? zeigt eine Liste der verfügbaren net-Befehle an.

netstat

- zeigt Protokollstatistiken und die aktuelle TCP/IP-Netzwerkverbindungen an.

nslookup

- zeigt Informationen von DNS-Namensservern (DNS = Domain Name System) an.

arp

- Ändert und zeigt die Zuordnungstabellen für IP-Adressen ↔ MAC (physikalische) Adressen an, die der Computer aktuell gespeichert hat.

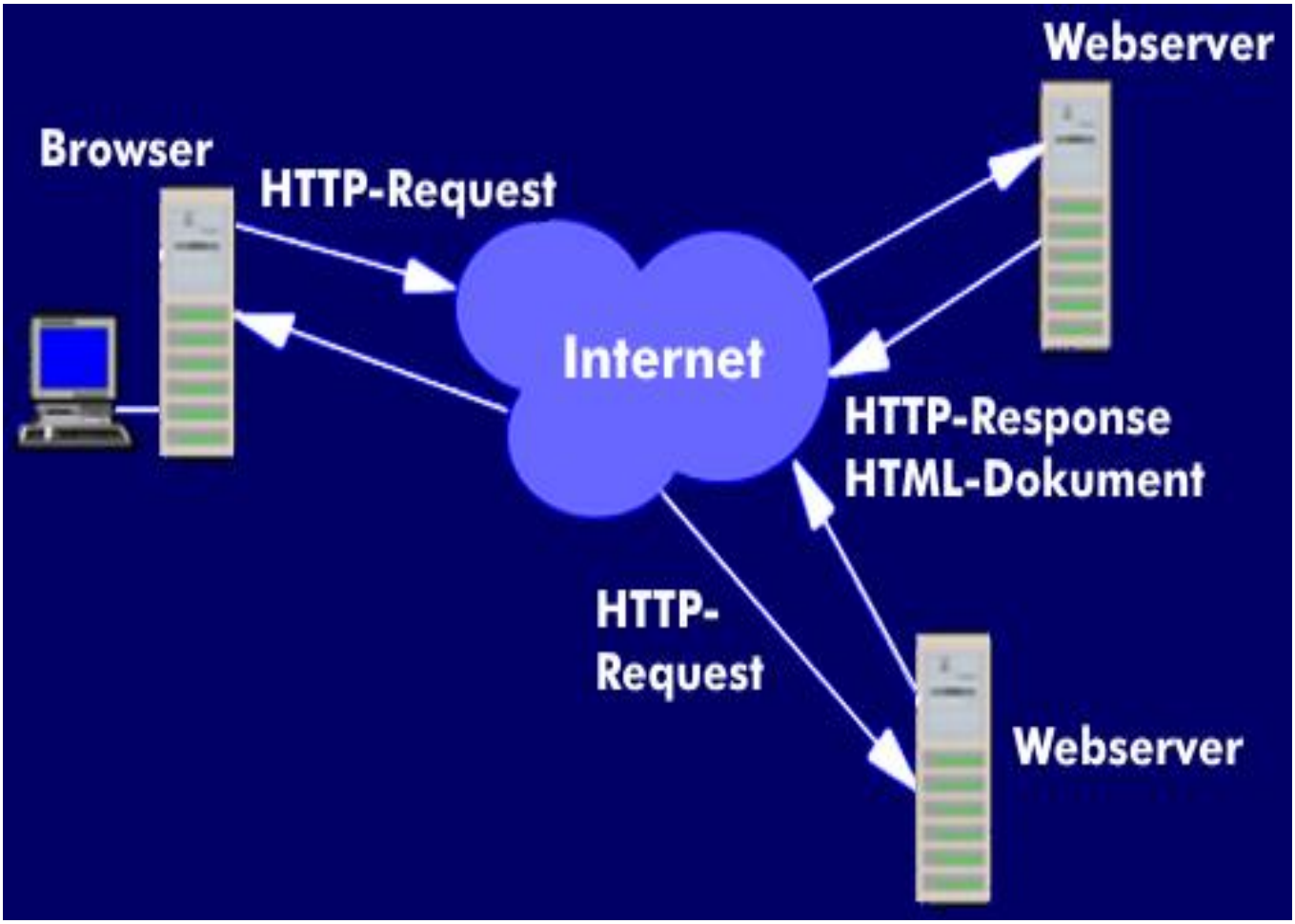
tracert (trace route)
ermittelt die Route zu einem Ziel, indem es ICMP-Echopakete (Internet Control Message Protocol/"Pings") mit schrittweise inkrementierenden TTL-Werten (Time-to-Live) sendet. Jeder im Pfad befindliche Router dekrementiert den TTL-Wert eines Paket vor dem Weiterleiten um 1. Somit gibt der Endstand des TTL-Werts die Anzahl der Abschnitte (Hops) der Route an.

route print (-4 oder -6 -> IP-Version)
Routingtabellen anzeigen

route add
um eine Route anzulegen

Webserver

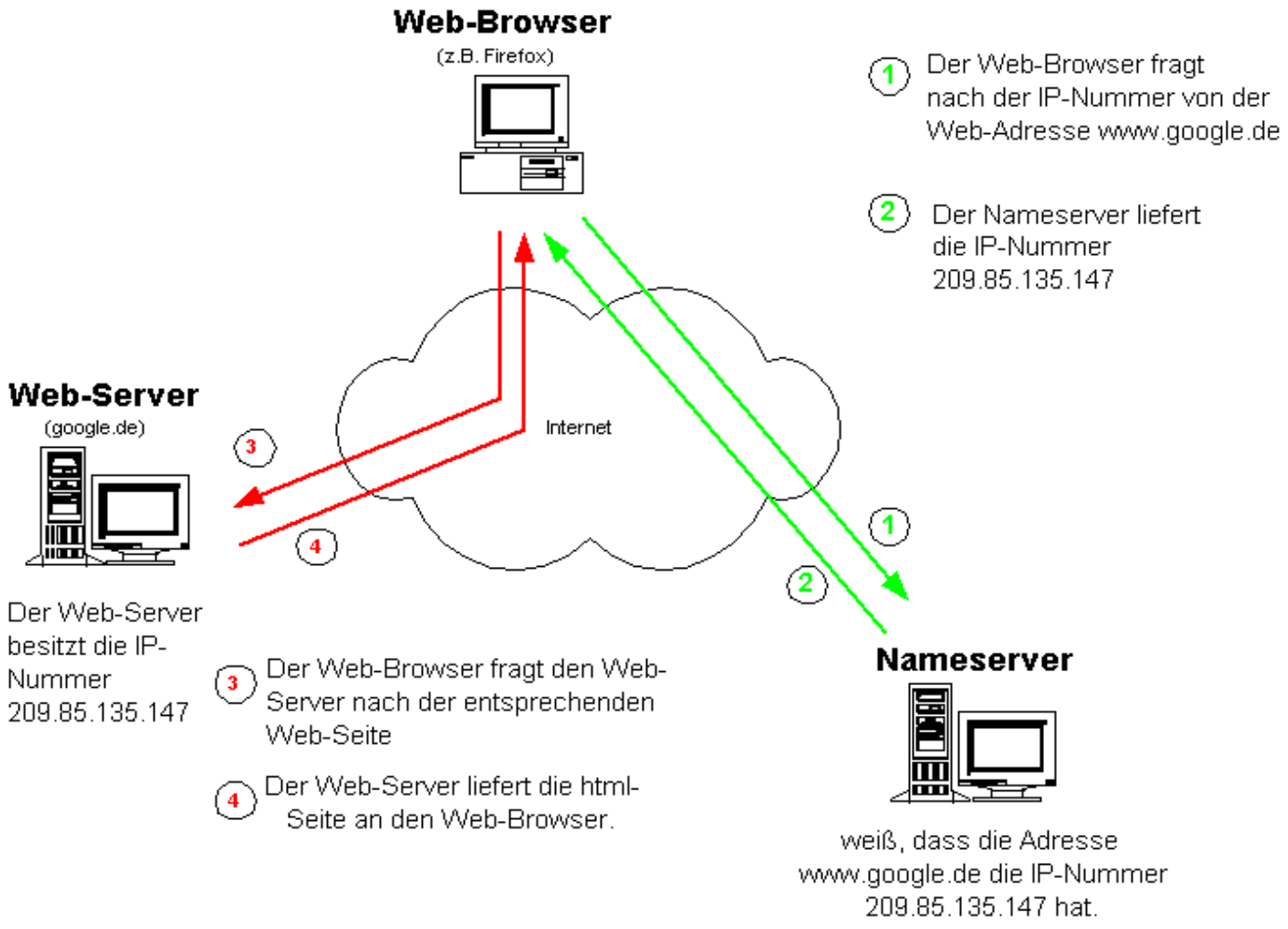
Webserver sind von z.B. Providern betriebene Server für das Webhosting.
Sie sind mit dem Internet oder Intranets verbunden und stellen Websites und andere Online-Informationen bereit, die beispielsweise auf Anforderung eines Browsers, das ist der Web-Client, über das Hypertext Transfer Protocol (HTTP) oder über HTTPS angefordert werden können.



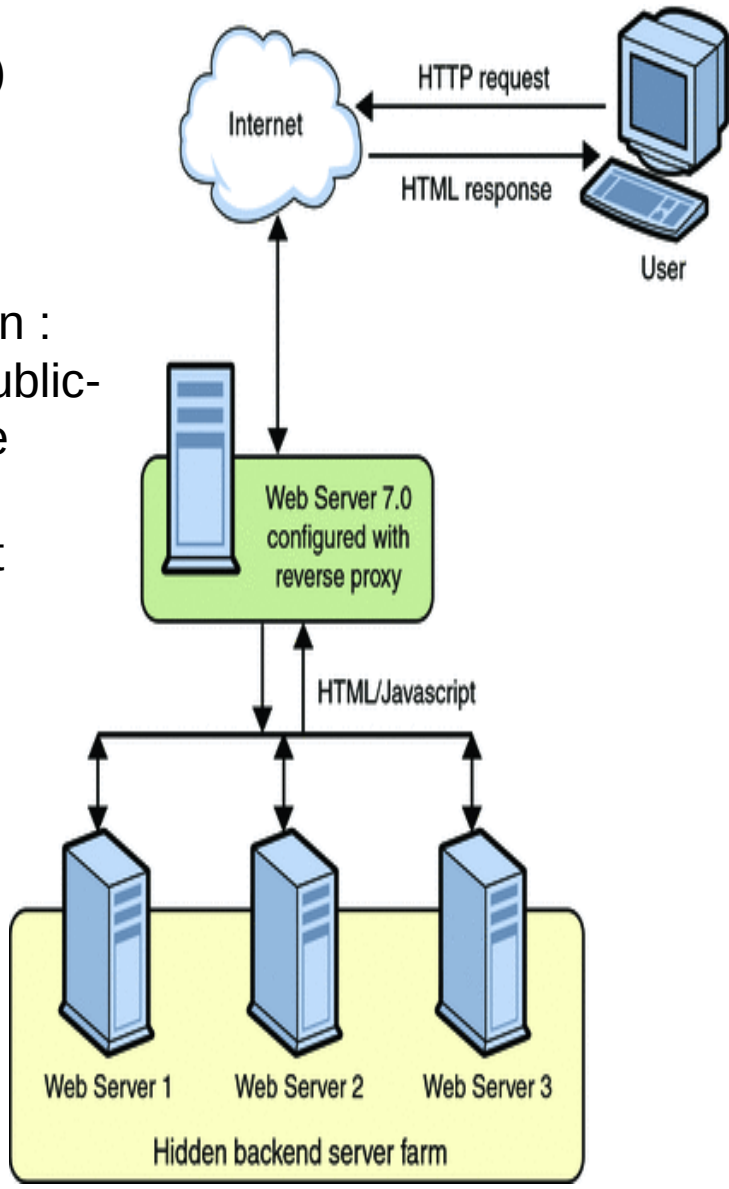
Aufruf einer Webseite durch einen Browser :

- Die in den Browser eingegebene Internetadresse wird zum Nameserver (-> DNS) geleitet.
- Der ermittelt aus dem Domainnamen die IP-Adresse.
- Der HTTP-Client des Web-Browsers baut eine TCP-Verbindung zum HTTP-Server des Webservers auf und stellt an diesen eine Anfrage (-> Request) in der er eine Webseite anfordert.
- Der HTTP-Server schickt die angeforderten Dateien an den HTTP-Client, der sie über den HTTP-Interpreter auf dem Bildschirm darstellt.
- Nach Erhalt der kompletten Webseite wird die TCP-Verbindung wieder abgebaut.

Da komplette Webseiten aus verschiedenen HTML-Texten, Grafiken, Flashs, Fotos oder Videos bestehen, muss der Client für jede Datei eine eigene Anfrage stellen, die der Webserver durch Übermittlung der Dateien beantwortet.



Informationen die auf Webservern bereitgestellt werden :
- HTML-Seiten
- CSS (Cascading Stylesheets)
- Text- und Grafikdokumente
- dynamische datenbankbasierte Seiten
- Audio und Videodateien
- Skriptdateien (Javascript, PHP)



Betriebssysteme von Webservern :
Unix und Linux -> als gängige Public-Domain-Software kommt Apache zum Einsatz. (-> XAMPP)
Kommerzielle Software : Internet Information Server (IIS) von Microsoft.

Webserver übernehmen auch sicherheitsrelevante Funktionen :
- Datenaustausch über das HTTPS-Protokoll
- Verwalten von Cookies
- geben über den HTTP-Status-Code Statusmeldungen an den Browser (z. B.: Webseite kann nicht aufgerufen werden oder existiert nicht).

Netzwerkzugang per Modem (analoge Telefonleitung) -> historisch

Mit einem Modem (**Mo**dulator und **Dem**odulator) werden digitale Daten durch Modulation eines analogen Signals über analoge Kommunikationsnetze (Telefonnetz, Kabel-TV), Standleitungen und per Funk übertragen.

Telefonmodems

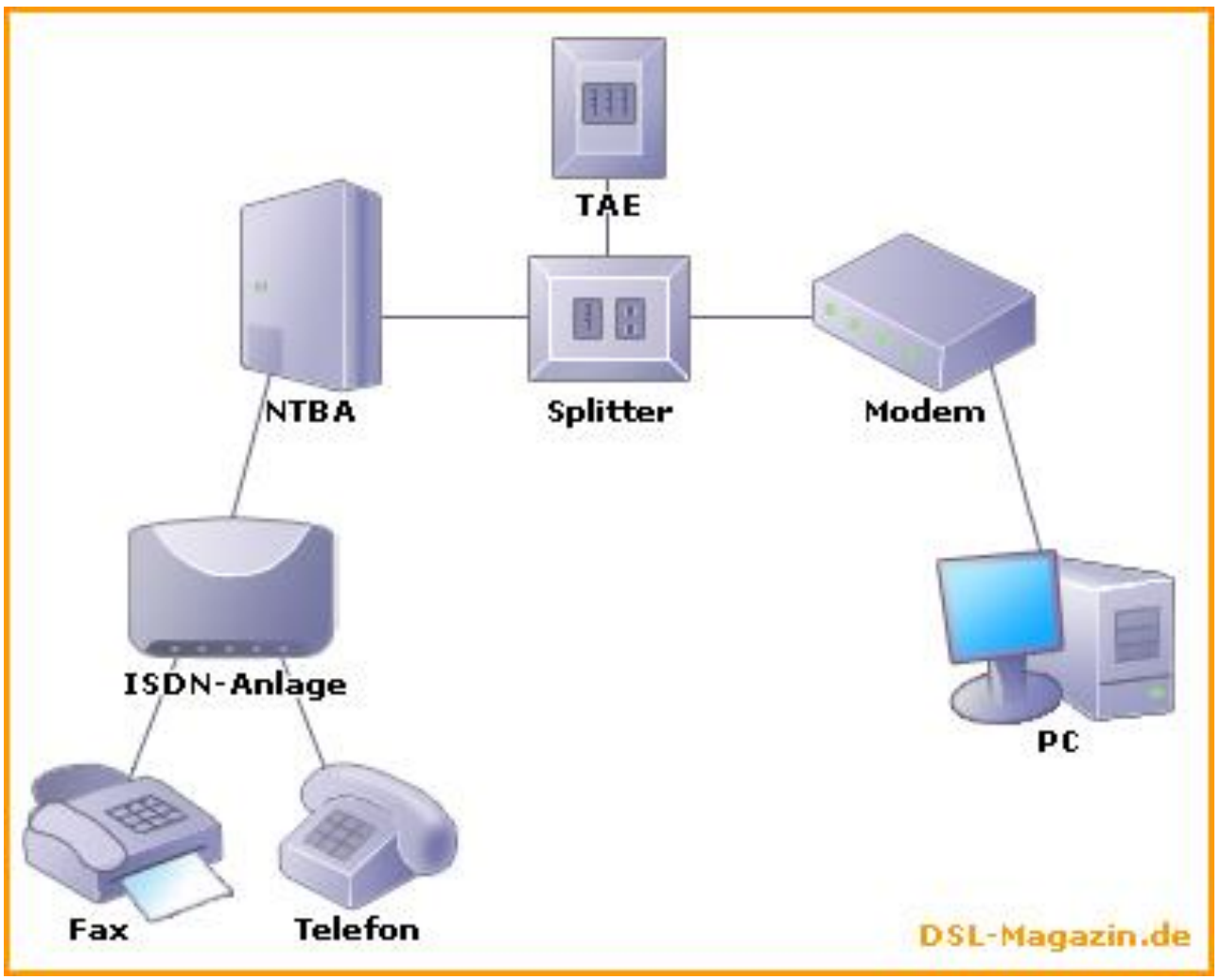
Telefonmodems sind an die Besonderheiten des Telefonnetzes angepasst.

Download-Datenrate von bis zu 56 kbit/s

xDSL-Modems

Das Endgerät beim Nutzer ist weiterhin ein Modem, wenn auch mit erheblich größerer Bandbreite.

Um die analoge und digitale Telefonie auf derselben Leitung gleichzeitig übertragen zu können, wird die Leitung durch einen sogenannten Splitter in zwei verschiedenen Frequenzbereichen genutzt.



Begriffe zu Kommunikationsnetzwerken

TAE (Telekommunikations-Anschluss-Einheit = Telefondose)

NTBA (Network Termination for ISDN Basic rate Access)

DSL-Modem, "**NTBBA**" (**N**etwork **T**ermination **B**road **b**and **A**ccess)

POTS Abkürzung für "**P**lain **o**ld **t**elephone **s**ervice" (englisch „einfacher alter Telefondienst“,

-> Bezeichnung für den analogen Telefondienst

DSLAM
Digital Subscriber Line Access Multiplexer

DSL

Über die **Digital Subscriber Line** (engl. für Digitale Teilnehmeranschlussleitung) können Haushalte und Unternehmen Daten mit hoher Übertragungsrate (bis 50.000 kbit/s) senden und empfangen.

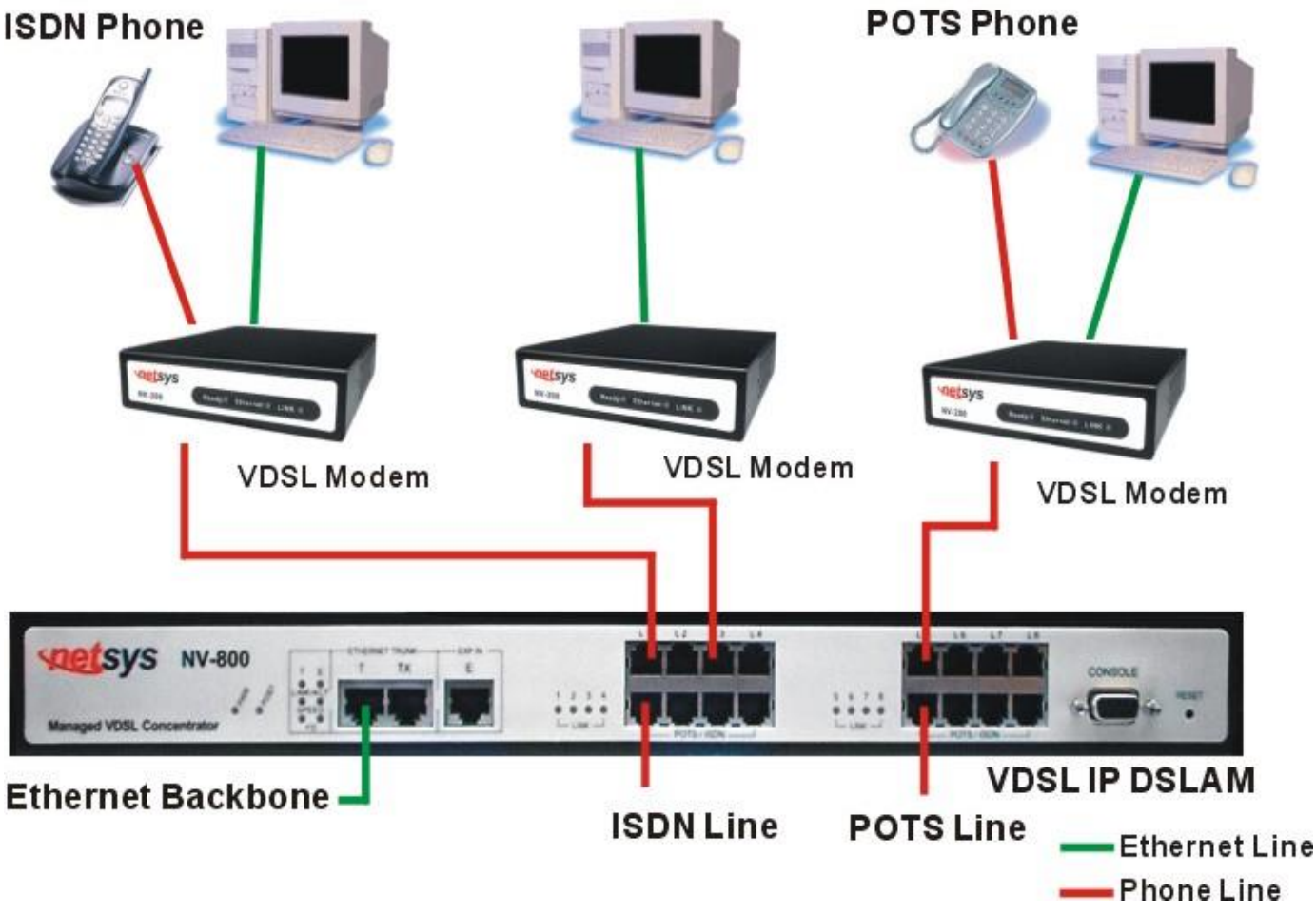
Die meisten DSL-Verfahren nutzen die bereits verlegte Kupfer-Doppelader des Telefonnetzes.

VDSL2

Very High Speed Digital Subscriber Line ist eine DSL-Technik, die wesentlich höhere Datenübertragungsraten über gebräuchliche Telefonleitungen liefert als beispielsweise ADSL oder ADSL2+.

Datenübertragungsraten von bis zu 200 Mbit/s

Kann mit Glasfaser-Kupfer-Mix umgehen

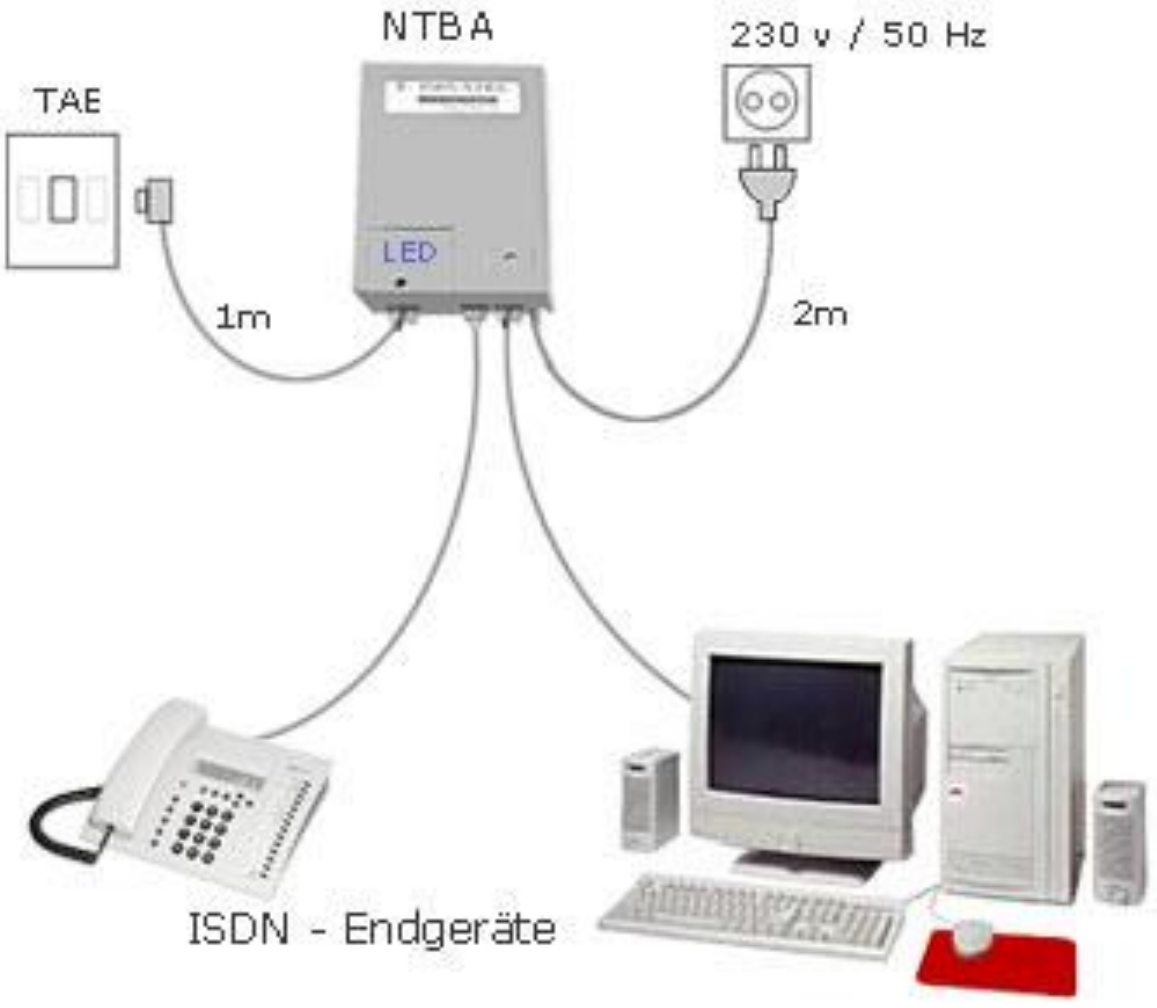


ISDN
(Integrated Services Digital Network)

Internationaler Standard für ein digitales Telekommunikationsnetz.

Verschiedene Dienste wie Fernschreiben (Telex), Datex-L (leitungsvermittelte Datenübertragung), Datex-P (paketvermittelte Datenübertragung) und Telefonie übertragen

Bandbreite 2 × 64 kbit/s



Netzwerkbetriebssystem
engl.: network operating system (NOS)

Das Netzwerkbetriebssystem wird auf den sogenannten Server geladen und erlaubt es den Benutzern an den angeschlossenen Arbeitsstationen bzw. Clients, Nachrichten und Daten auszutauschen, sowie Dateien und Peripheriegeräte gemeinsam zu nutzen.

Konzept des Netzwerkbetriebssystems wurde 1983 von Novell eingeführt.

Die bekanntesten Netzwerkbetriebssysteme sind Netware von Novell, einige Linux-Derivate, Windows NT, Windows 2000, Windows 2003 und Unix.

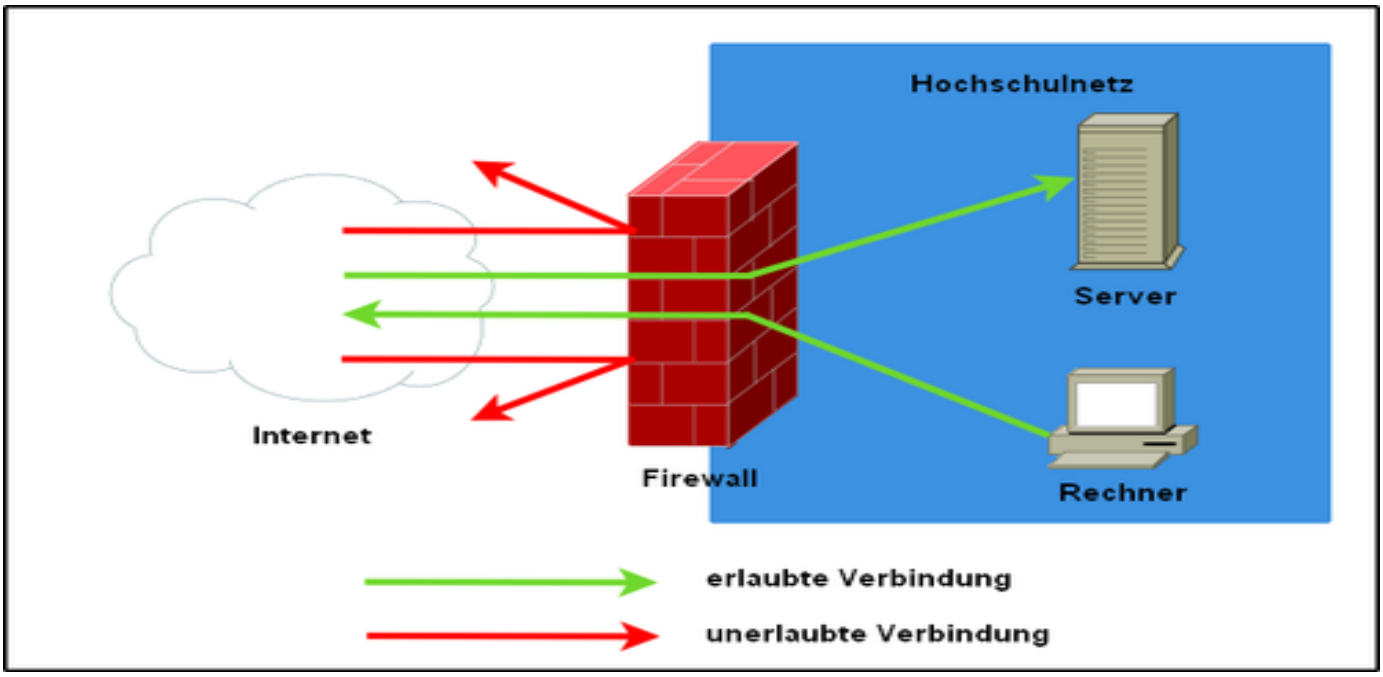
Möglichkeiten von Benutzerverwaltung im Netzwerk

Peer-to-Peer (Arbeitsgruppe)
DOS, Windows 95/98/ME/XP/Vista, MacOS

Server-Client (Domäne)

Windows NT Server, 2000 Server, 2003 Server (mit Active Directory), Linux (mit NIS) oder Novell NDS.

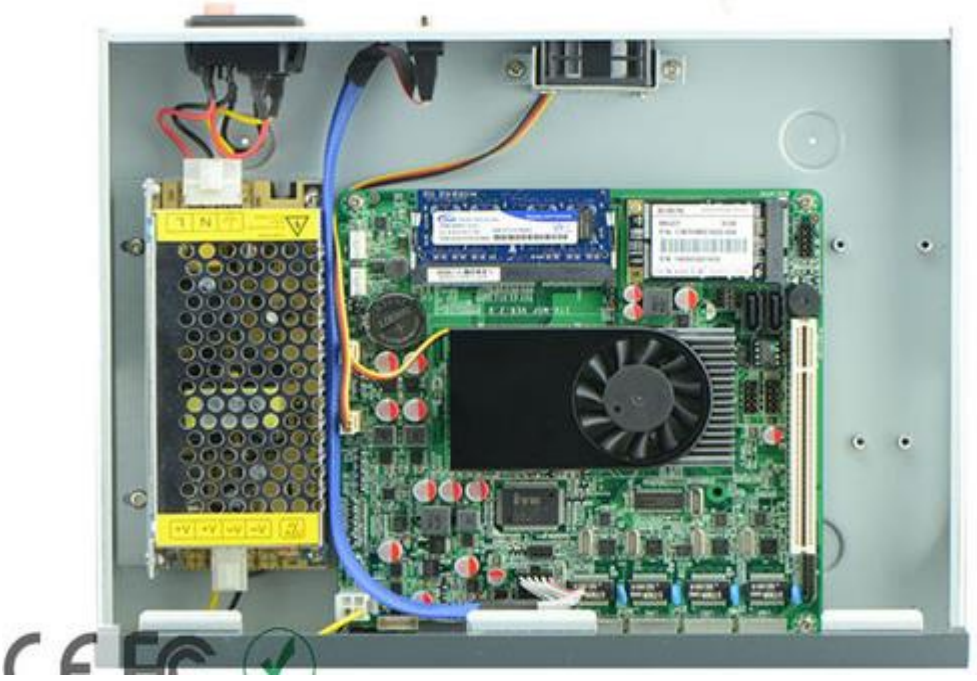
Firewall (engl. Brandwand)



Hauptaufgabe :

Unterbinden von Datenverkehr von extern zum geschützten Bereich und umgekehrt.

- sitzen an Schnittstellen zwischen einzelnen Netzen.
- kontrollieren den Datenverkehr zwischen den Teilbereichen.
- verhindern ungewünschten Verkehr.
- häufiger Einsatz zwischen LANs und WANs.



Hardware :

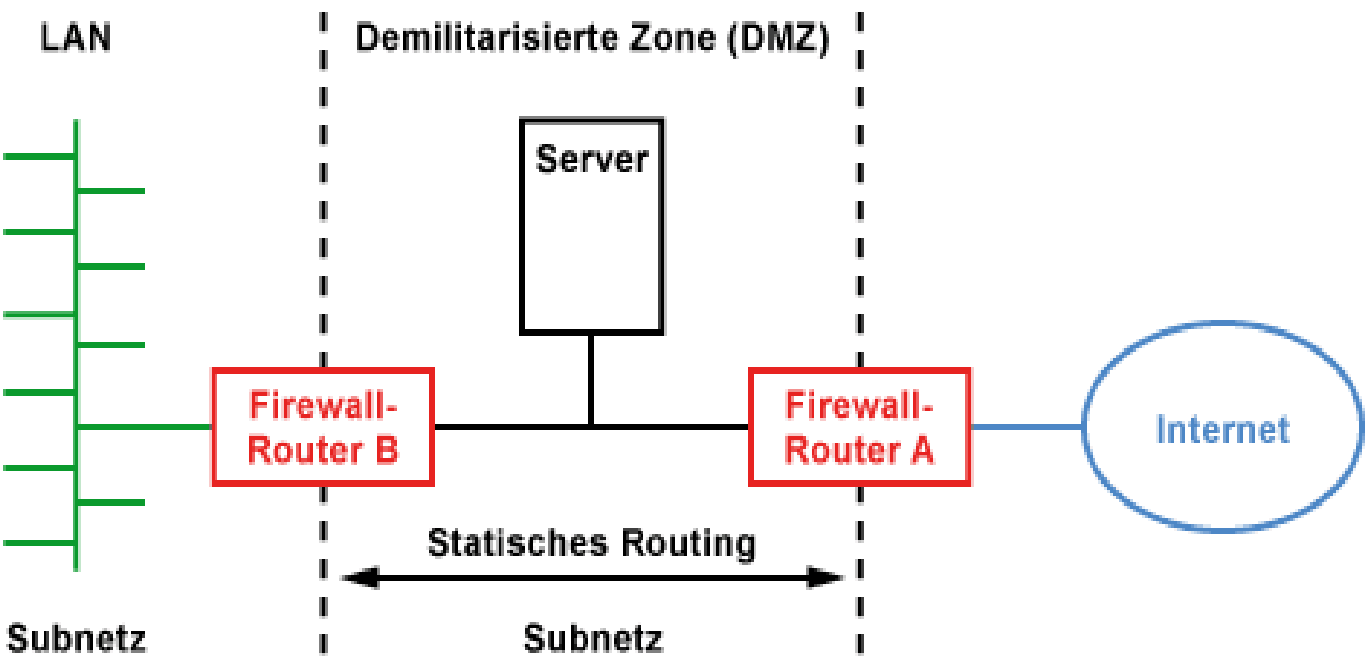
- für das Senden und Empfangen der Datenpakete zuständig.
- kein sicherndes Element.
- häufige Netzelemente: Router, Gateways.

Software

- regelt den Datenverkehr
  (wer darf, wer nicht?).
- läuft oft auf spezieller Hardware.

Netzwerk-Firewall

- Gerät mit mehreren Netzwerkschnittstellen.
- darauf laufende Software dient hauptsächlich als Firewall.
- In der Regel wird zwischen drei Netzwerkzonen unterschieden :
  - das externe Netz (WAN -> Internet), nicht vertrauenswürdig => **Untrusted**
  - die demilitarisierte Zone (DMZ), vom externen Netz aus erreichbare Server.
  - das interne Netz (LAN), vertrauenswürdig => **Trusted**



Host-Firewall

- Software arbeitet auf Hardware die auch für andere Zwecke verwendet wird.
  (PC mit Windows oder Linux)
- Host-Firewalls und „Personal Firewalls“ werden als Software-Firewall bezeichnet.
- Software arbeitet auf den Schichten 2-7 des OSI-Referenzmodells.

Personal Firewall

- lokale Installation auf dem zu schützenden Rechner.
- Regelt nur Verkehr vom und zum Rechner.
- Keine Überwachung zwischen verschiedenen Netzen.
- Einfache Konfiguration.
- Stealth-Modus.
- Eher geringe Schutzwirkung.

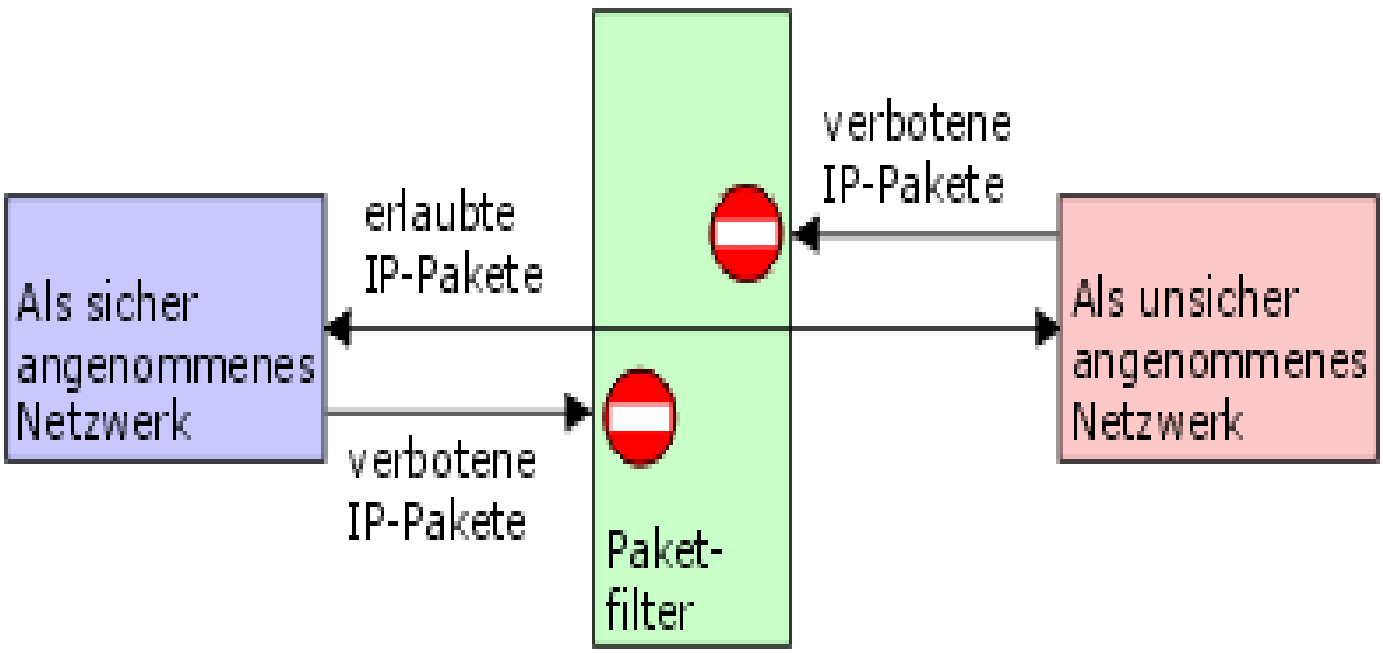
Paketfilter

- Paket-Filter Firewalls kontrollieren die Datenpakete auf der dritten Schicht des OSI Modells –> Netzwerk-Schicht (IP).

- Vergleich von Quell –und/oder Zieladresse der Pakete
- nimmt Filterungen anhand der erstellten Regeln vor :

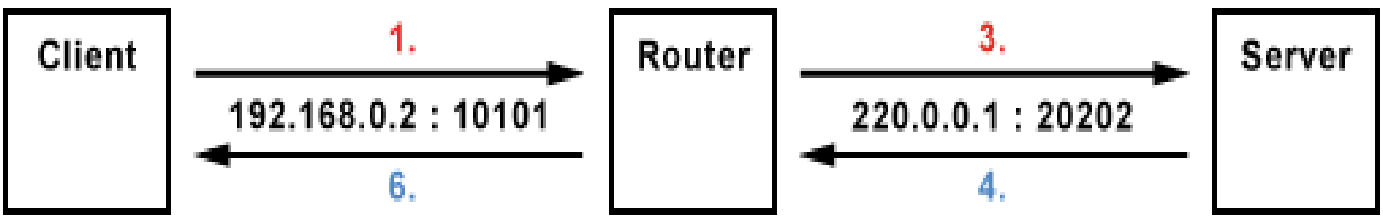
- Ebene der Ports
  - z.B.: FTP – Port 21 sperren

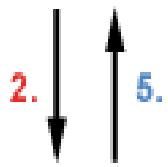
- Ebene der IP-Adressen
  - z.B.: Paket von 87.92.100.100 nicht durchlassen



- NAT – **N**etwork **A**ddress **T**ranslation
- PAT – **P**ort **A**ddress **T**ranslation
- Umsetzung von privaten IP – Adressen auf eine öffentliche
  - z.B. DSL – Anschluss mit dynamischer IP

- Dadurch ist das Netzwerk nach Außen nicht sichtbar.





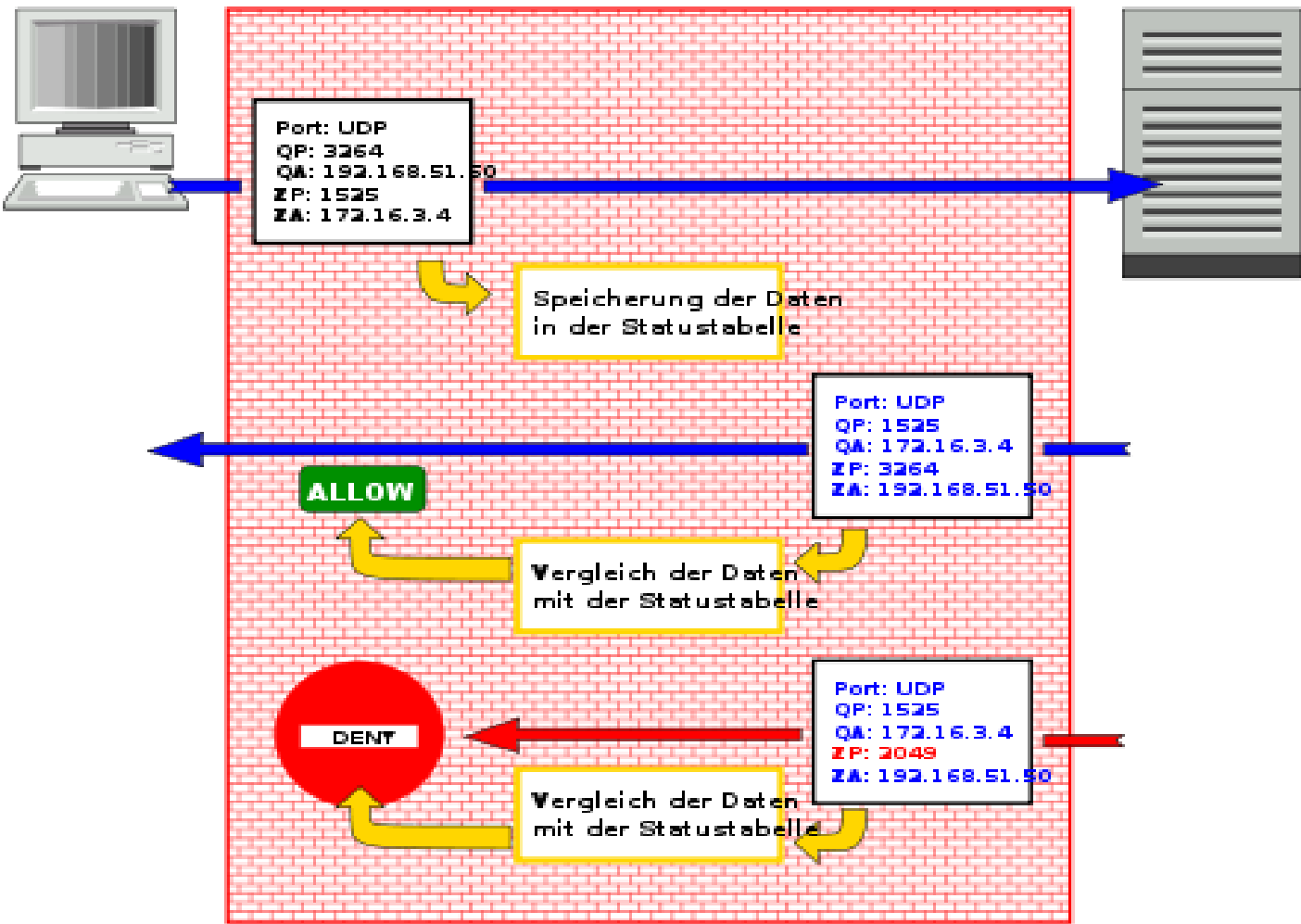
NAT-Tabelle

LAN-Port	LAN-Adresse	WAN-Port
10101	192.168.0.2	20202
.	.	.
.	.	.

Content-Filter – Stateful Inspection

- Filter höherer Ebenen
- Aufgaben
  - Herausfiltern von z.B. ActiveX oder JavaScript in angeforderten HTML-Seiten
  - Filtern/Kennzeichnen von Spam-Mails
  - Informationen herausfiltern (vertrauliche Bilanzen)

- betrachtet wird der ganze Datenverkehr (z.B. HTML-Seite)
- Pakete werden zusammengesetzt
- Überprüfung
- Pakete werden wieder in ursprünglichen Datenstrom zerlegt



DNS Grundlagen

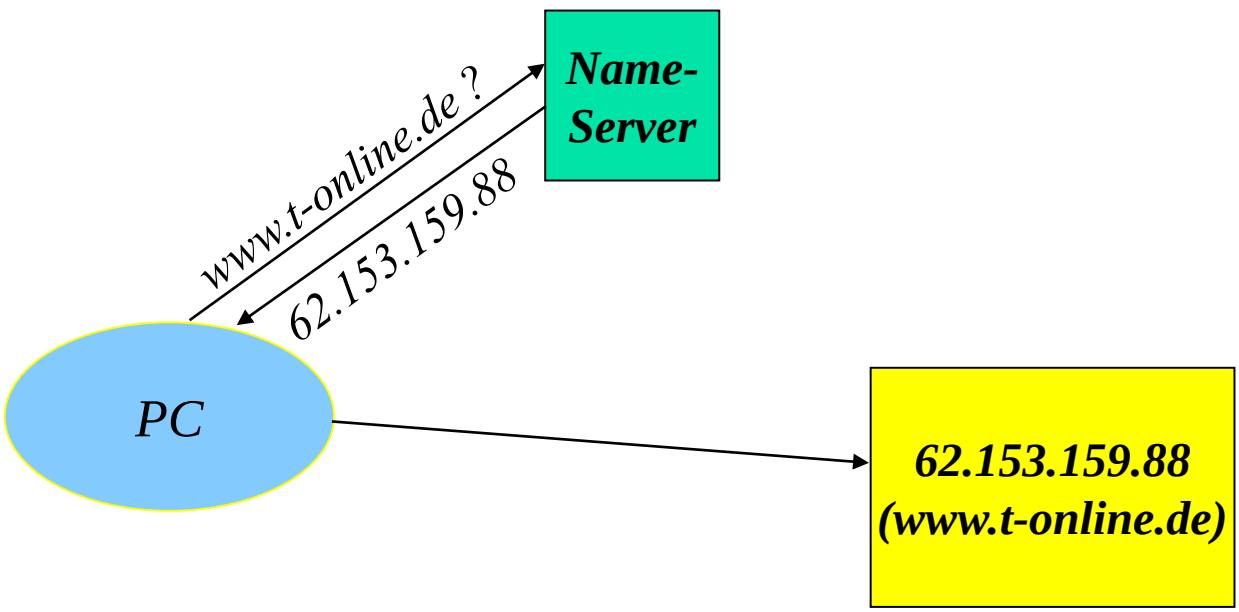
- IPv4-Adressen -> 32 Bit -> Dezimalzahlen
  - IPv6-Adressen -> 128 Bit -> Hexzahlen
- gut für Computer, nicht für Menschen

-> Namen (www.t-online.de) sind leichter zu merken

-> wie z.B. Telefon → Auskunft (Telefonbuch)

- im WWW → DNS (Domain Name System) → Tabelle mit Rechnernamen und IP-Adressen

Wie funktioniert die Namensauflösung ?



Verschiedene Techniken ! (die wichtigste ist DNS → WWW, WINS (von Microsoft) → (veraltet))

Früher (aber immer noch vorhanden): die hosts-Datei

- Jeder Rechner hat ein lokales “Telefonbuch“

-> C:\Windows\System32\drivers\etc\hosts (Win10)

-> /etc/hosts (Unix)

Verbindung zu anderem Rechner :

- Eine Betriebssystemfunktion (resolver) holt IP-Adresse aus hosts Datei.

-> damit ist die IP-Adresse bekannt und die Verbindung kann aufgebaut werden.

Analogie: Telefonbuch

- Liste mit Namen und Nummern
- nach Namen sortiert
- Suche nach Name

hosts-Datei: Beispiel

```
# Copyright (c) 1993-1995 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows NT.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

127.0.0.1            localhost
192.168.1.101        dbserv
192.168.1.102        mora
192.168.1.100        vaio
192.168.1.200        icon-95
192.168.1.103        david
```

Probleme

Wie bleibt die hosts-Datei aktuell ?

- Wenn neue Rechner dazukommen oder wegfallen
- Bei Adressänderungen

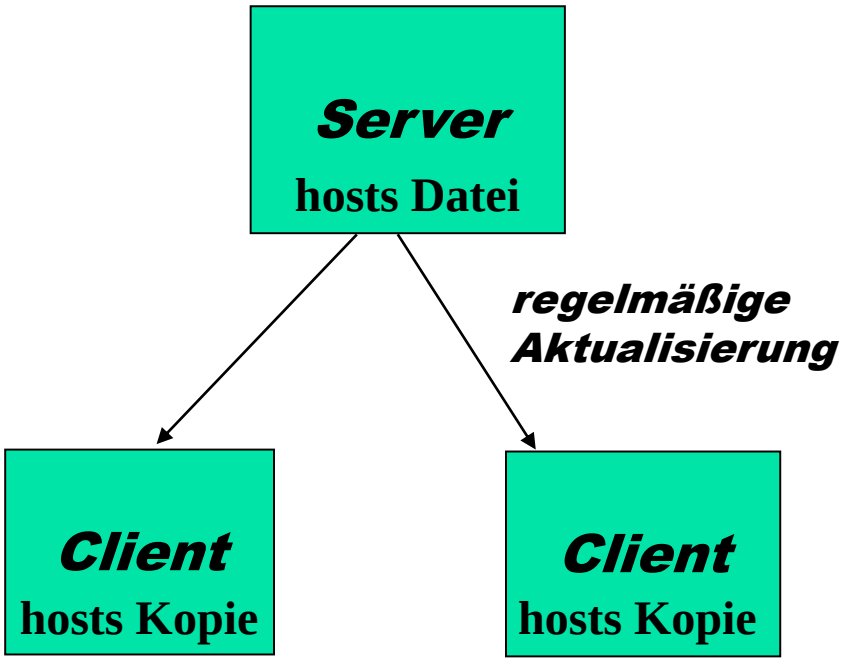
ARPA-Net (Vorläufer des Internet)

- 4-100 Rechner
- hosts Datei wurde (auf allen Rechnern) von Hand gepflegt

später

- einige hundert bis tausend Rechner
- hosts Datei wurde auf einem Server gepflegt
- auf alle anderen kopiert (FTP, email)

replizierte hosts Datei



Probleme heute :

- Annahme: 1 Million Rechner
  -> hosts Datei ist dann etwa 100 MB groß
- Aktualisierung stündlich
  - 1.000.000 * 100 MB/Stunde
    -> etwa 1000 Gbit/s
- Annahme: 1 Million Änderungen pro Jahr
  - etwa 5000 pro Tag
  - automatisch:
    Wer löst Konflikte (doppelte Namen,...) ?
  - von Hand: ..... ??
- Lösung: Ein/mehrere zentrale Auskunftsrechner
  - etwa 1.000.000 Anfragen/Sekunde

Lösung **DNS -> Domain Name System**

- Domain Hierarchie
- Eine zentrale Stelle pflegt "Root" oder "First-Level"-Domains (.de, .com, .net,..)
- Verwaltung der "Subdomains" wird delegiert
- Klare Regelung der Kompetenzen

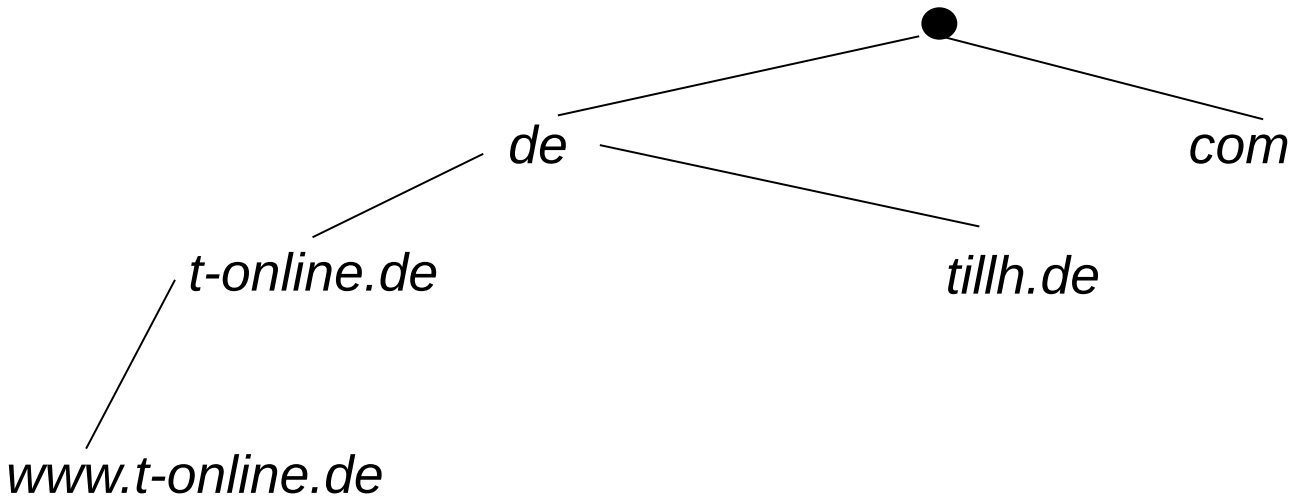
Das Domain-Name-System ist in einer Baumstruktur organisiert.

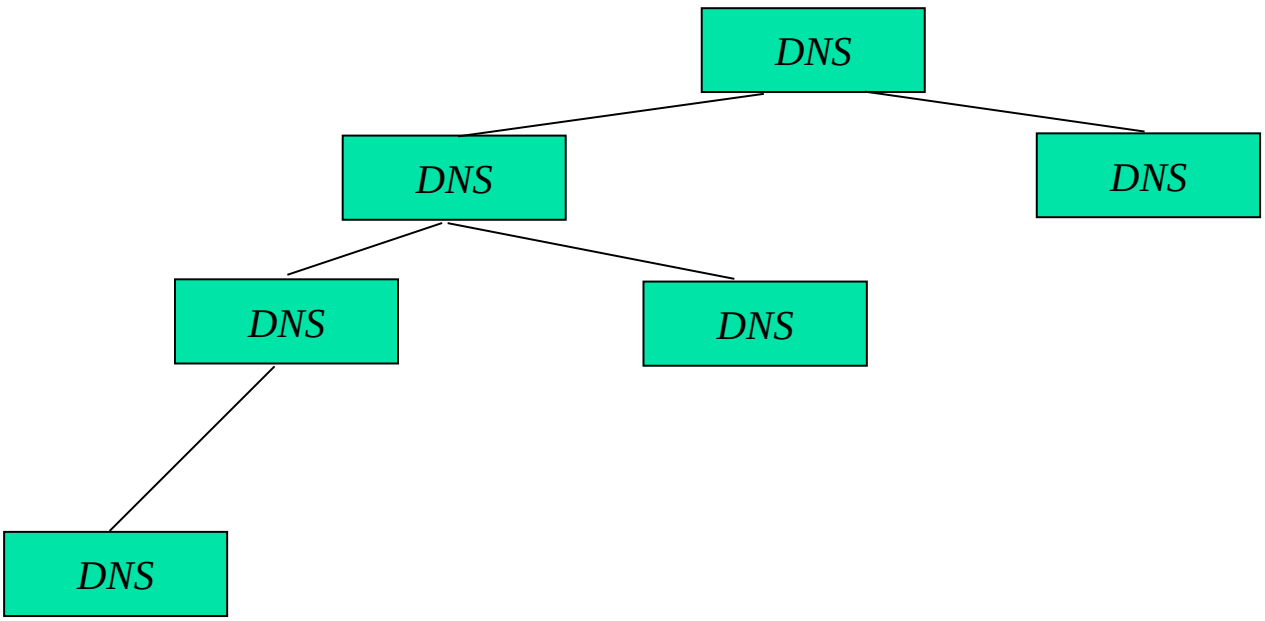
Dabei kann man die Blätter mit den Hostnames gleich setzen.

Nach der Wurzel (Root)

folgen als oberste Ebene die

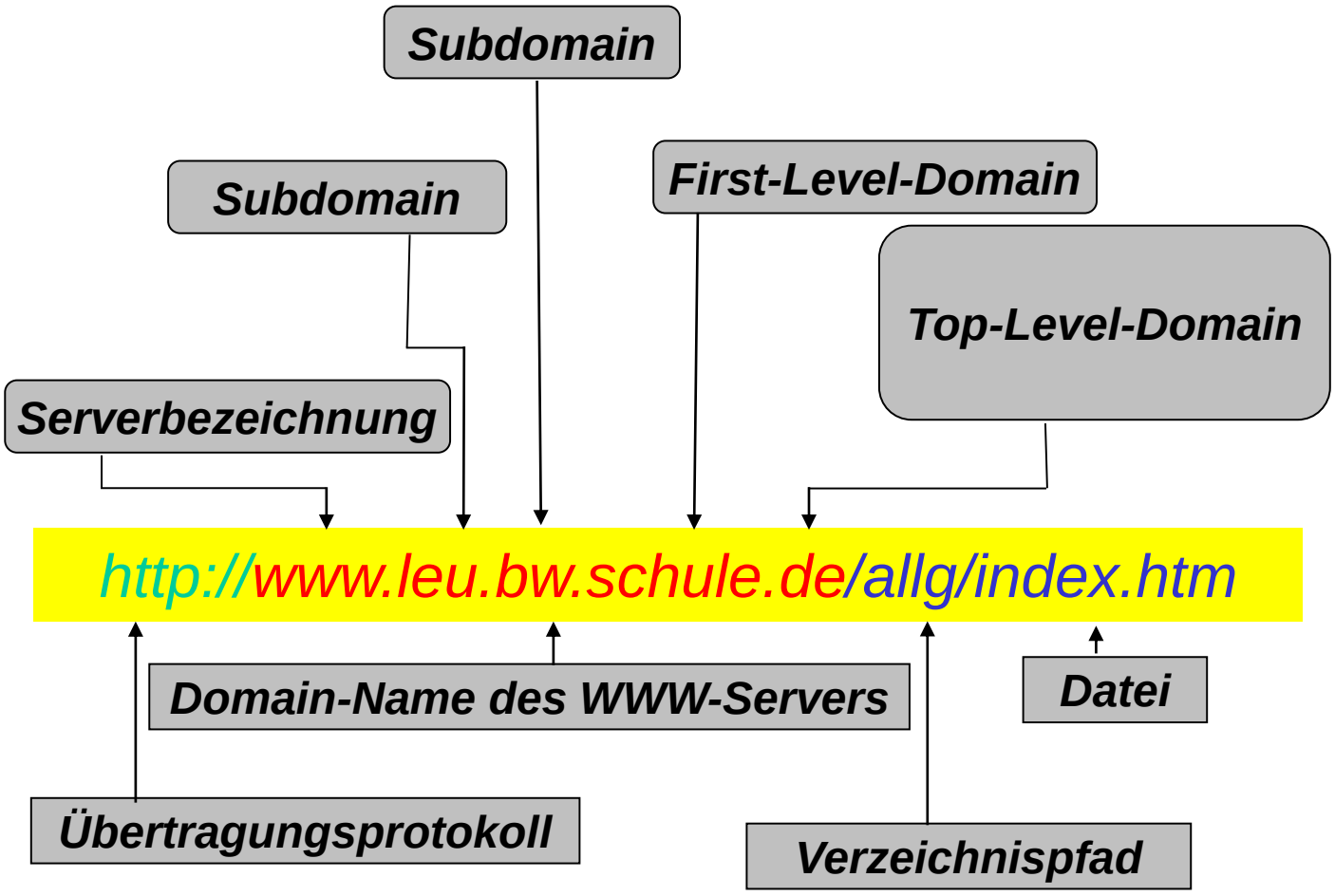
- Top-Level-Domains (TLDs), darunter folgen die
- First-Level-Domains eventuell gefolgt von einer oder mehreren
- Subdomains





URL: Uniform Resource Locator

Jede Seite besitzt eine eindeutige URL !



www gehört zum Servernamen.

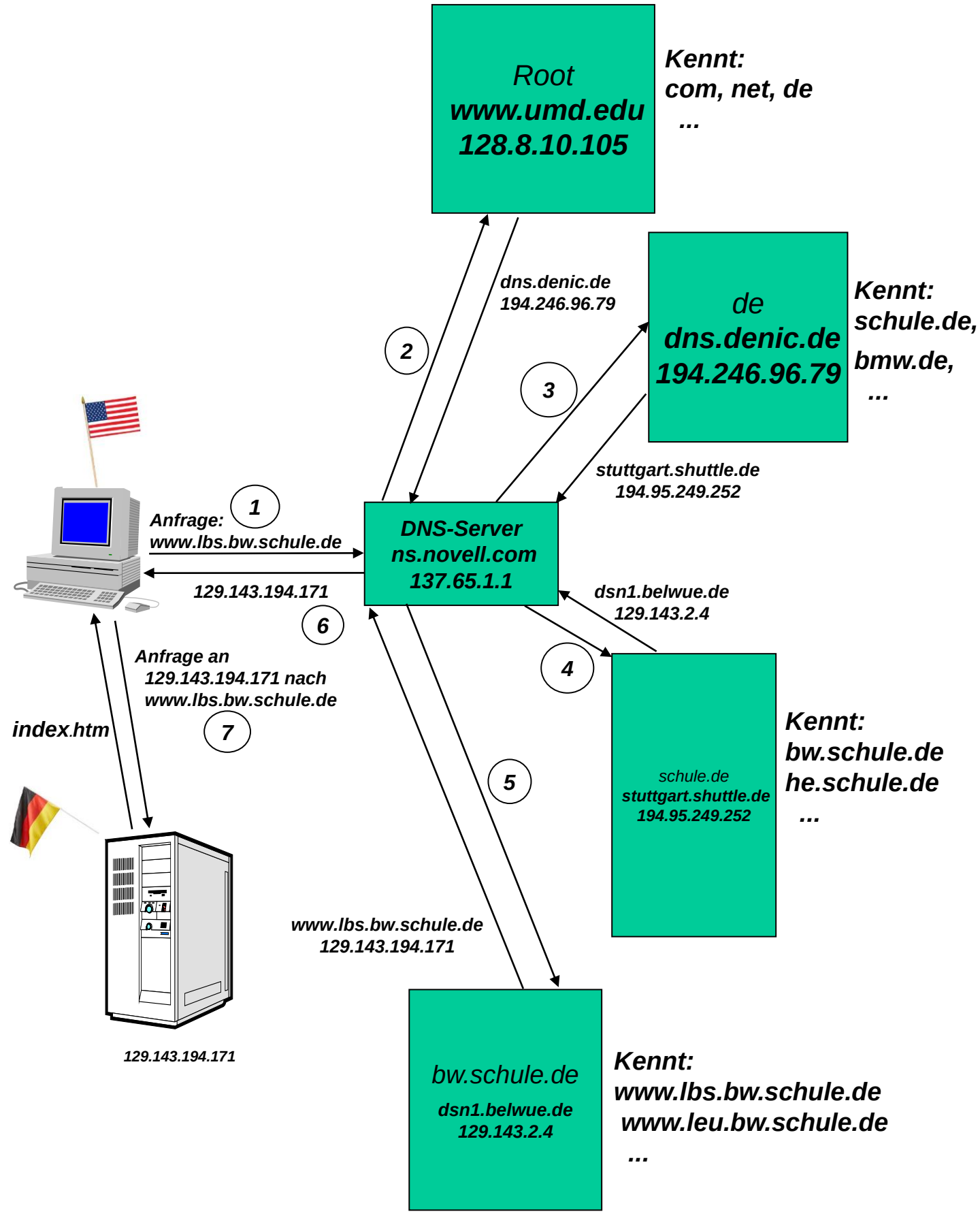
Das Protokoll wird allein durch http:// festgelegt.

http:// www.novell.com
http:// support.novell.com
http:// developer.novell.com

dies sind 3 verschiedene Webserver von Novell

Ablauf einer DNS-Abfrage

Beispiel: ein Mitarbeiter von Novell-USA will eine Seite vom Landesbildungsserver abrufen. -> ***www.lbs.bw.schule.de***



Root-Nameserver

- *Es gibt 13 Root-Nameserver (A.ROOT-SERVER – M.ROOT-SERVER)*
- *Im Root-Zonen-File des A.ROOT-SERVERs werden alle Informationen zentral verwaltet.*
  Auf den Rootservern B bis M befindet sich je eine Kopie des Root-Zonen-Files.
- *Jeder Nameserver im Internet kennt in der Regel alle 13 Rootnameserver*

Server-name	Betreiber	URL des Betreibers	IP des Nameservers	Standort
A	Network Solutions	www.netsol.com	198.41.0.4	Herndon, VA, USA
B	Information Sciences Institute, University of Southern California	http://www.isi.edu/	128.9.0.107	Marina Del Rey, CA, USA
C	PSINet	http://www.psi.net/	192.33.4.12	Herndon, VA, USA
D	University of Maryland	http://www.umd.edu/	128.8.10.90	College Park, MD, USA
E	NASA	http://www.nasa.gov/	192.203.230.10	Mountain View, CA, USA
F	Internet Software Consortium	http://www.isc.org/	192.5.5.241	Palo Alto, CA, USA
G	Defense Information Systems Agency	http://nic.mil/	192.112.36.4	Vienna, VA, USA
H	Army Research Laboratory	http://www.arl.mil/	128.63.2.53	Aberdeen, MD, USA
I	NORDUNet	http://www.nordu.net/	192.36.148.17	Stockholm, Schweden
J	TBD		198.41.0.10	Herndon, VA, USA
K	RIPE-NCC	http://www.ripe.net/	193.0.14.129	London, Großbritannien
L	TBD		198.32.64.12	Marina Del Rey, CA, USA
M	WIDE	http://www.wide.ad.jp/	202.12.27.33	Tokio, Japan

Domain (Domäne)

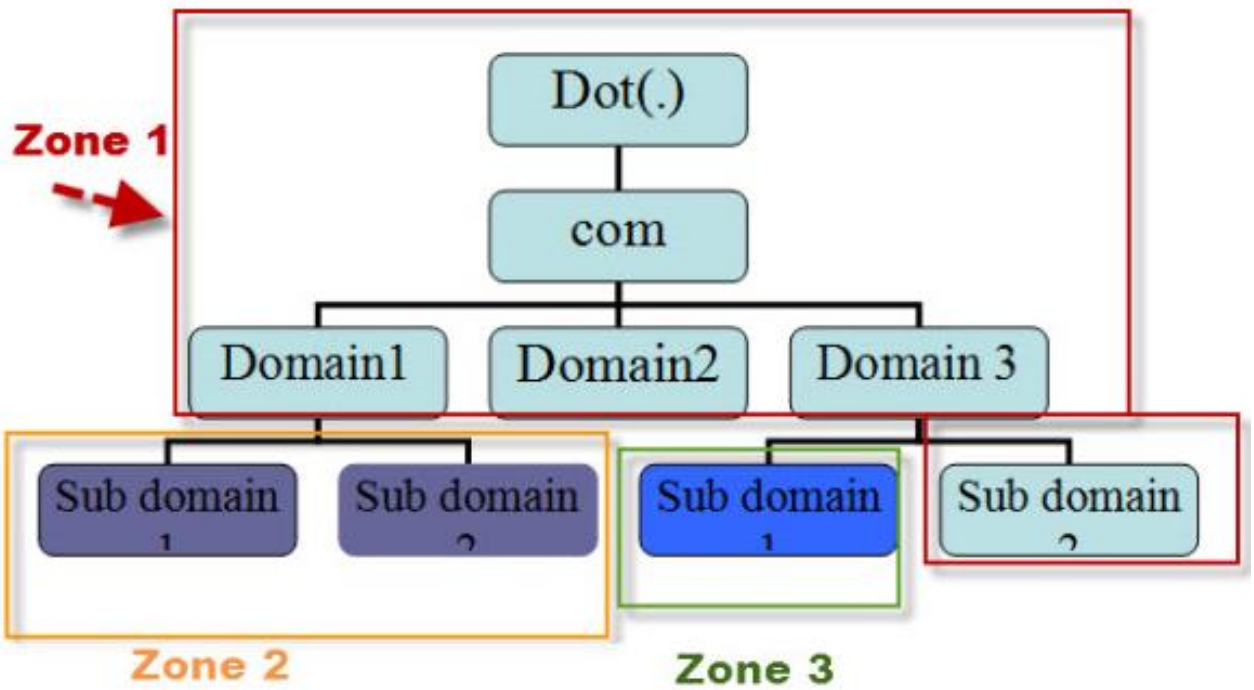
- *Jede Domain hat einen eindeutigen Namen und enthält alle untergeordneten Domänen.*

  Beispiel :

  - *t-online.de*
    - *enthält Rechner wie www.t-online.de*
    - *enthält Unterdomänen (subdomains) wie bhp.t-online.de*
    - *die wiederum Rechner (ftp.bhp.t-online.de) oder Domänen enthalten können*
  - *de enthält z.B. t-online.de*
  - **.** *(root) enthält alle darunterliegenden Domänen*
  - *vollständiger Name z.B. www.t-online.de***.**
    - *Punkt am Ende (für root-Domain)*
    - *Fully Qualified Domain Name (FQDN)*

Zone

- *Ein abgeschlossener Bereich in der Domänenstruktur, der von einem primären Nameserver selbstständig und ohne Hilfe anderer Nameserver verwaltet wird.*
- *Eine Zone umfasst meist nur eine Domäne und enthält keine anderen Zonen.*
- *Der Nameserver verwaltet eine Zone in der sogenannten **Zonendatei**, sie enthält Informationen zu einzelnen Hosts oder zu zuständigen Nameservern untergeordneter Domains.*



Beispiel einer Zonen-Datei

```
netplanet.org. IN SOA ns.eplan.net. hostmaster.eplan.net
        ( 2003053102 ; serial
          28800      ; refresh
          7200       ; retry
          604800     ; expire
          86400 )    ; minimum
        IN NS ns.eplan.net.
        IN NS ns1.eplan.net.
        IN NS ns2.eplan.net.
        IN MX 10 mailsrv1.eplan.net.
        IN MX 20 mailsrv2.eplan.net.
        IN A 80.245.65.1
www         IN A 80.245.65.1
www2        IN CNAME www.netplanet.org
```

*Die einzelnen Einträge in einer **Zonendatei** bezeichnet man als Resource Record (RR). Diese haben den Aufbau "Domain - Klasse - Typ - Eintrag":*

Die Domain enthält den Namen der Domain, für die die Zonendatei zuständig ist.
Hier lautet diese Domain "netplanet.org" und gibt somit an, dass die Zonendatei entsprechend für diese Domain zuständig ist.

Die Klasse gibt das Netz an, für das der Eintrag gelten soll. Hier steht "IN" für das Internet.
Der Typ kennzeichnet den Typ des DNS-Eintrages.

Eine Zonen-Datei beinhaltet alle notwendigen Informationen für einen DNS-Server, die dieser benötigt um einen Host-Namen in eine IP-Adresse aufzulösen.

SOA - Start of Authority

Erster Eintrag in der Zonendatei die für eine bestimmte Domain autoritativ zuständig sein soll.

NS - Nameserver

Mit dem NS-Eintrag werden die Nameserver angegeben, die für die Domain der Zonendatei autoritativ zuständig sind.

Die hier angegebenen Nameserver führen synchron die gleiche Zonendatei, wobei ein Nameserver als primärer Nameserver fungiert, der das Original der Zonendatei bereithält, der/die weiteren Nameserver als sekundäre Nameserver arbeiten, die sich die Zonendatei gemäß den Zeitfaktoren im SOA-Eintrag kopieren.

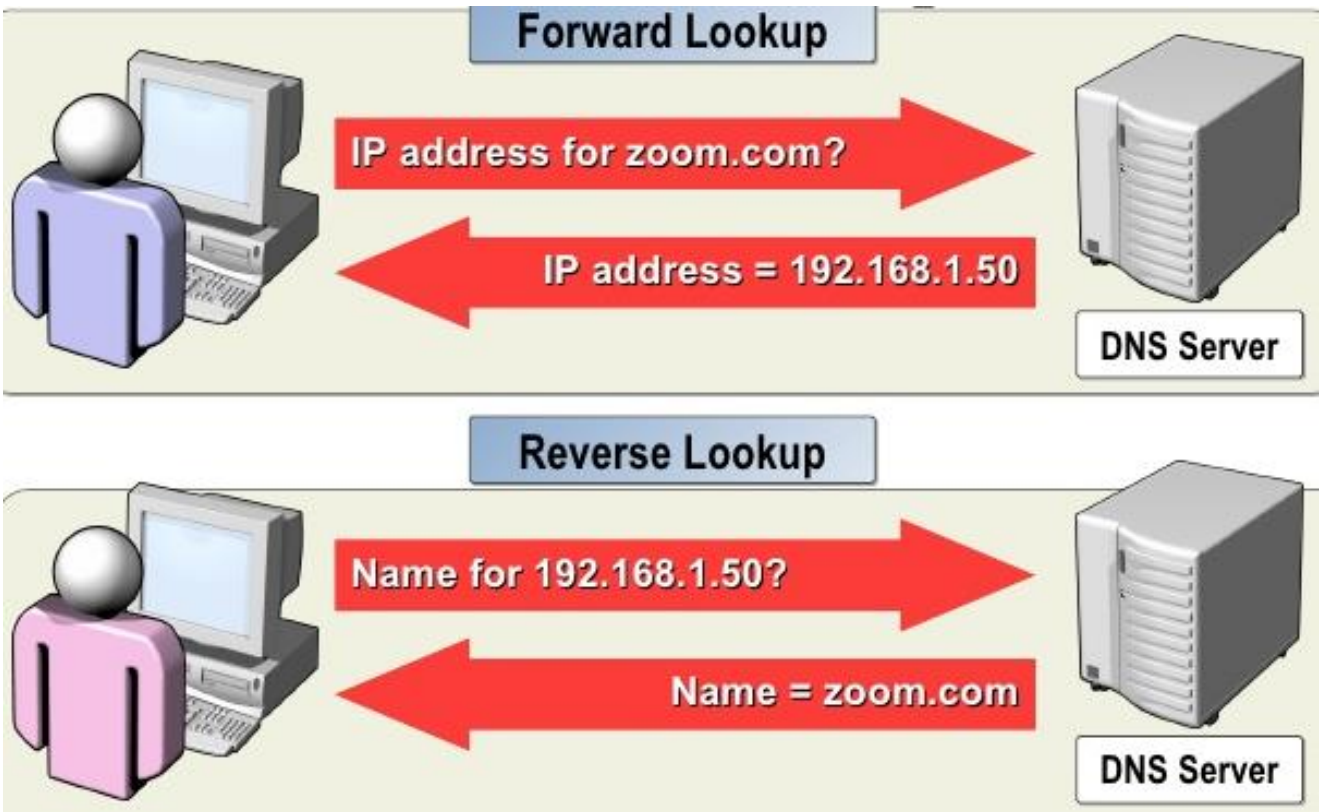
MX - Mail Exchange

Die MX-Einträge dienen zur Angabe der Mailserver, die für die Domain zuständig sein sollen.

Forward Lookup und Reverse Lookup

Forward Lookup → dient dazu Hostnamen in IP-Adressen zu wandeln.

Reverse Lookup → dient dazu IP-Adressen in Hostnamen zurück zu wandeln.

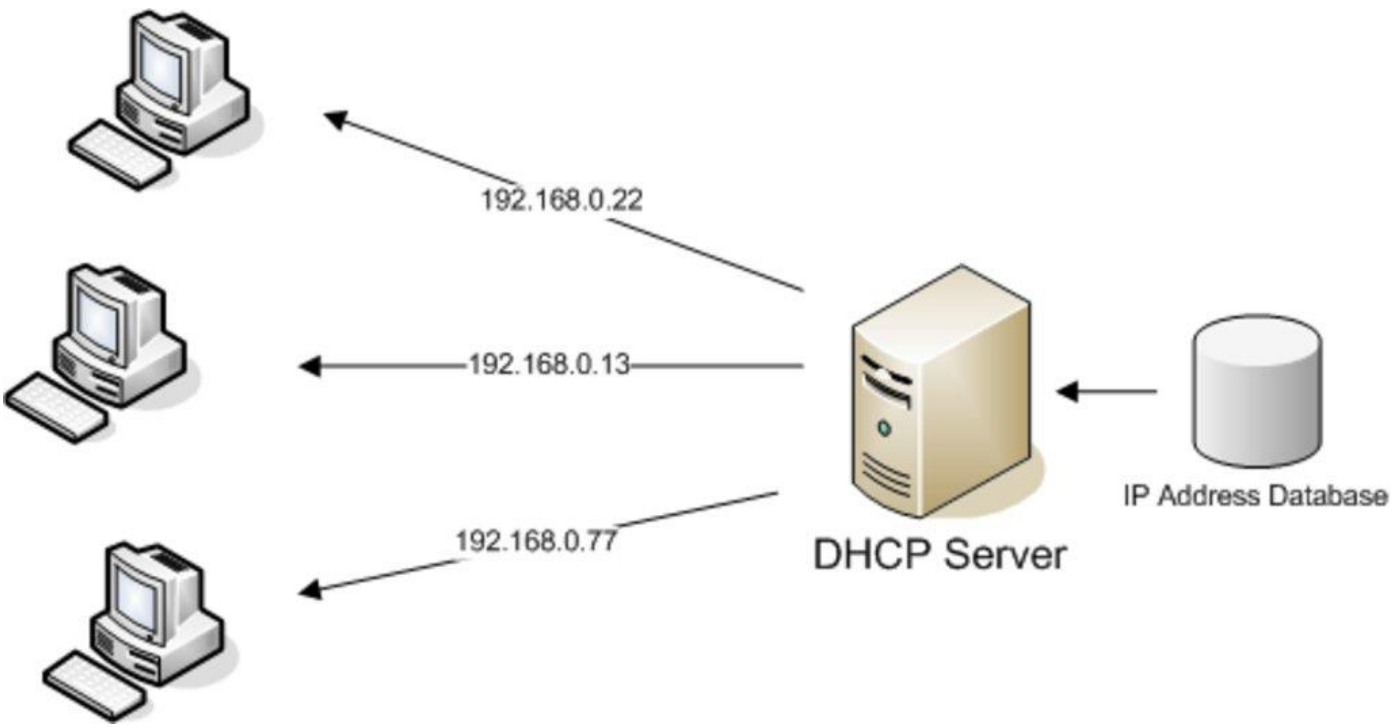


DHCP

*Das **D**ynamic **H**ost **C**onfiguration **P**rotocol ermöglicht die dynamischen Zuweisung der IP-Netzwerkeinstellungen an einen Host, der in einem Netzwerk kommunizieren will.*

Durch DHCP zu konfigurierende Parameter :

- *Zuweisung einer IP Adresse mit einer einstellbaren „Lebensdauer“ (-> LEASE)*
- *Zuweisung von Gateway und DNS Adressen*
- *IP-Maske (Subnetting)*
- *Zurückweisen von nicht zulässigen MAC – Adressen*



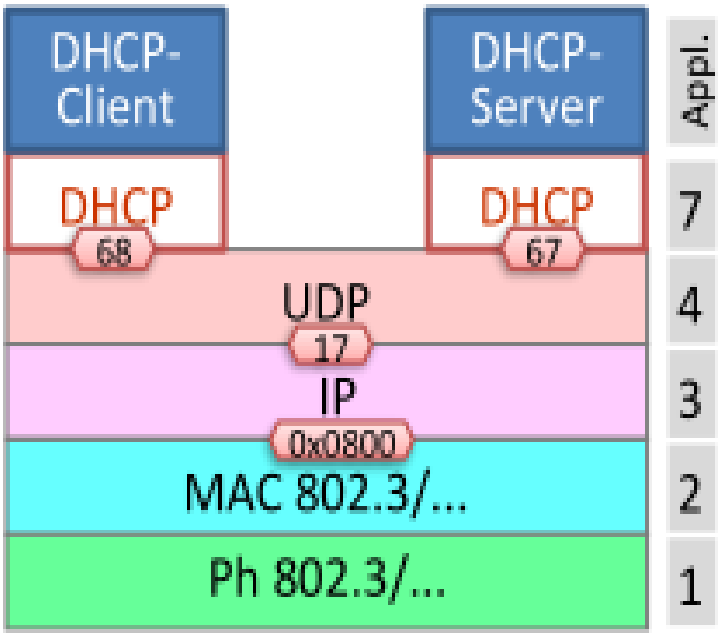
Funktionsweise von DHCP

Die Funktionsweise von DHCP entspricht dem Client-Server-Prinzip.
DHCP-Server sind Bestandteil der Microsoft Server-Software oder von Linux-Distributionen.

DHCP unterstützt die Zuweisung von BOOTP-Parametern, wie z.B. Boot-Images.

Die dynamische Hostkonfiguration erfolgt über die UDP-Ports 67 und 68.

BOOTP
(bootstrap protocol)
→ (älteres) Client-Server-Protokoll, das der Vergabe von IP-Adressen dient und auf dem UDP-Protokoll aufsetzt.



Damit der Client einen DHCP-Server nutzen kann, muss sich dieser im selben Netzwerksegment befinden, da DHCP Broadcasts verwendet und Router keine Broadcasts weiterleiten (Router bilden Broadcast-Domänen).

Befindet sich der DHCP-Server in einem anderen Netzwerksegment, so muss ein so genannter DHCP-Relay-Agent installiert werden, der die DHCP-Anfragen an den eigentlichen Server weitergibt.

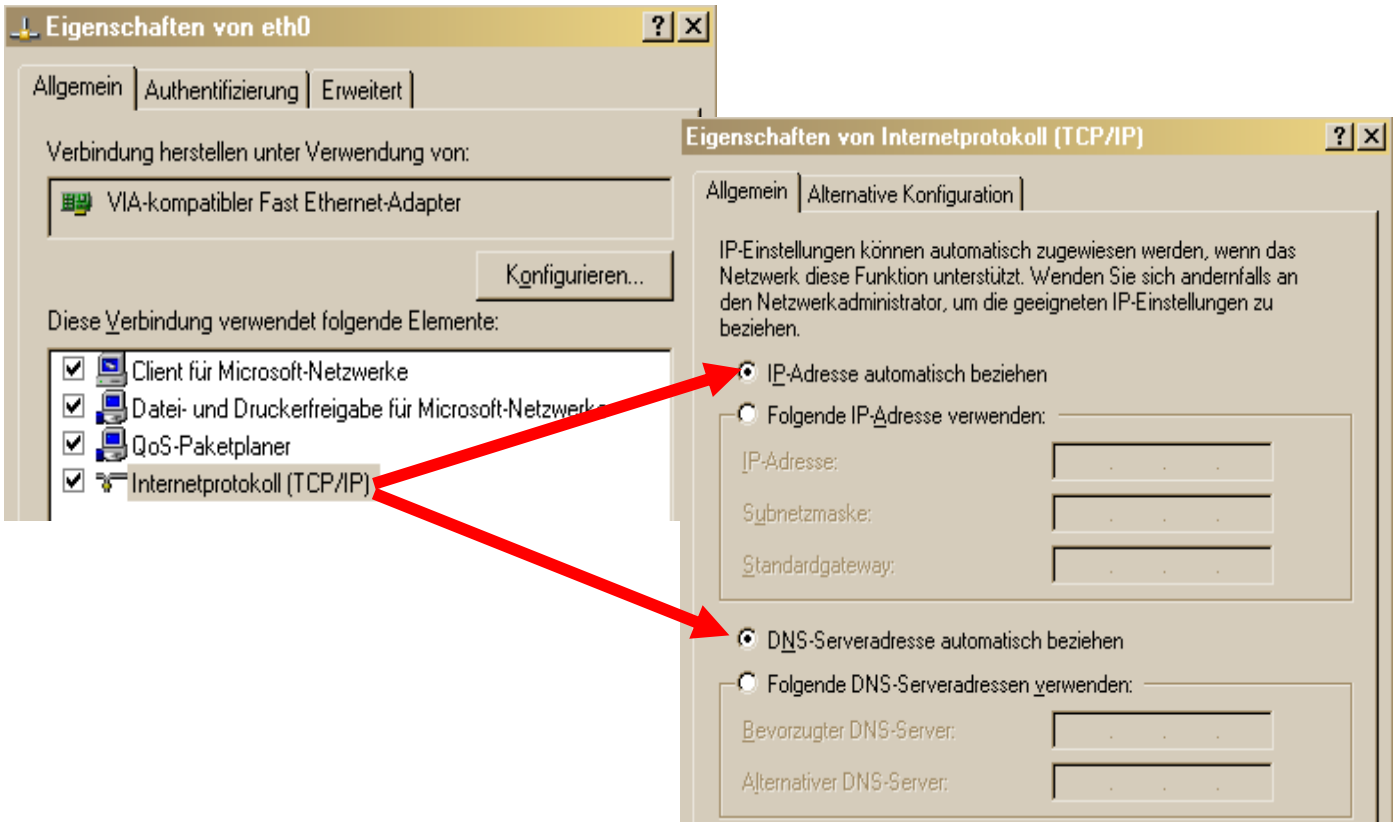
DHCP-Relay ist eine Funktion, um DHCP über Netzgrenzen (Broadcastdomäne) hinaus nutzen zu können. Damit wird die Notwendigkeit der Bereitstellung eines DHCP-Servers in jedem Subnetz, in dem sich DHCP-Clients befinden, vermieden. Die DHCP-Relay-Funktion wird meist durch den Router selbst erbracht.

Ablauf einer DHCP-Anfrage

1. Booten eines hosts

Booten eines Hosts….

Wenn in den Netzwerkeinstellungen DHCP eingestellt ist starten die nun folgenden Aktionen ..



Wird ein Host mit einem aktivierten DHCP-Client gestartet, wird ein funktional eingeschränkter Modus des TCP/IP-Stacks gefahren.
Dieser hat *keine* gültige IP-Adresse, *keine* Subnetzmaske und *kein* Standard-Gateway.
Das einzige, was der Client machen kann, ist IP-Broadcasts verschicken.

1. *Booten eines hosts*
2. *Anfrage an ein Netzwerk*

DHCP-Discover

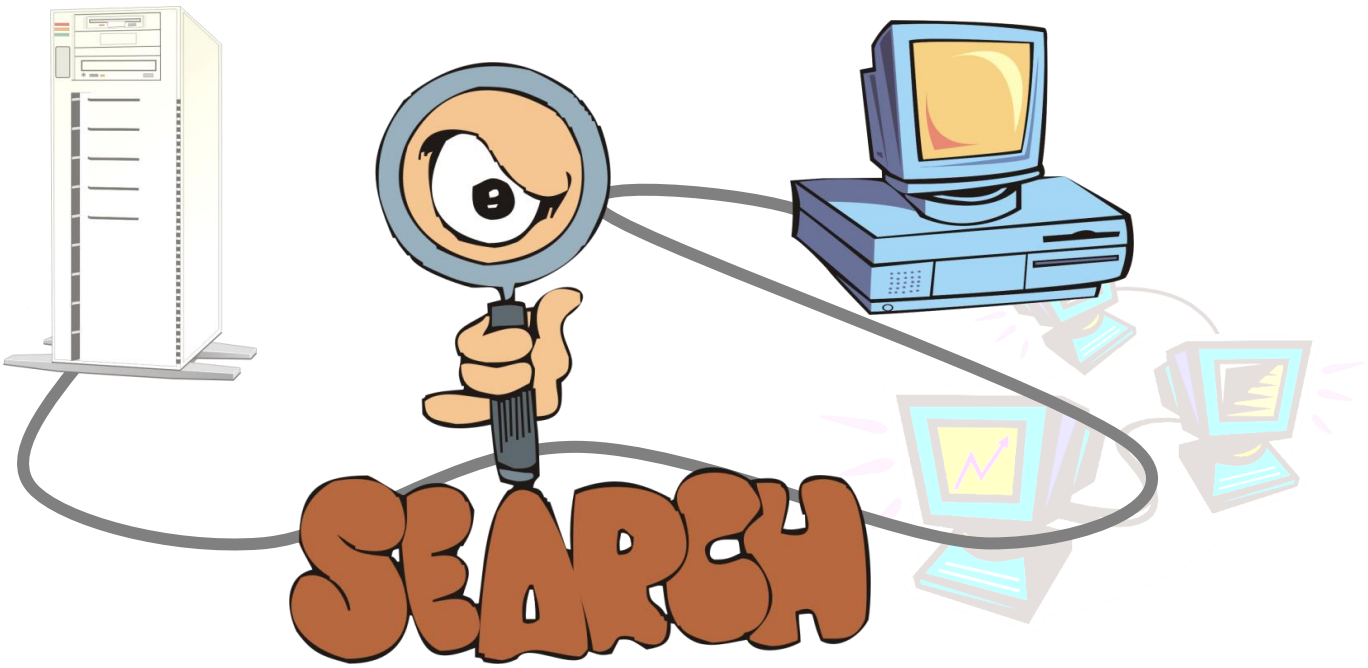
Anfrage eines Hosts in einem Netzwerk

An alle (-> Broadcast)…255.255.255.255

Wenn du ein DHCP Server bist, dann antworte mir,

meine MAC Adresse ist 00-90-4B-0E-FA-EA

(Absender-IP : 0.0.0.0)



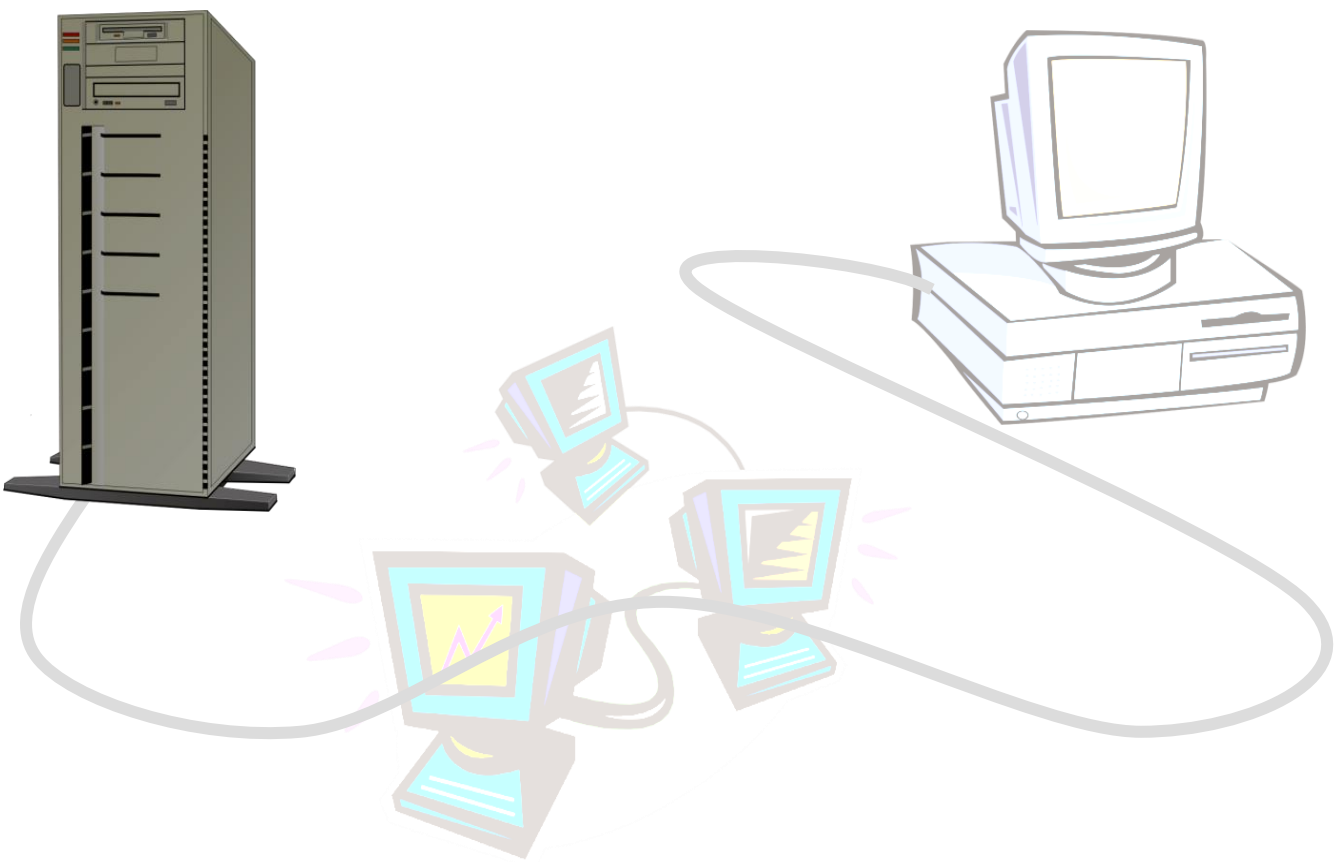
1. *Booten eines hosts*
2. *Anfrage an ein Netzwerk*
3. *DHCP Server gefunden*

DHCP-Offer

DHCP Server gefunden…

Ich bin ein DHCP Server

Lass mich überlegen….



1. ***Booten eines hosts***
2. ***Anfrage an ein Netzwerk***
3. ***DHCP Server gefunden***
4. ***DHCP Dienstprogramm entscheidet***

DHCP Dienstprogramm wird aktiv

Die Einstellungen meines Administrators werden folgendermaßen abgearbeitet :

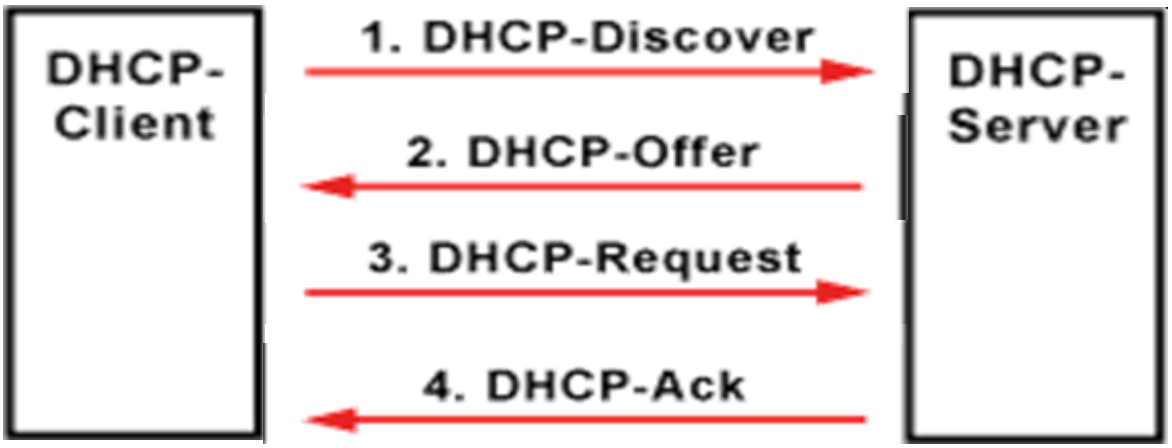
1. Ist deine MAC Adresse (z.B. 00-90-4B-0E-FA-EA) zulässig ?

2. Wenn du innerhalb des zugewiesenen Zeitrahmens (LEASE) bereits eine IP Adresse (z.B. 172.22.1.157) erhalten hast, dann bekommst du dieselbe Adresse.

3. Sonst bekommst du die nächste noch freie Adresse 172.22.1.120 aus dem Adressraum (POOL), den mir mein Admin zu Verteilung zugewiesen hat.

DHCP-Request

Aus der Auswahl von eventuell mehreren DHCP-Servern sucht sich der DHCP-Client eine IP-Adresse heraus. Daraufhin verschickt er eine positive Meldung an den betreffenden DHCP-Server. Alle anderen DHCP-Server erhalten die Meldung ebenso und gehen von der Annahme der IP-Adresse zugunsten eines anderen DHCP-Servers aus.



DHCP-Acknowledgement

Anschließend muss die Vergabe der IP-Adresse vom DHCP-Server bestätigt werden. Doch nicht nur die Daten zum TCP/IP-Netzwerk kann DHCP an den Client vergeben. Sofern der DHCP-Client weitere Angaben auswerten kann, übermittelt der DHCP-Server weitere Optionen:

- Time Server
- Name Server
- Domain Name Server (Alternative)
- WINS-Server
- Domain Name
- Default IP TTL
- Broadcast Address
- SMTP Server
- POP3 Server

Sobald der DHCP-Client die Bestätigung erhalten hat, speichert er die Daten lokal ab. Abschließend wird der TCP/IP-Stack vollständig gestartet.

1. *Booten eines hosts*
2. *Anfrage an ein Netzwerk*
3. *DHCP Server gefunden*
4. *DHCP Dienstprogramm entscheidet*
5. *DHCP-Server sendet*

DHCP Dienstprogramm sendet zum Beispiel an Host :

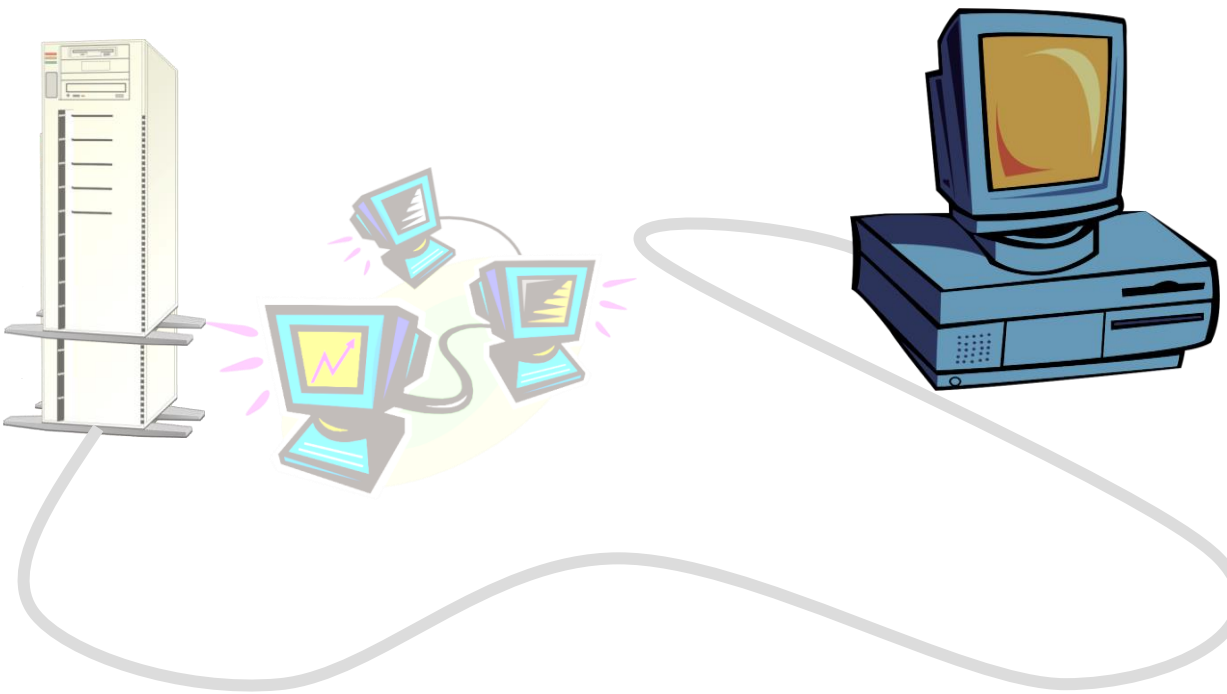
Meine Antwort an 00-90-4B-0E-FA-EA:

Deine IP Einstellungen sind:

IP	*172.22.1.157*
Subnetmaske	*255.255.0.0*
Gateway	*172.22.1.250*
DNS1	*172.22.10.10*
DNS2	*193.170.239.3*
DNS3	*193.171.4.60*

1. ***Booten eines hosts***
2. ***Anfrage an ein Netzwerk***
3. ***DHCP Server gefunden***
4. ***DHCP Dienstprogramm entscheidet***
5. ***DHCP-Server sendet***
6. ***Host empfängt die Daten***

Der Host empfängt die Daten und kann nun in diesem Netzwerk und allen daran angeschlossenen Netzwerken kommunizieren.



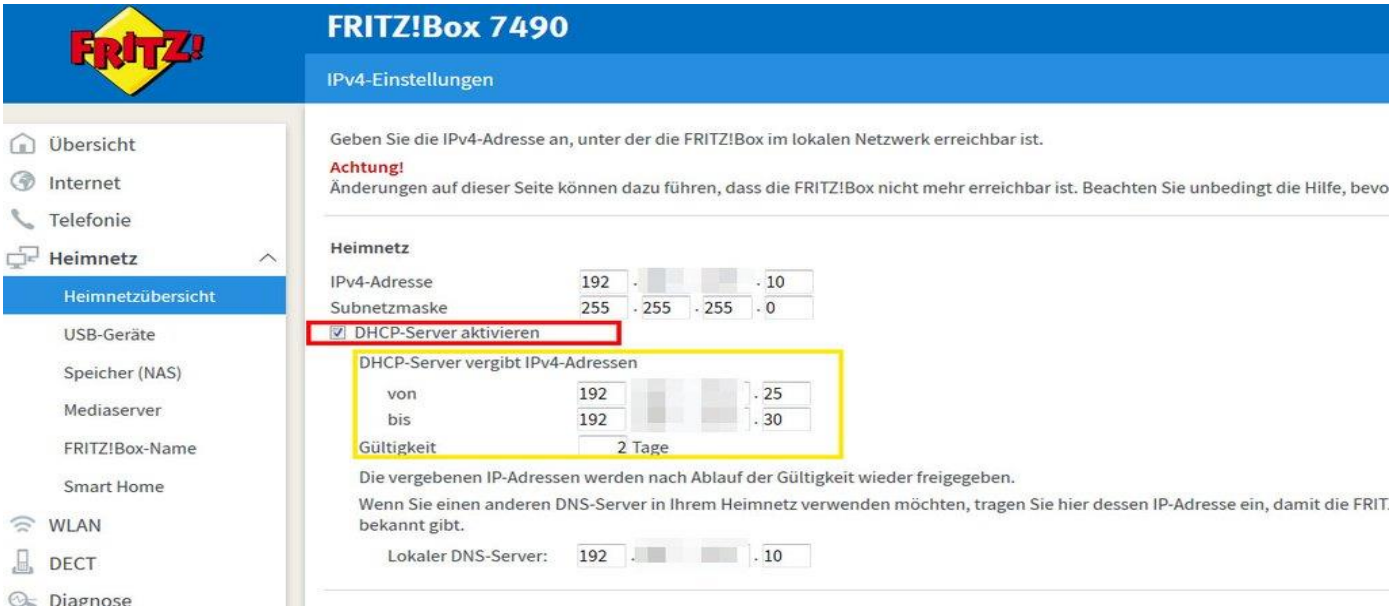
Sobald der DHCP-Client die Bestätigung erhalten hat, speichert er die Daten lokal ab. Abschließend wird der TCP/IP-Stack vollständig gestartet.

Die drei verschiedenen Betriebsmodi eines DHCP-Servers:

- Manuell : -> statisches DHCP -> am DHCP-Server werden die IP-Adressen bestimmten MAC-Adressen fest zugeordnet.

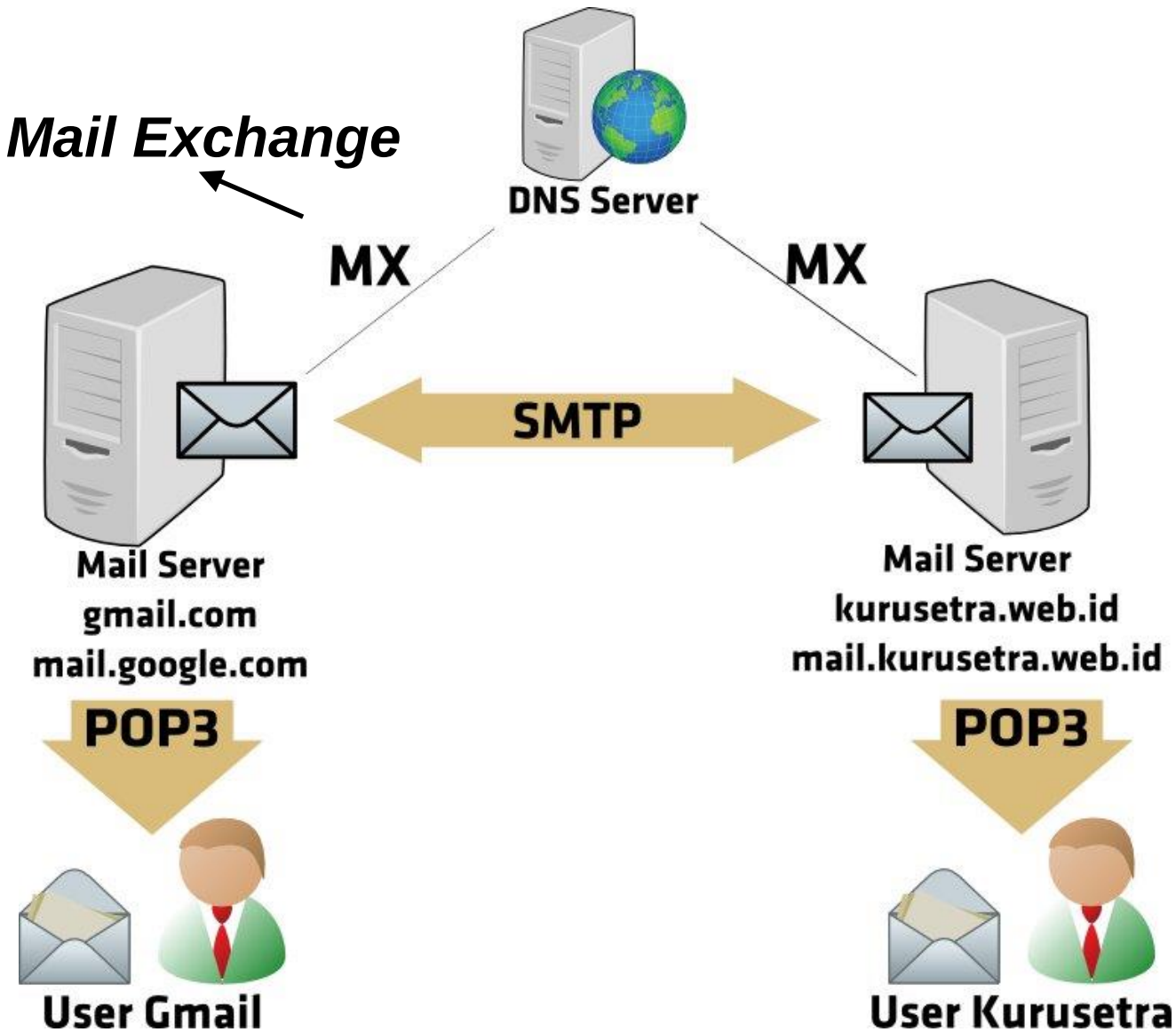
- Automatisch : am DHCP-Server wird ein Bereich von IP-Adressen (range) definiert. IP-Adressen werden automatisch an die MAC-Adressen von neuen DHCP-Clients zugewiesen, was in einer Tabelle festgehalten wird.

- Dynamisch : dieses Verfahren gleicht der automatischen Zuordnung, allerdings hat der DHCP-Server hier in seiner Konfigurationsdatei eine Angabe, wie lange eine bestimmte IP-Adresse an einen Client „verliehen“ werden darf -> Lease



(E)-Mail-Server

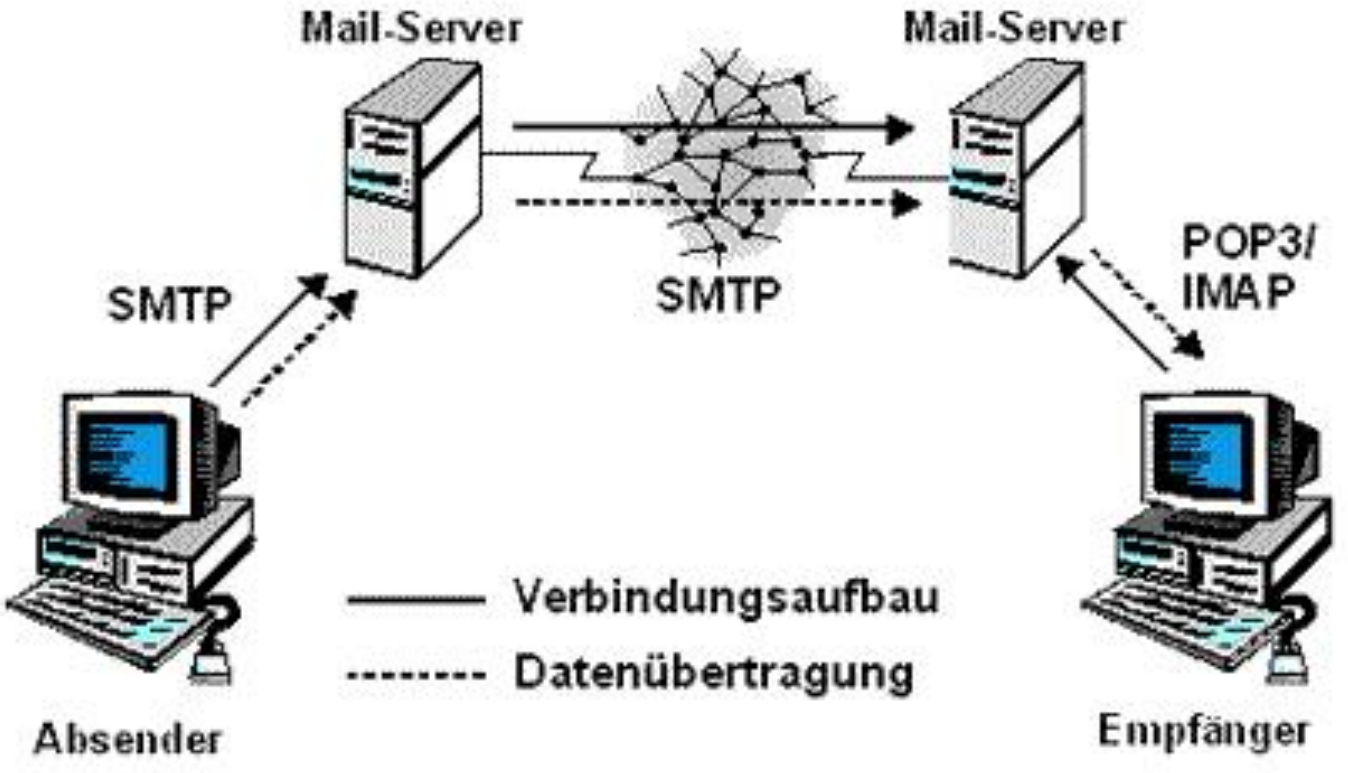
Software auf einem Server, der Nachrichten und Mitteilungen empfangen, senden, zwischenspeichern und weiterleiten kann.



Arbeitsweise eines Mail-Servers

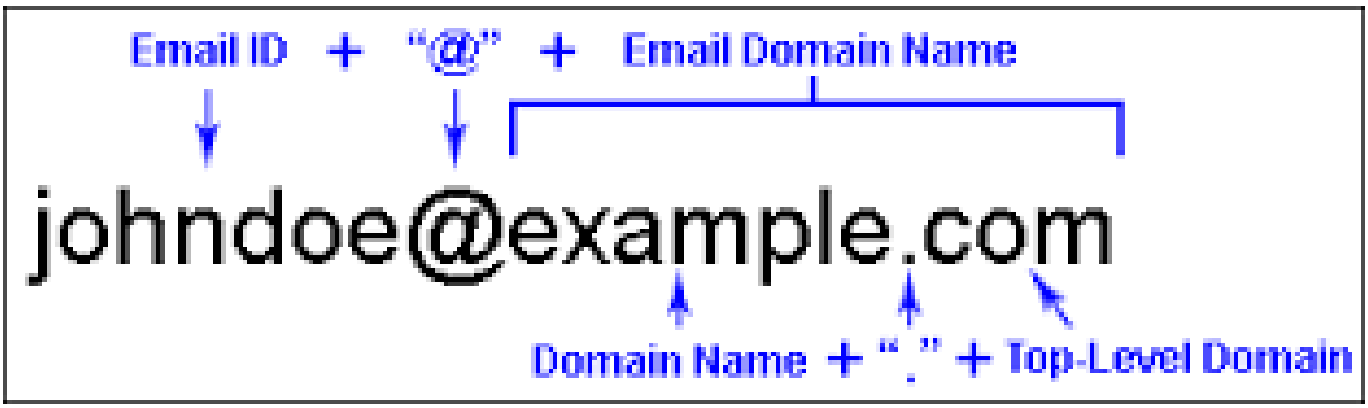
- *E-Mails können von E-Mail-Clients abgerufen und bearbeitet werden.*

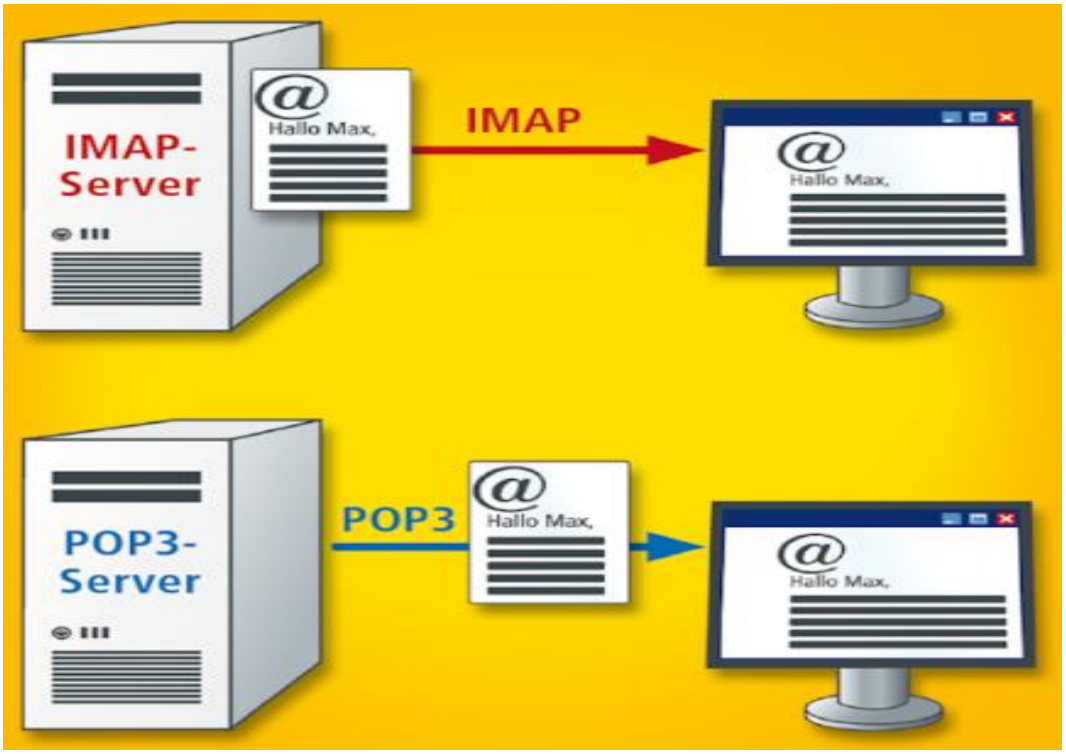
- *Mail-Server fungieren als Mail Transfer Agents (MTA), die die gespeicherten Nachrichten mit dem Simple Mail Transfer Protocol (SMTP) zum nächsten Mail-Server weiterleiten, bis hin zu dem Mail-Server in den sich der empfangende Benutzer mit seiner E-Mail-Adresse eingeloggt hat.*



Benutzer können über ihren E-Mail-Account mit der E-Mail-Adresse auf E-Mail-Server zugreifen.

Die Mail-Adresse beinhaltet die Hostadresse, häufig die eines Providers, und die Länderkennzeichnung, die Top Level Domain (TLD).



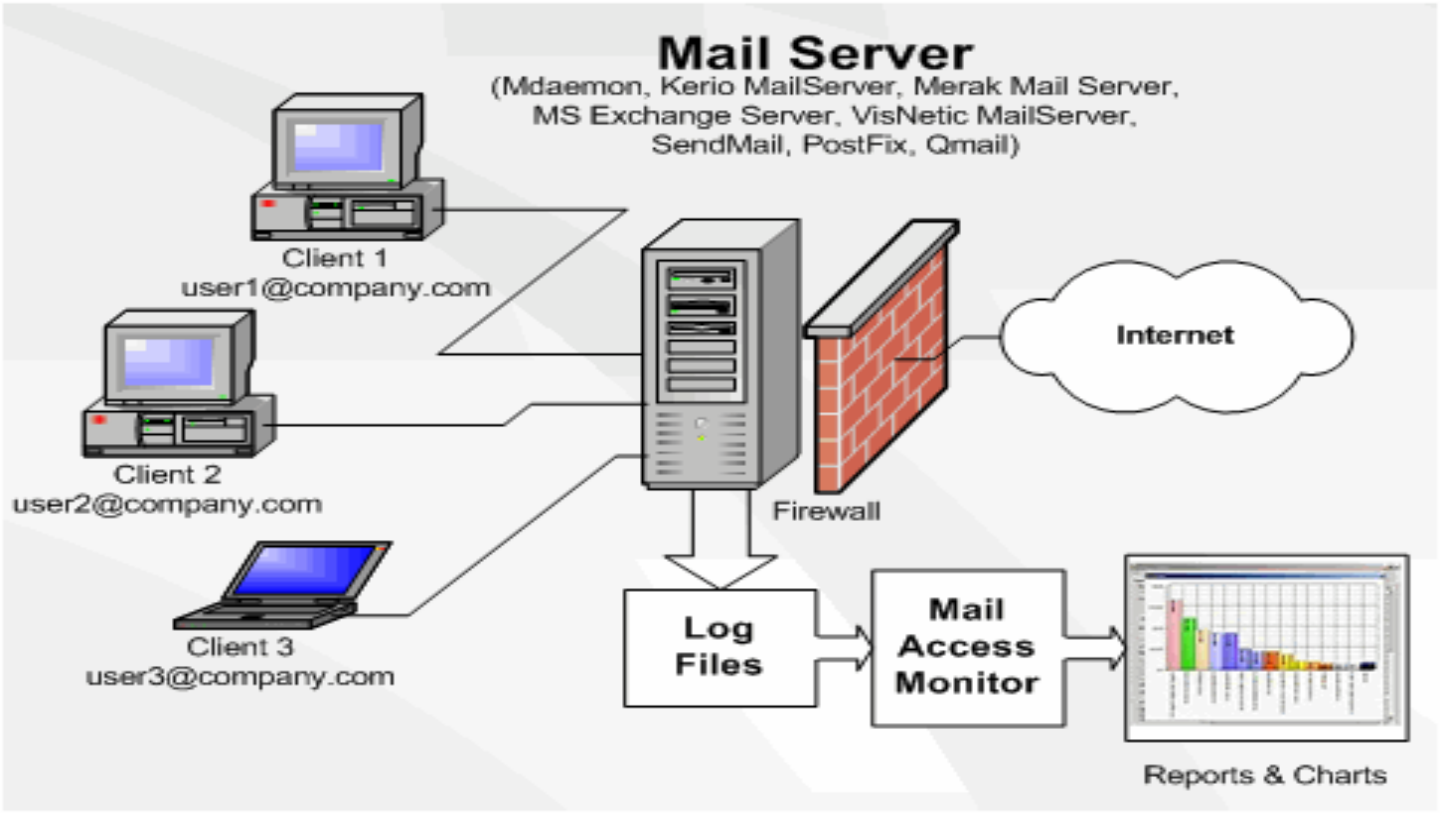


Die von einem E-Mail-Client an einen E-Mail-Server gesendeten E-Mails werden solange zwischengespeichert bis sie vom Empfänger abgeholt werden.

Dies erfolgt mit dem Post Office Protocol (**POP**)
-> erlaubt nur das Auflisten, Abholen und Löschen von E-Mails am E-Mail-Server.

oder dem

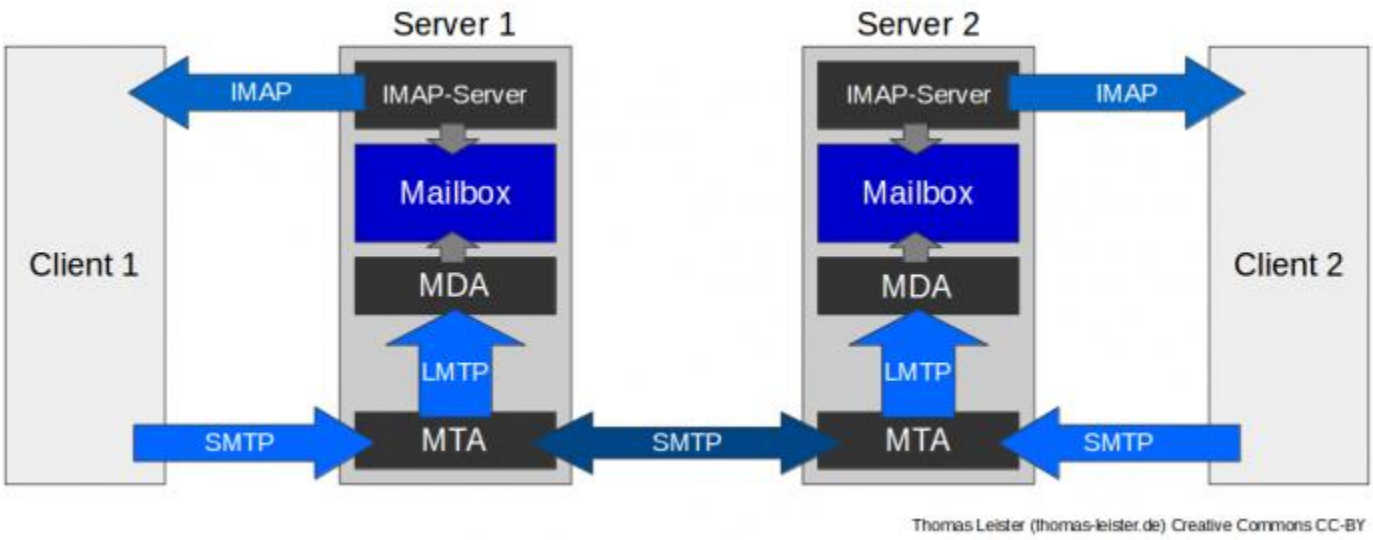
Internet Message Access Protocol (**IMAP**).
-> stellt ein Netzwerkdateisystem für E-Mails bereit, d.h. E-Mails werden direkt auf dem E-Mail Server verwaltet.



Authentifizierung der Benutzer :
Mail-Server haben eigene Datenbanken mit den Zugriffsdaten.
(Zugriff auf Internet-Verzeichnisdienste -> Open Database Connectivity (ODBC), Lightweight Directory Access Protocol (LDAP); Authentifikation -> Active Directory (AD-> Microsoft) und Secure Socket Layer (SSL)).

***E-Mail-Sicherheit** :*
Schutz vor Viren, Spams und Hackern.
Mail-Server haben Spam-Filter mit denen sie Spams kenntlich machen und Virenscanner mit denen sie virenbelastete Mails sperren.

Mailserver-Module



Bei den meisten Mailservern arbeiten mehrere Module zusammen:

- *der Mail Transfer Agent nimmt E-Mails an und leitet sie weiter.*
- *Mail Retrieval Agents rufen E-Mails von anderen Servern ab.*
- *Mailfilter blockieren Spam und Schadprogramme.*
- *der Mail Delivery Agent sortiert E-Mails in E-Mail-Postfächer ein.*
- *der Message Store gewährt Zugriff auf die Postfächer.*

Local Mail Transfer Proto

Pakete und Zellen

- Aufteilung der Bandbreite in LANs durch Übertragung der Daten in kleinen Blöcken.

Varianten

– Blöcke variabler Länge: Pakete (Frames)

- an Bedarf anpassbar.
- meist große Maximallänge (>1000 Byte).
- überwiegend in LANs verwendet.

– Blöcke konstanter Länge: Zellen (Cells)

- bessere Eignung bei Anforderung nach konstanten Datenraten.
- meist kleine Längen (50-100 Byte).
- mehr in WANs üblich.