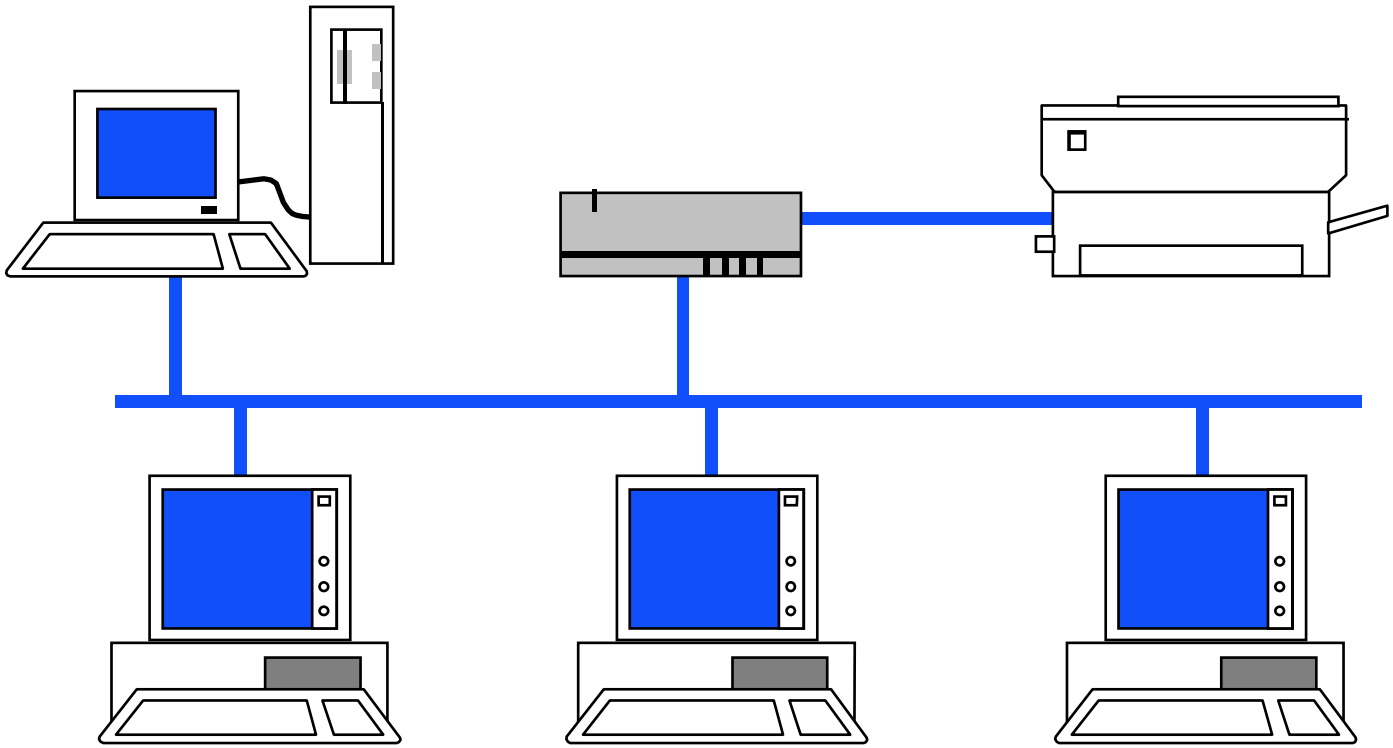
NVS1 B 5+6. Semester

Mag. Dr. Klaus Coufal



Übersicht

- Kompetenzbereiche
  - Netzwerkmanagement und -sicherheit
  - Netztechnologien
  - Netzdienste

I. Netzwerkmanagement und -sicherheit

- Netzwerkmodelle
- Entwurfsmethoden

II. Netztechnologien

- Protokolle
- Private Servernetze
- Switching und Routing
- Öffentliche Netze

III. Netzdienste

- DNS, DHCP, Web
- Verzeichnisdienste

I.1. Referenzmodelle

- ISO-Referenzmodell OSI
- TCP/IP-Referenzmodell
- Novell-Referenzmodell
- ...

ISO-Referenzmodell

Anwendung	
7	**Application Layer (Anwendungsschicht)**
6	**Presentation Layer (Präsentationsschicht)**
5	**Session Layer (Sitzungsschicht)**
4	**Transport Layer (Transportschicht)**
3	**Network Layer (Netzwerkschicht)**
2	**Data Link Layer (Datensicherungsschicht)**
1	**Physical Layer (Physikalische Schicht)**
Übertragungsmedium (Kabel, Funk, LWL, ...)	

Physical layer

- ISO Schicht 1
- Kabel- und Steckerspezifikationen
- Übertragungstechnologie
- Spezifikation der Signalpegel
- Unstrukturierter Bitstrom
- z.B.: X.21, V.24, Ethernet Hardwareteil
- Geräte: Repeater, Hub

Data Link layer

- ISO Schicht 2
- HW-Adressierung, Frameformat
- Flusskontrolle und Fehlerprüfung zwischen nächsten Nachbarn
- Rahmen (Frames)
- z.B.: HDLC, Ethernet MAC und LLC
- Geräte: Bridge, Switch

Network layer

- ISO Schicht 3
- Logische Adressierung
- Wegewahl und Routing
- Auf- und Abbau von Netzverbindungen
- Pakete (Packets)
- z.B.: X.25, IP, IPX
- Geräte: Router

Transport layer

- ISO Schicht 4
- Ende zu Ende Flußkontrolle
- Ende zu Ende Fehlerprüfung
- Sequencing
- Fragmente, Pakete (Packets)
- z.B.: TCP, SPX
- Geräte: Gateway

Session layer

- ISO Schicht 5
- Passwortkontrolle
- Gebührenabrechnung
- Auf- und Abbau einer Sitzung
- Verbindungswiederaufbau
- Kaum Standards
- Geräte: Access Controller

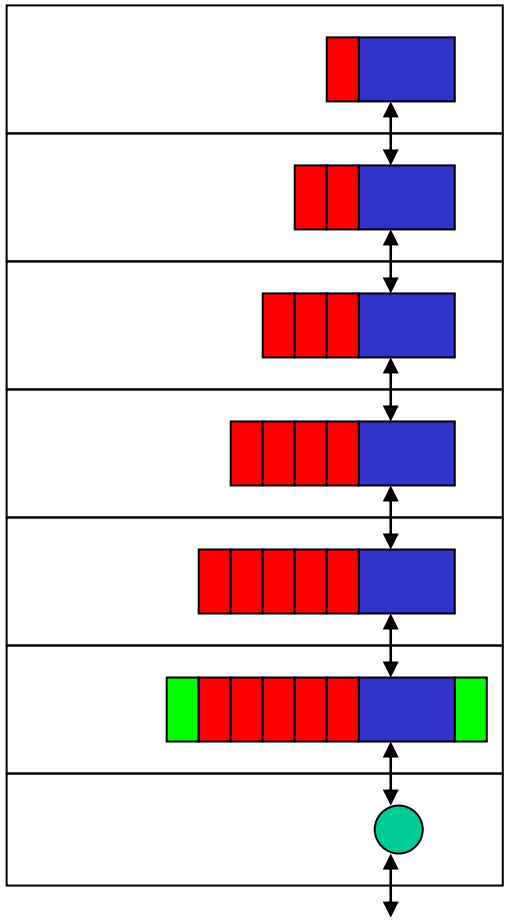
Presentation layer

- ISO Schicht 6
- Vereinbarung über Kodierung (Zahlendarstellung, Dateiformate, ...)
- Formatumwandlung
- Codeumwandlung
- z.B.: ASCII $\leftrightarrow$ EBCDIC

Application layer

- ISO Schicht 7
- APIs (Application Programming Interface) für die Anwendungen
- Standarddienste (Dateitransfer, Virtuelles Terminal, ...)
- z.B.: Sockets, FTAM, X.400, X.500

Schichtenkommunikation



Applikationsschicht

Präsentationsschicht

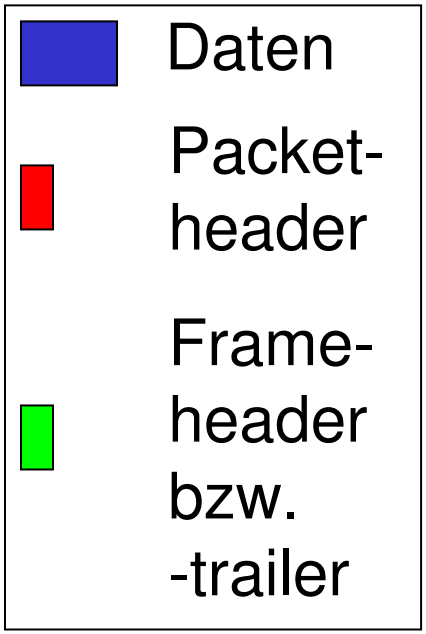
Sitzungsschicht

Transportschicht

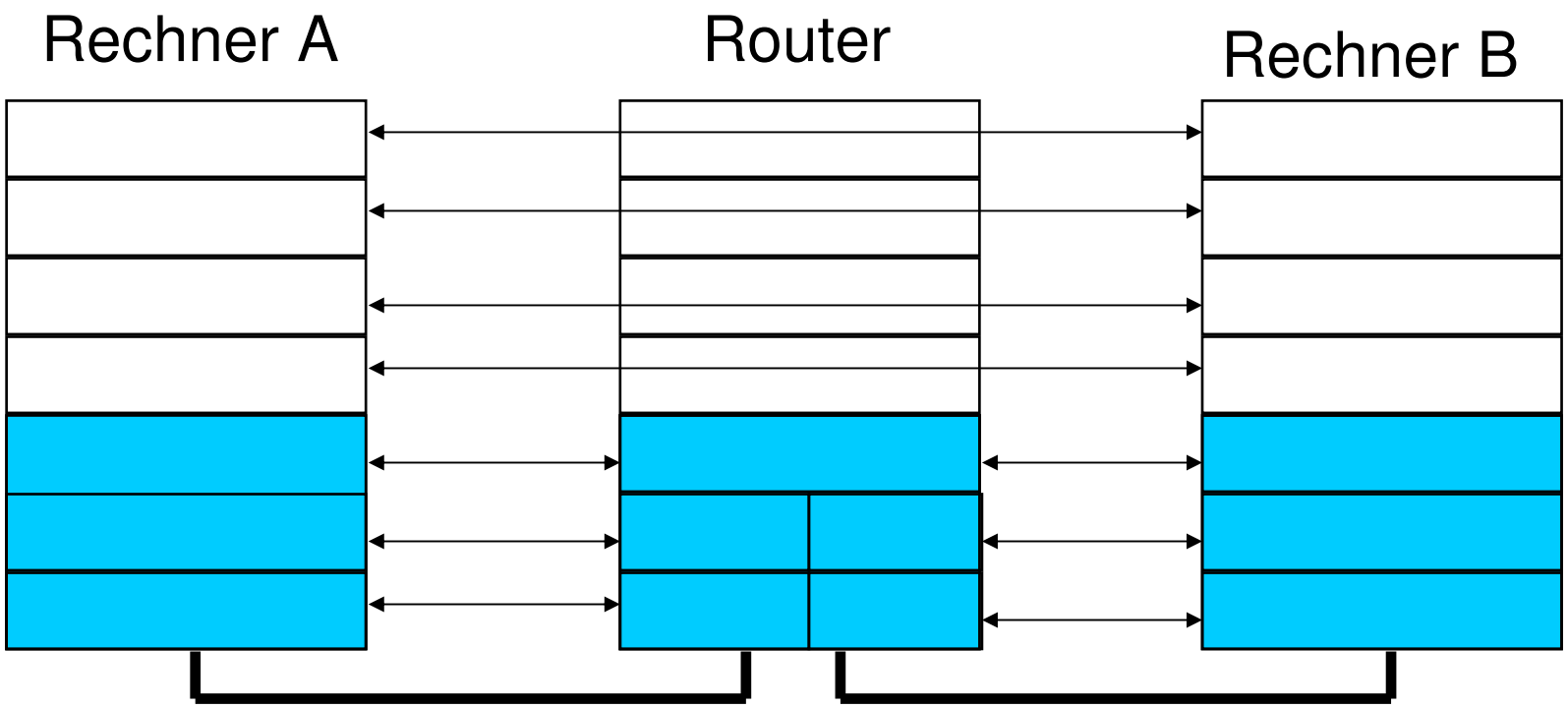
Netzwerkschicht

Datenverbindungsschicht

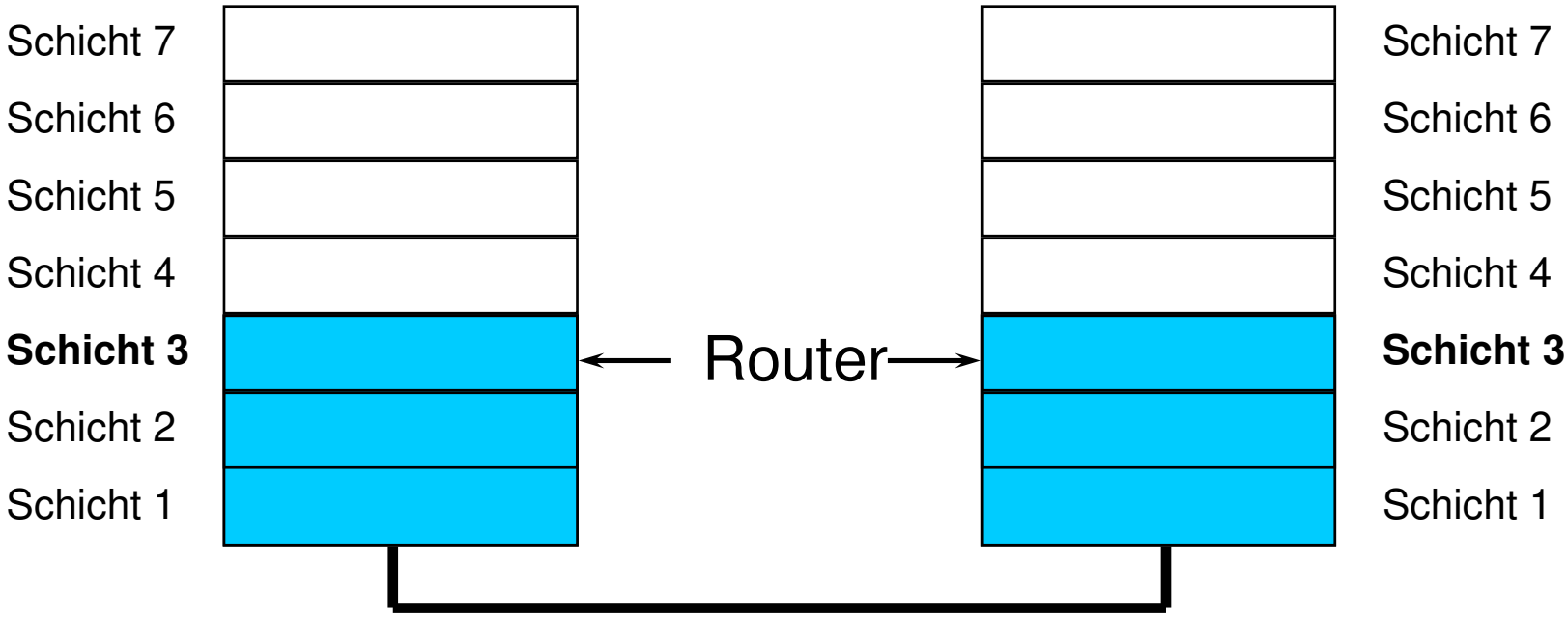
Physikalische Schicht



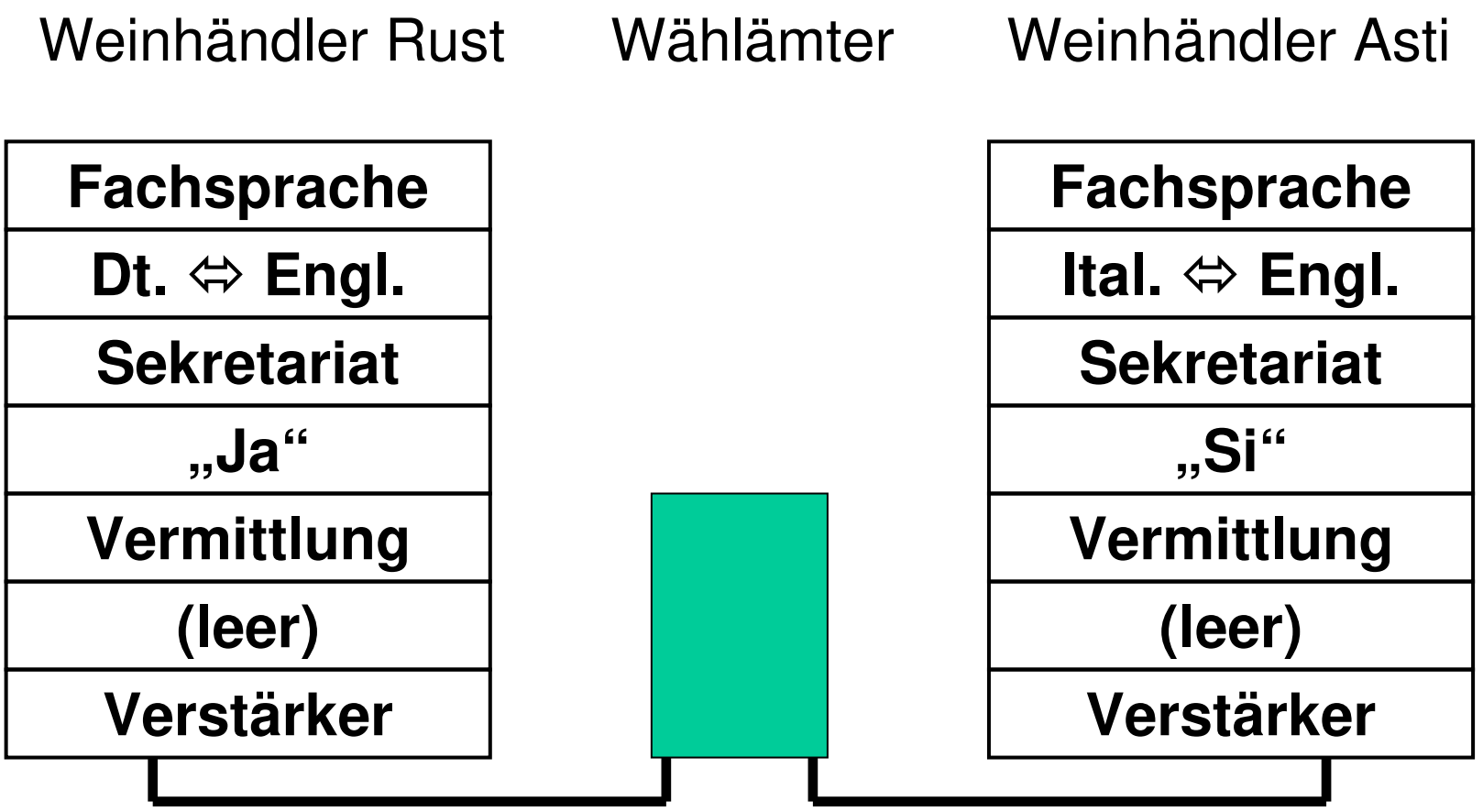
Kommunikation über Router



Schichtenmodell am Beispiel Router



Beispiel


Weinhändler Rust
Wählämter
Weinhändler Asti
Fachsprache
Dt. ⇔ Engl.
Sekretariat
„Ja“
Vermittlung
(leer)
Verstärker
Fachsprache
Ital. ⇔ Engl.
Sekretariat
„Si“
Vermittlung
(leer)
Verstärker

TCP/IP-Referenzmodell

OSI		Anwendung	TCP/IP
7	Application Layer	4	Application
6	Presentation Layer		
5	Session Layer		
4	Transport Layer	3	Transport
3	Network Layer	2	Internet
2	Data Link Layer	1	Host to Net
1	Physical Layer		

Übertragungsmedium (Kabel, Funk, LWL, ...)

Novell-Referenzmodell

OSI	Anwendung	Novell	
7	Application Layer	5	Application Layer
6	Presentation Layer		
5	Session Layer		
4	Transport Layer	4	Transport Layer
3	Network Layer	3	Network Layer
2	Data Link Layer	2	Data Link Layer
1	Physical Layer	1	Physical Layer
Übertragungsmedium (Kabel, Funk, LWL, ...)			

I.2. Entwurfsmethoden

- Warum?
- Arten des Entwurfs
  - Top-Down-Entwurf
  - Bottom-Up-Entwurf
- Schritte eines Entwurfs

Warum ?

- Nur mittels eines Planes kann eine effiziente Fehlervermeidung bzw. Fehlersuche durchgeführt werden
- Nur ein gut geplantes Netzwerk bietet die Möglichkeit auf Veränderungen zu reagieren.
- Vermeidung von chaotischen Systemen.

Top-Down-Entwurf

- Von der höchsten Stufe beginnend
- z.B.: Internetzugang oder Server
- Auch die gewünschte Topologie kann der Ausgangspunkt sein
- …
- Als letzter Punkt wird der Arbeitsplatz geplant

Bottom-Up-Entwurf

- Bedarfsorientiert von Anwender ausgehend
- Verbindungen zwischen den Arbeitsplätzen
- …
- Am Ende stehen dabei die zentralen Komponenten

Methodenwahl

- Heute werden die Methoden meist kombiniert oder abwechselnd in einer Planung verwendet
- Begonnen wird üblicherweise mit der Anwendung, da dies die einzige Konstante am Anfang ist.

Schritte eines Entwurfs

- Übersicht über die Planungschritte
- Erhebung des Istzustandes
- Erhebung des Sollzustandes
- Allgemeines
- Planung der einzelnen Komponenten
- Gesamtkonzept
- Phasenplan

Übersicht – Planungsschritte

- Erhebung des Istzustandes
- Erhebung des Sollzustandes
- <solange die Planung unvollständig>
  - Planung der Arbeitsstationen
  - Planung der Drucker
  - Planung der Netzwerkhardware
  - Planung der Verkabelung
  - Planung des Netzwerkbetriebssystems
  - Planung der Server
  - Planung der Netzwerkkomponenten
  - Planung der Umgebungsbedingungen
  - Erstellen eines Gesamtkonzeptes
- Erstellen eines Phasenplans zur Umsetzung

Erhebung des Istzustandes

Die Erhebung des Istzustandes ist die einfachste Aufgabe, da hier nur festgestellt werden muß, was an einzubindenden Komponenten existiert. In diesem Unterpunkt muß eine Auflistung der vorhandenen Hardware und deren Standorte, der „Firmen“struktur, der Organisationsabläufe, der Kommunikationsströme und „alle“ Mängel in diesem System erfolgen.

Erhebung des Sollzustandes

Die wesentlich komplexere Aufgabe der Erhebung des Sollzustandes muß auch auf eventuelle Erweiterungen vorbereitet sein. Hier muß erhoben werden welche Aufgaben das Netzwerk übernehmen soll, wie eventuell Strukturen in der Organisation geändert, welche Mängel beseitigt und welche neue Aufgaben hinzugefügt werden sollen. Daraus ist eine Liste der notwendigen Arbeitsplätze zu erstellen und das Kommunikationsaufkommen abzuschätzen.

Allgemeines

Die weiteren Punkte sind mehr oder weniger von einander abhängig daher, sollten diese Punkte mehrmals (mindestens zweimal) durchlaufen werden, wobei grob begonnen werden kann und erst beim letzten Durchlauf alle Details festgelegt werden.

Planung der Arbeitsstationen

In dieser Phase müssen die einzelnen Arbeitsplätze nach verwendeten Typ, der benötigten Hardware, des Betriebssystems und der notwendigen Anwendungssoftware detailliert spezifiziert werden. Ein Standortplan (Gebäudeplan) ist in dieser Phase schon sehr hilfreich.

Planung der Drucker

Für jeden Arbeitsplatz müssen die Druckmöglichkeiten geplant werden (lokal, zentral, ...)

Planung der Netzwerkhardware

In dieser Phase muß die Entscheidung getroffen werden, welche Hardware für die Vernetzung Verwendung finden muß (Ethernet, Token-Ring, ARCnet, ...). Die Planung der verwendeten Varianten und die Netzwerkkarten fällt ebenfalls in diesen Punkt.

Planung der Verkabelung

Spätestens bei diesem Punkt ist ein detaillierter Gebäudeplan notwendig, mit dessen Hilfe ein genauer Plan des Kabelverlaufes (inklusive Abschlußwiderständen, Erdungspunkten, Repeatern, Bridges, ...) erstellt wird. Dabei ist auch auf Erweiterungsmöglichkeiten bedacht zu nehmen, auch wenn diese zum Zeitpunkt der Planung unwahrscheinlich erscheinen.

Planung des Netzwerkbetriebssystems

Jetzt sollte die Entscheidung für ein Netzwerkbetriebssystem (OES, Windows, Linux, (Peer-to-peer,) ...) fallen, wobei nur auf die Aufgaben des Netzwerkes bedacht zu nehmen ist.
„Glaubensentscheidungen“ sind in diesem Zusammenhang wenig hilfreich.

Planung der Server

In dieser Phase muß auf der Grundlage der bisherigen Planungen die Anzahl und der Ausbau der Server spezifiziert werden. Beim Plattenplatz und beim Hauptspeicher ist eine großzügige Dimensionierung anzustreben.

Planung sonstiger Netzwerkkomponenten

Fax

WAN

Einbindung anderer Rechnerwelten

...

Planung der Umgebungsbedingungen

Eigene Stromversorgung für Netzwerkkomponeten (Erdung besonders beachten - mehrere Gebäude)

Klimaanlagen

Schutz gegen statische Elektrizität

...

Erstellen eines Gesamtkonzeptes

Aus diesen Teilen muß ein Gesamtkonzept erstellt werden, da dabei eventuelle Unverträglichkeiten und sonstige Fehler zu Tage treten und die entsprechenden Korrekturmaßnahmen eingeleitet werden können.

Erstellen eines Phasenplanes

Die letzte Aufgabe ist die Erstellung eines Phasenplanes, bei dem der Übergang vom Istzustand zum Sollzustand in einzelne Abschnitte gegliedert ist. Für jeden Abschnitt ist die Angabe der dafür notwendigen Komponenten, eines Zeitplanes und der Gesamtkosten notwendig. Bei größeren Projekten ist auch die Wechselwirkung der einzelnen Phasen notwendig, da sonst „Lücken“ entstehen könnten.

Beispiel

- Siehe eigene Beispielangabe

II.1. Protokolle

- Definition
- Beispiele (nicht Netzwerke)
- Beispiele (Netzwerke)
- Ein konkretes Beispiel

Definition 1

- **Protokoll**: Die Gesamtheit aller Vereinbarungen über einen Ablauf
- Auch die Niederschrift über einen Vorgang (z.B.: Prüfungsprotokoll)
- **Kommunikationsprotokoll**: Die Gesamtheit aller Vereinbarungen über den Kommunikationsablauf

Definition 2

- **Netzwerkprotokoll**: Die Gesamtheit aller Vereinbarungen, Regeln und Formaten (**Syntax**) für das Kommunikationsverhalten (**Semantik**) zweier oder mehrerer Teilnehmer (Benutzer, Computer) über ein Netzwerk.

Beispiel 1

- Protokoll zum Telephonieren
  - Telephon aktivieren (Hörer abheben, …)
  - Rufnummer wählen
  - Gegenstelle meldet sich (Name, Nummer)
  - Eigene Meldung und Begrüßung
  - … (eigentliches Gepräch)
  - Verabschiedung
  - Telephon deaktivieren („auflegen“, …)

Beispiel 2

- Protokoll zum Fahrkartenkauf (Schalter)
  - Kontaktaufnahme (Begrüßung)
  - Nennung von Ziel und Abfahrtszeit
  - Abklären der Optionen (Klasse, …)
  - Erfahren des Preises
  - Zahlvorgang (eig. Protokoll)
  - Beendigung

Beispiel 3

- Protokoll zum Mail abholen (POP3)
  - Verbindungsaufnahme mit Server Port 110
  - Authentifizierung
    - „USER <username>“
    - „PASS <password>“
  - Transaktion (Schleife)
    - „STAT“
    - „RETR <nr>“
    - „DELE <nr>“
  - Update und Ende
    - „QUIT“

Beispiel 4

- Protokoll zum Mail versenden (SMTP)
  - Verbindungsaufnahme mit Server Port 25
  - Eröffnung und Authentifizierung
    - „HELO <hostname>“ oder „EHLO <hostname>“
  - Transfer
    - „MAIL FROM:<mail-adresse>“
    - „RCPT TO:<mail-adresse>“
    - „DATA … .“
  - Beendigung
    - „QUIT“

Konkretes Beispiel

Eine Abfrage einer Webseite wird mittels Wireshark mitprotokolliert.

- Die einzelnen Pakete werden besprochen
- Aufgaben der Protokolle ARP, DNS und HTTP besprechen

II.2. Private Servernetze

- Server im eigenen Netz i.a. ohne Zugriff für die Öffentlichkeit
- Meist eine RFC 1918-Adresse
- Mehrere Aufgaben
  - Fileserver, Printserver
  - Datenbankserver, Mailserver
- Nur organisatorische und keine technische Entscheidung

Privater Server - Beispiel

- Planung eines „Core“-Server
- Erstellung der notwendigen Aufgaben
- Auflistung der in Frage kommenden Betriebssysteme
- Kosten-Nutzen-Überlegungen
- Installation
- Betrieb

II.3. Switching und Routing

- Übersicht Netzwerkgeräte
- Switching
- Routing

II.3.1 Netzwerkgeräte

- Repeater
- Hub
- Bridge
- Switch
- Access Point
- Router
- Gateway

Repeater

- Repeater sind reine Signalverstärker, die keinerlei Prüfung der Frames (Rahmen) vornehmen, sondern nur die physischen Signale auf einem Port (Anschluß) empfangen und auf einem anderen Port neu versenden, wodurch größere Entfernungen erreichbar sind.
- Arbeiten in ISO-Schicht 1

Hub

- Hubs sind Multiportrepeater
- Arbeiten in ISO-Schicht 1
- Trennen daher keine „Collision-Domains“
- Gemeinsame Bandbreite für alle angeschlossenen Geräte

Bridge

- Bridges empfangen einen Frame und versenden ihn nach Prüfung neu.
- Arbeiten in den ISO-Schichten 1 und 2.
- Trennen „Collision-Domains“
- Unterschieden werden:
  - MAC-Bridges
  - LLC-Bridges

Switch

- Switches sind Multi-Port-Bridges.
- Arbeiten in den ISO-Schichten 1 und 2.
- Trennen „Collision Domains“
- Unterschieden werden:
  - Cut through, Store and Forward, Error free cut through
  - Symmetrisch und Asymmetrisch
  - Shared und Port Based Memory

Access Point

- Ein Access Point verbindet (bridged) wireless Segment mit wired Segmenten eines Netzwerkes oder nur wireless Komponenten.
- Arbeitet in den ISO-Schichten 1 und 2.
- Trennt „Collision-Domains“

Router

- Ein Router dient der Vermittlung von Netzwerkpaketen. An Hand der Zieladresse und einer Subnetmaske (Routingtabelle) wird entschieden, wie das Paket weitergeleitet wird.
- Arbeitet in ISO-Schicht 3
- Man unterscheidet Routingprotokolle und geroutete Protokolle.
- Trennt Broadcastdomänen

Gateway

- Zur Verbindung von Netzwerken mit verschiedenen Strukturen (z.B.: ISO und nicht-ISO) werden Gateways benutzt.
- Verbindungen auf höherer ISO-Schicht als 3 werden ebenfalls mit Hilfe von Gateways realisiert.

II.3.2 Switching

- Grundlagen
- Funktionsweise
- Techniken
- Bandbreite
- Speicheraufbau
- Weitere Merkmale

Switching – Grundlagen

- Ein Switch ist grundsätzlich ein Layer 2 Device
- Heute gibt es auch Switches die Aufgaben höherer Schichten übernehmen
- Der Ausdruck Layer-3-Switch ist daher am Markt präsent aber falsch

Switching – Funktionsweise 1

- An Hand der Ziel-MAC-Adresse im Paket leitet der Switch das Paket an einem bestimmten Port weiter
- Sollte die Ziel-MAC-Adresse unbekannt sein, wird das Paket an alle Ports (außer dem Port an dem es eingelangt ist) weitergeleitet

Switching – Funktionsweise 2

- Die Quell-MAC-Adresse wird in die Tabelle eingetragen
- Zur Verweidung von Switchingloops wird STP (Spanning Tree Protocol) eingesetzt
- VLANs werden mit Hilfe von Switches umgesetzt

Switching – Techniken

- Store and Forward
- Cut through (Fast forward)
- Error free cut through

Store and Forward

- Das ganze Paket wird empfangen und geprüft (FCS)
- Nach Auswertung der Ziel-MAC-Adresse wird das Paket weitergeleitet
- Fehlerhafte Pakete bzw. Kollisionsfragmente werden nicht weitergeleitet

Cut Through

- Auch „Fast Forward“ genannt
- Sobald die Ziel-MAC-Adresse erkannt ist, wird mit der Weiterleitung begonnen
- Fehlerhafte Pakete werden daher ebenfalls weitergeleitet
- Schnell

Error Free Cut Through

- Hier werden die ersten 64 Byte des Pakets gelesen
- Die Ziel-MAC-Adresse ausgewertet und das Paket weitergeleitet
- Collisionsfragmente sind kürzer als 64 Byte und werden daher nicht weitergeleitet.

Switching – Bandbreite

- Hier wird unterschieden ob die Bandbreite der Ports gleich oder verschieden ist
- Symmetrisch
  - Alle Port haben die gleiche Bandbreite
- Asymmetrisch
  - Ports haben unterschiedliche Bandbreite

Switching – Speicheraufbau

- Port Based Memory
  - Speicherbereich sind den Ports zugeordnet
  - Eingangsbuffer
  - Ausgangsbuffer
- Shared Memory
  - Speicher kann dynamisch für jedes Port verwendet werden

Switching – Weitere Merkmale

- Portanzahl (8, 16, 24, …)
- PoE (Power over Ethernet)-Fähigkeiten
- Managed oder Unmanaged

II.3.3. Routing

- Grundlagen
- Router-Details
- Cisco IOS
- IOS Basiskonfigurationsbeispiel

Grundlagen

- Routing – Was ist das?
- Einordnung in das Netzwerkumfeld
- Protokolle
- Routingvarianten
- IP-Subnetting

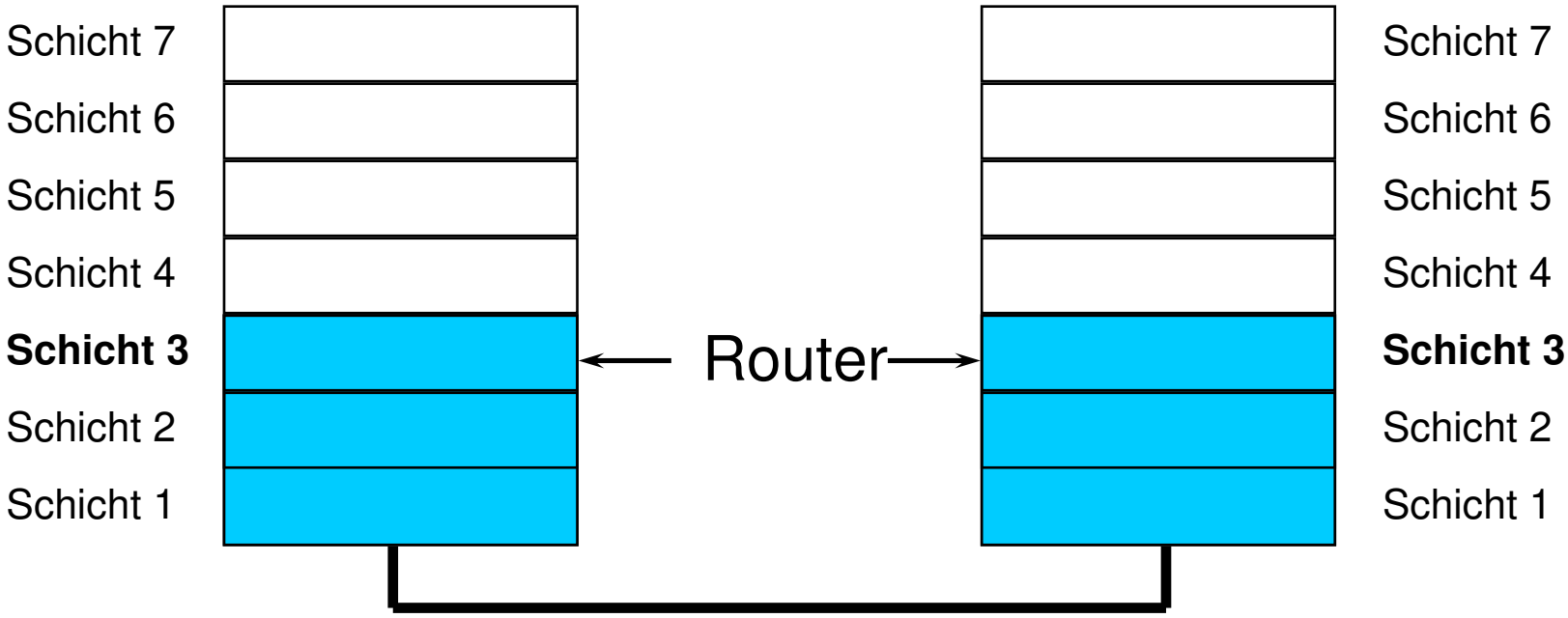
Grundlagen – Routing

- Wegefindung und –auswahl im Netz
- Durchführung entweder non-dedicated oder dedicated
- Non-dedicated: Softwarelösungen (Serversoftware z.B.: Linux, Netware, Windows, Shareware, ...)
- Dedicated: CISCO, 3COM, ...

Grundlagen – Einordnung

- Im ISO-Modell in Schicht 3 angesiedelt
- Im Internetmodell in der Schicht Internet (IP) ausgeführt
- d.h. damit ein Paket weitergeleitet werden kann, muß es bis zur entsprechenden Schicht ausgepackt werden.

Grundlagen – Einordnung



Grundlagen – Protokolle

- Routing Protocol (Protokolle mit deren Hilfe Informationen über das Routing ausgetauscht werden)
  - RIP
  - OSPF
- Routed Protocols (Protokolle, die geroutet werden)
  - IP
  - IPX

Grundlagen - Varianten

- Static routing
  - Durch Administratoren festgelegte Wege
- Dynamic routing
  - Dynamisch von Router festgelegte Wege (z.B. Shortest Path, ...)
  - Distance Vector –Protokolle (RIP)
  - Link-State Protokolle (OSPF, IGRP)

Grundlagen – IP-Subnetting

- Teile einer IP-Adresse
- Warum Aufteilung?
- Adressklassen
- Classless Interdomain Routing
- Versteckte Adressen
- Kleinste (0=Netz) Adresse meist reserviert
- Größte (-1=Broadcast) Adresse reserviert

Grundlagen – IP-Adressen

- Jede IP-Adresse besteht aus 2 Teilen
  - Netzanteil

    Bestimmt den gemeinsamen Teil der Adresse, der für alle Rechner im selben Netz gleich ist.
  - Hostanteil

    Ist der „Unique“-Anteil der Adresse, den nur diesem Rechner zugeordnet ist.

Grundlagen – Aufteilung

- Sehr oft wird nicht der gesamte Adressbereich für ein Netz benötigt, dann kann dieses Netz in Subnetze geteilt werden, d.h. ein Teil der Host-Adresse wird für den Subnetzanteil verwendet.
- Aufteilung eines Netzes in Subnetze

Grundlagen – Aufteilung

- Die Adressen haben eigentlich 3 Teile:
  - Netzanteil, Subnetzanteil, Hostanteil
- Für alle beteiligten Systeme ist aber weiterhin nur eine 2-Teilung sinnvoll
  - Netzanteil, Hostanteil
- Der Subnetzanteil wird je nach Betrachtungsweise zum Netz- oder Hostanteil dazugerechnet.

Grundlagen – Adressklassen

- Früher war das durch die Adressklasse bestimmt
- Je nach Firmengröße wurde eine der verfügbaren Klassen zugeteilt.
- Klassen A bis C
- Klasse D und E für besondere Zwecke

Grundlagen – Adressklassen

- Klasse A
  - 8-Bit Netzadresse
  - 24-Bit Hostadresse
  - Erkennbar am 1. Bit der Adresse (=0)
  - Adressbereich (0 – 127)

Grundlagen – Adressklassen

- Klasse B
  - 16-Bit Netzadresse
  - 16-Bit Hostadresse
  - Erkennbar an den ersten 2 Bit der Adresse (=10)
  - Adressbereich (128.0 – 191.255)

Grundlagen – Adressklassen

- Klasse C
  - 24-Bit Netzadresse
  - 8-Bit Hostadresse
  - Erkennbar an den ersten 3 Bit der Adresse (=110)
  - Adressbereich (192.0.0 – 223.255.255)

Grundlagen – Adressklassen

- Klasse D
  - Multicastadressen
  - Erkennbar an den ersten 4 Bit der Adresse (=1110)
  - Adressbereich (224.0.0.0 – 239.255.255.255)

Grundlagen – Adressklassen

- Klasse E
  - Adressen für experimentelle Zwecke
  - Erkennbar an den ersten 4 Bit der Adresse (=1111)
  - Adressbereich (240.0.0.0 – 255.255.255.255)

Grundlagen - Classless

- Seit 1994 verwendet man meist „Classless Routing“, um den flexiblen Anforderungen Rechnung tragen zu können
- Angabe einer Subnetmaske notwendig, um bestimmen zu können, welche Teil ist Netzadresse und welcher Teil ist Hostadresse.

Grundlagen – Classless

- Die Angabe der Subnetzmaske kann auf zwei Arten erfolgen:
  - Als Bitmaske (erfolgt als eigenständige Angabe)

    z.B.: 255.255.255.0 (für Klasse-C-Netze)
  - Als Anzahl der Netzbits (wird hinter die Netzadresse angehängt.

    z.B.: /24 (für Klasse-C-Netze)

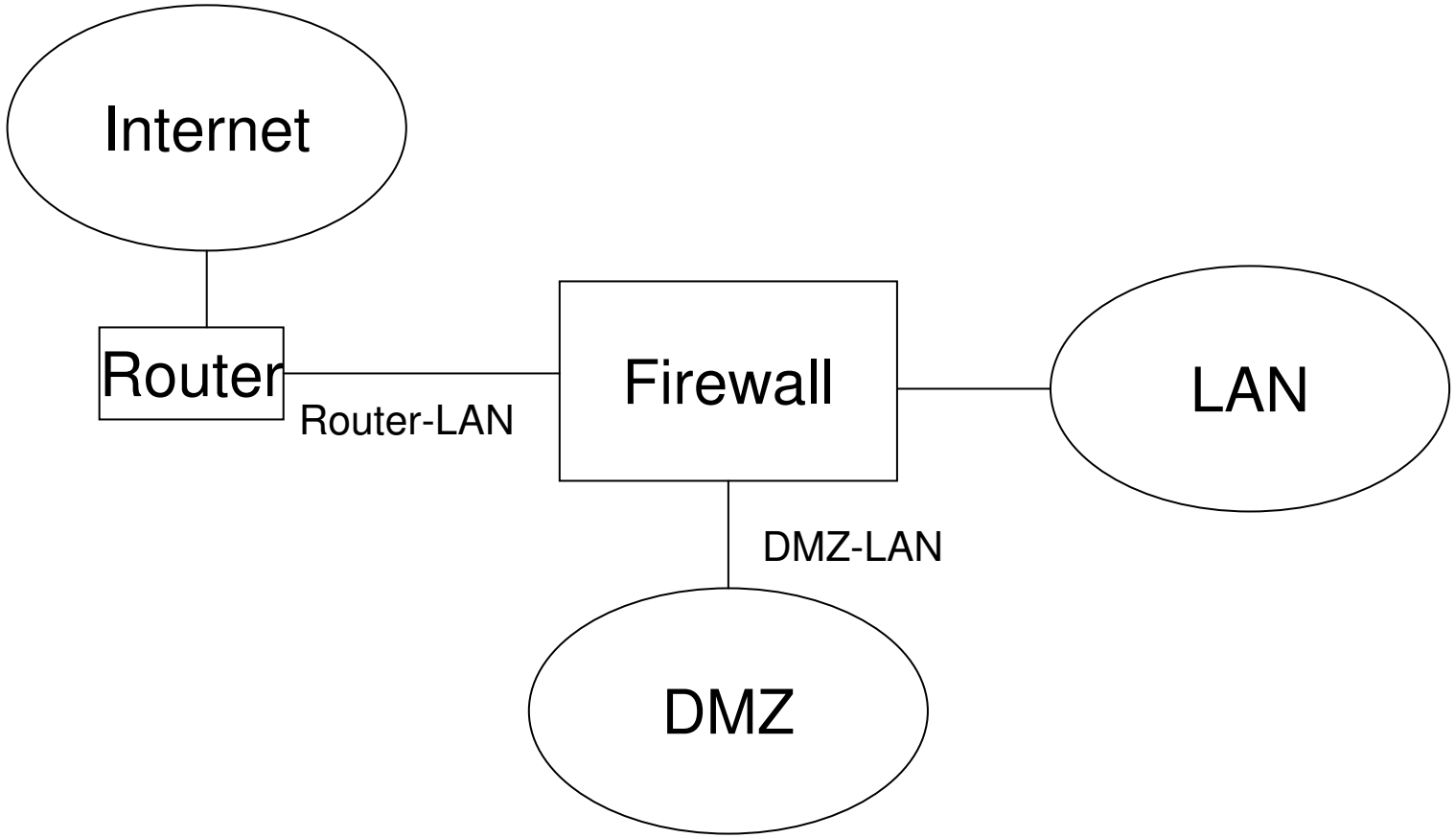
Grundlagen – Classless

- Eine Firma bekommt z.B. den folgenden Adressbereich zugeteilt:
  - Netzadresse 193.170.108.192
  - Subnetmaske 255.255.255.240
- Das bedeutet, daß der Firma 16 Adressen (193.170.108.192 bis 193.170.108.207) zugeordnet sind, von denen sie 14 frei nutzen kann.

Grundlagen – Classless

- Bei weiterer Unterteilung (z.B. durch eine Firewall, werden immer weniger Adressen nutzbar):
- Router-LAN (193.170.108.192/30)
  - 2 nutzbare Adressen
- DMZ (193.170.108.200/29)
  - 6 nutzbare Adressen

Grundlagen – Classless



Grundlagen – Adressen für private Internets

- Damit der zunehmende Bedarf an Adressen gedeckt werden kann und
- um eine höhere Sicherheit zu ermöglichen,
- wurde eine Reihe von Netzadressen reserviert, die auch als versteckte Adressen gelten und nicht in das Internet gerouted werden dürfen.

Grundlagen – Adressen für private Internets

- Definiert durch RFC 1918
- Daher auch RFC 1918-Adressen,
- Oder nicht routbare Adressen genannt
- Manchmal auch versteckte Adressen genannt

Grundlagen – Adressen für private Internets

- RFC1918-Adressen der Klasse A
  - 10.0.0.0 – 10.255.255.255
  - 10.0.0.0/8
- RFC1918-Adressen der Klasse B
  - 172.16.0.0 – 172.31.255.255
  - 172.16.0.0/12
- RFC1918-Adressen der Klasse C
  - 192.168.0.0 – 192.168.255.255
  - 192.168.0.0/16

Grundlagen - APIPA

- Automatic Private IP Adressing
- Meist wenn DHCP-Server nicht erreichbar
- Bereich:
  - 169.254.0.0-169.254.255.255
  - 169.254.0.0/16
- RFC 3330: Special-Use IPv4 Addresses

Grundlagen - APIPA

- Mittlerweile „IPv4 Link Local Adresses“
- Im Rahmen einer ergebnislosen „Zero Configuration Networking“-Initiative der IETF
- RFC 3927 „Dynamic Configuration of IPv4 Link-Local Addresses”

Router

- Aufbau
- Funktionsweise
- Wegefindung
- Beispiele

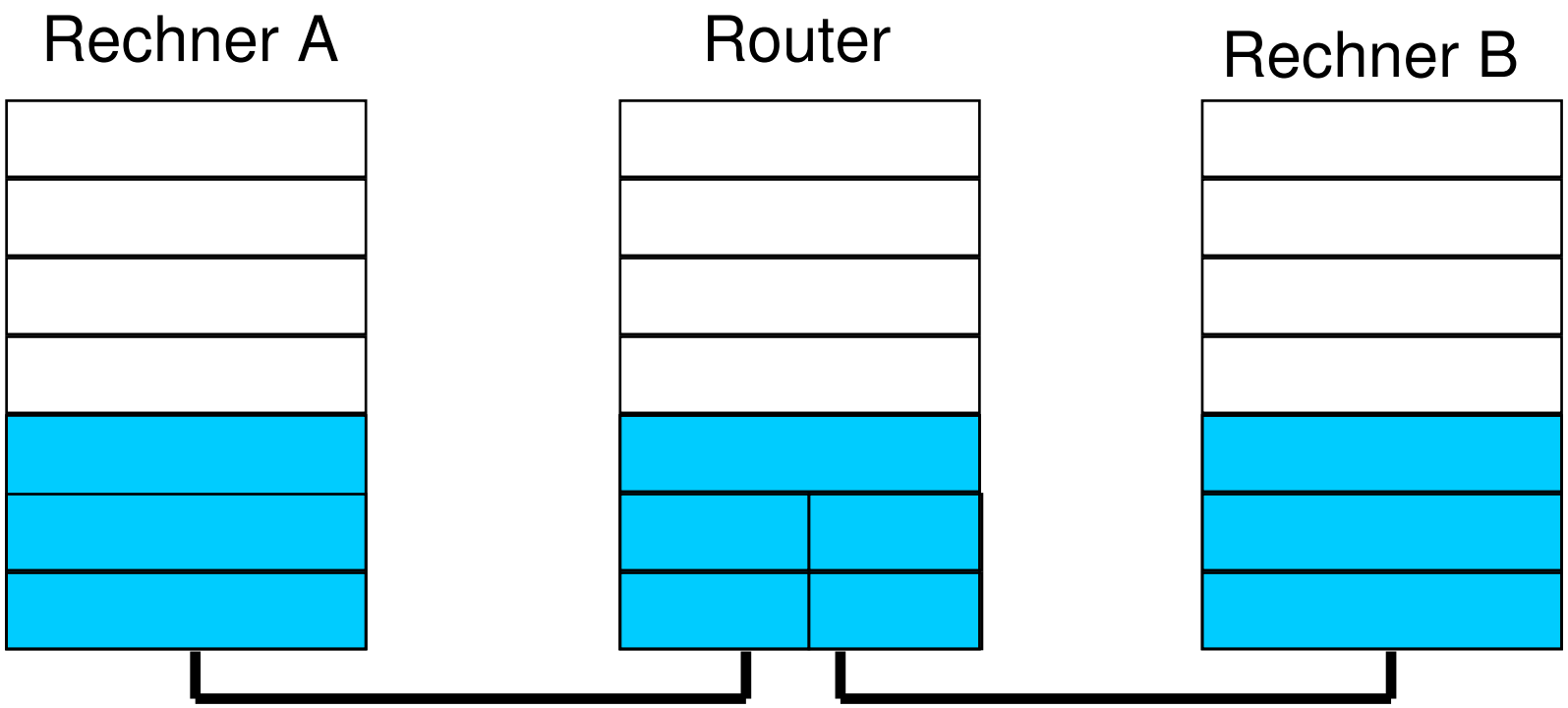
Router – Aufbau

- Prozessor
- Speicher (für Tabellen, ...)
- Netzwerkschnittstellen (üblicherweise zumindest zwei)
- Optional: Anzeigen

Router – Funktionsweise

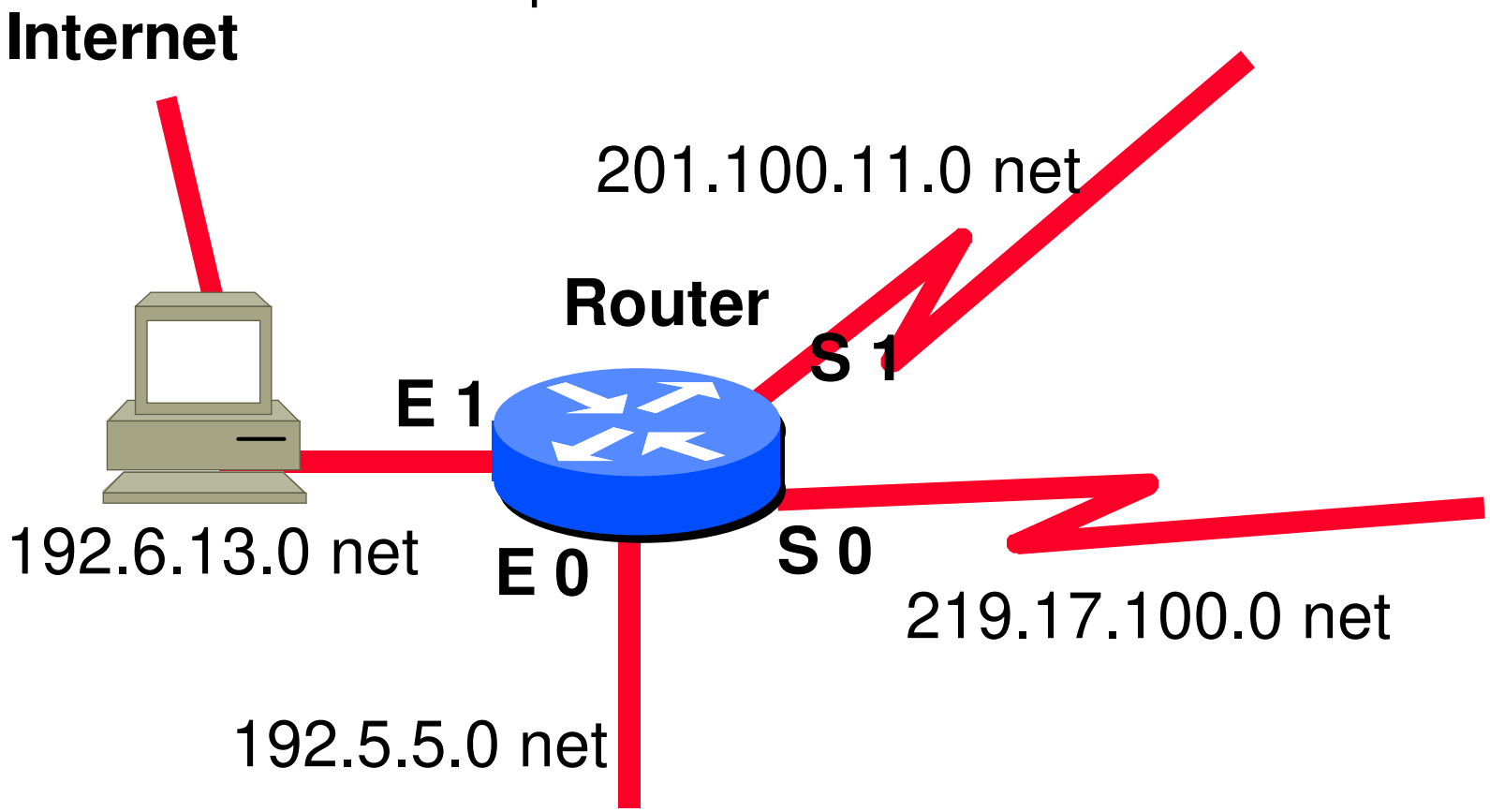
- Entpacken eines Frames bis zur Routing Schicht
- Vergleich der Netzanteils der Adresse mit den Einträgen der Routingtabelle
- Weiterleiten zur entsprechenden Schnittstelle
- Einpacken in einen neuen Frame

Router – Funktionsweise



Router – Funktionsweise

Beispiel



Router – Funktionsweise

Beispiel Routingtabelle

Netz	Schnittstelle
192.5.5.0	E0
192.6.13.0	E1
201.100.11.0	S1
219.17.100.0	S0
223.8.151.0	S1
Default	E1

Router – Wegefindung

- Kriterien für die Beurteilung eines Weges
  - Meßbare Kriterien
  - Maßzahl
- Unterscheidung
  - Stub-Netzwerk-Router
  - Backbone-Router

Router – Meßbare Kriterien

- Kosten
- Anzahl der Hops
- Bandbreite
- Verfügbarkeit
- Sicherheit
- ...

Router – Stub-Netzwerk

Vor allem in kleineren Firmen meist sogenannte Stub-Netzwerke, da besteht die Wegefindung des Routers nur aus der Entscheidung intern oder extern (für beides existieren üblicherweise zwei getrennte Schnittstellen), wodurch die Wegefindung wesentliche vereinfacht wird.

Router – Back-Bone

Back-Bone-Router haben meist mehrere Wege zum Ziel und müssen nach vorgegebenen Kriterien (Kosten, Durchsatz, Verfügbarkeit, ...) den günstigsten Weg suchen, dazu wird für alle Wege die Summe der „Kosten“ gebildet und der „beste“ Weg ausgewählt.

Router – Beispiele

- Internetsharing z.B. mit Windows ME
- Server mit mehreren Netzwerkschnittstellen
- BayNetworks RT328 ISDN-Router
- Cisco 2500
- Cisco 12000

IOS

- Was ist das?
- IOS-Modi
- Wichtigste Befehle

IOS – Was ist das?

- IOS steht für Internet Operating System und ist das Betriebssystem der Netzwerkgeräte der Firma CISCO (mit Ausnahme der Kleinstgeräte).
- IOS erlaubt die Konfiguration der Geräte über eine standardisierte Textschnittstelle

IOS – IOS-Modi

- Run Mode (Betrieb)
- User Mode (Wenige Befehle)
- Privileged Mode (Alle Befehle zur Verwaltung des Gerätes)
- Configuration Mode (Alle Konfigurationsbefehle)

IOS – Wichtigste Befehle

- ?
- ENable / DISAble
- CONFig Terminal
- EXIt
- SHow
- PIng /TRaceroute

Basiskonfiguration

- Erstellen
- Testen
- Speichern
- Beispiel

Basiskonfiguration – Erstellen

- Nicht konfigurierter Router hat beim ersten Start einen „initial configuration dialog“
- Besser durch die entsprechenden Befehle
- Zumindest die Netzwerkschnittstellen
- Passwörter (Sicherheit)

Basiskonfiguration – Testen

- Testen der Konfiguration durch entsprechende Befehle (ping, traceroute)
- Bei Fehlern Konfiguration anpassen, solange bis alle Funktionen korrekt erfüllt werden.
- SHOW RUNNING

Basiskonfiguration – Speichern

- COPY RUNNING-CONFIG STARTUP-CONFIG
- Sichern der Konfiguration
  - Log eines SHOW RUNNING
  - COPY RUNNING-CONFIG TFTP
- REBOOT

Basiskonfiguration - Beispiel

- Anbindung eines LANs per 128 Kbit/s-Standleitung über einen Provider
- Verwendet wird ein CISCO 2500
- Alles für das LAN wird an einen Rechner (z.B.: Firewall) geschickt
- Alles für das Internet wird an den Provider weitergeleitet

Basiskonfiguration - Beispiel

- !Allgemeines
  - service password-encryption
  - hostname <logischer Name>
  - enable password <password>
  - ip subnet-zero
  - ip domain-name <domain-name>
  - ip name-server <dns-server>

Basiskonfiguration - Beispiel

- !Schnittstellen
  - interface Ethernet0
  - ip address <IP-Adresse> <Netzmaske>
  - interface Serial0
  - bandwidth 128
  - ip address <IP-Adresse> <Netzmaske>
  - encapsulation frame-relay ietf
  - frame-relay lmi-type ansi

Basiskonfiguration - Beispiel

- !Routing Informationen
  - ip classless
  - ip route 0.0.0.0 0.0.0.0 <gateway>
  - ip route <netz> <maske> <ziel>

Basiskonfiguration - Beispiel

- !Zugang
  - line con 0
  - password <Passwort für lokalen Zugang>
  - login
  - line vty 0 4
  - password <Passwort für Telnetzugang>
  - login

II.4. Öffentliche Netze

- Einführung und Abgrenzung
- Arten von öffentlichen Netzen
- Verwendung von öffentlichen Netzen
- Mobile Netze
- Anwendungsbeispiele

Einführung und Abgrenzung

- Private Netze
- Öffentliche Netze
- Öffentliche Netze ↔ Private Netze

Private Netze

- Auf eigenem Bereich (Firmengelände)
- Mit eigenem Equipment (Router, Switches, Kabel, …)
- Volle Verantwortung für die Funktionsfähigkeit beim „Betreiber“
- Alle technischen Möglichkeiten verwendbar

Öffentliche Netze 1

- Öffentliche Netze sind für die Benutzung für alle
- Im öffentlichen Raum
- Betrieb durch einen „Service Provider“ (Telefongesellschaft, ISP, Kabelanbieter) mit Auflagen
- Equipment vom Anbieter

Öffentliche Netze 2

- Rechtlicher Rahmen und Verfügbarkeit von der Allgemeinheit (Staat) im Rahmen von Gesetzen definiert
- Internationale Verträge sichern die Ausbreitung über Staatsgrenzen hinweg (trotzdem landesspezifische Eigenschaften)

Arten von öffentlichen Netzen

- Kabelgebundene öffentliche Netze
  - Telephon (analog, ISDN, T1, …)
  - DSL (ADSL, VDSL, HDSL, …)
  - Koaxialkabel, LWL, Stromnetze
- Kabellose öffentliche Netze
  - Rundfunk, Fernsehen
  - Mobilfunk, Richtfunk
  - Satellitenverbindungen

Verwendung v.öffentl. Netzen

- Vertrag mit einem Serviceanbieter (Provider)
- Oft mit Service Level Agreement (SLA)
- Übergabepunkt (POP) zwischen öffentlichem und privatem Netz (Zähler, Modem, Splitter, Router, …)

Mobile Netze

- Grundlagen Funkübertragung
- Geschichte
- Überblick
- GSM
- UMTS
- LTE
- Details zur Realisierung

Funkübertragung

- Funkübertragungen werden in zunehmenden Maße für die Datenkommunikation eingesetzt.
- Die Übertragung erfolgt mit Hilfe elektromagnetischer Wellen ohne definiertes Medium.

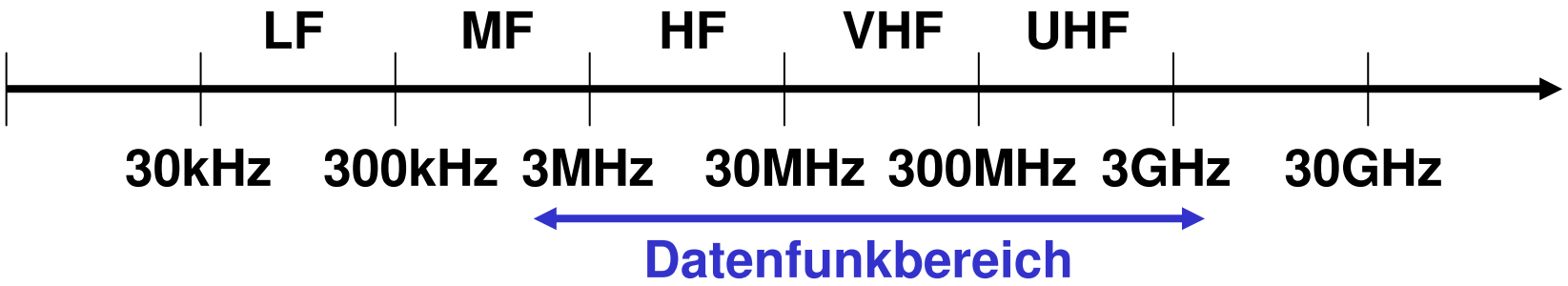
Vorteile der Funkübertragung

- Kabellose Verbindung (keine „Stemmarbeiten“)
- Schnelle Installation
- Mobile Sender und Empfänger
- Breitband-Fähigkeiten
- Broadcastfähigkeiten

Nachteile der Funkübertragung

- Interferenzen und Ausbreitungsprobleme
- Frequenzknappheit
- Datensicherungsprobleme
- Designprobleme (Lage der Antennen)
- Behördliche Restriktionen (Funk- und „Bau“probleme) und Lizenzvergabe

Frequenzband

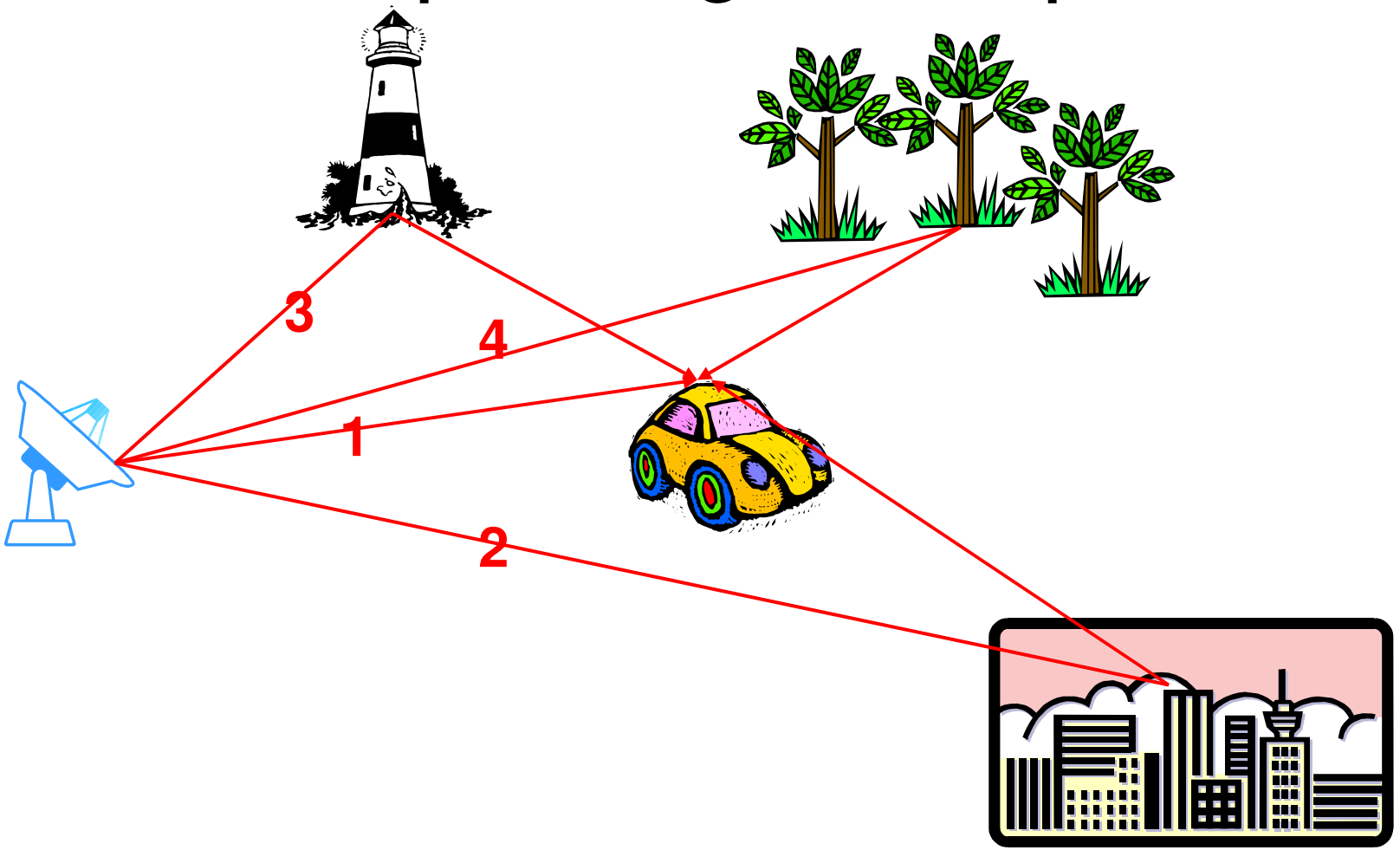


- Unter 2 MHz nicht möglich, da die Antennen zu groß wären
- Über ca. 5 GHz Dämpfung bereits durch Luftfeuchtigkeit (Regen, ...)
- Auch Hörfunk und TV nutzen diese Frequenzen

„Multipathing“

- Wellen erreichen den Empfänger auf verschiedenem Weg und daher nicht gleichzeitig.
- Phasenverschiebung der Wellen zueinander durch unterschiedliche Anzahl von Reflexionen.
- Die Überlagerung verursacht Interferenzen, die bis zur Auslöschung des Signals führen können.

„Multipathing“- Beispiel



Dopplereffekt

- Durch die Bewegung des Senders oder des Empfängers (oder beider) ändert sich die Frequenz scheinbar

$$f = f_0\left(1+\frac{v}{c}\right)$$

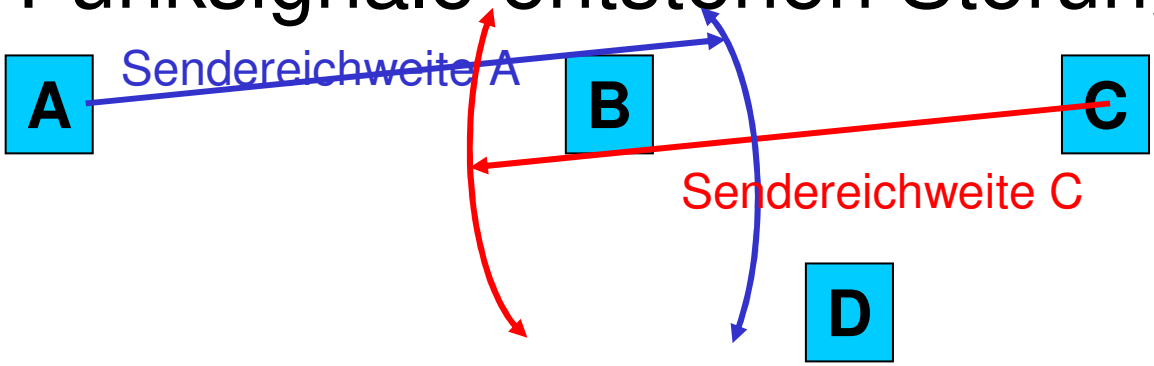
Empfänger bewegt sich auf die feststehende Quelle zu

$$f = f_0\left(1-\frac{v}{c}\right)$$

Empfänger bewegt sich von der feststehenden Quelle fort

„Versteckte“ Stationen

- Durch die begrenzte Reichweite der Funksignale entstehen Störungen:



- A sendet an B, doch kann B nicht empfangen wenn C zeitgleich an B oder D sendet (C ist für A versteckt).

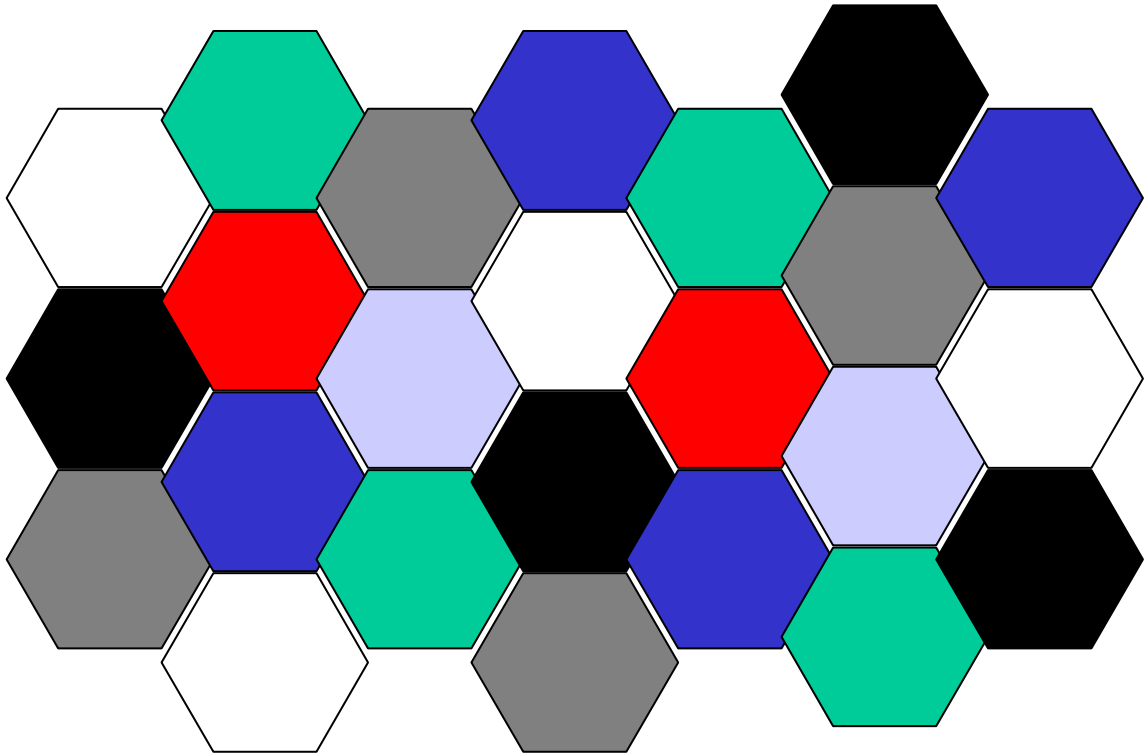
Sonstige Fehler

- Thermisches Rauschen
- Atmosphärisches Rauschen
- „Elektromagnetische Umweltverschmutzung“
- Räumliche Ausbreitung führt zu großem Energieverlust

Zellsysteme

- Um der Frequenzknappheit zu begegnen, werden Frequenzen in verschiedenen räumlichen Gebieten wiederverwendet.
- Dabei wird die begrenzte Sendereichweite ausgenützt.
- Bei Bewegung aber Frequenzumschaltung notwendig

Zellsysteme – Beispiel



Jedes Sechseck ist eine Zelle

7 Zellen bilden einen Cluster (jede Zelle mit den sechs angrenzenden Zellen)

Jede Farbe stellt eine Frequenz dar

Mobile Netze – Geschichte1

- 1924 USA: Funkvermittlungssystem für Züge mit einzelnen Funkstationen
- 1946 USA: 1. Mobilfunknetz in Missouri
- 1958 Deutschland: 1. Mobilfunknetz (A-Netz, bis 1977 flächendeckend aktiv)
- 1972 Deutschland: B-Netz
- 1973 Öst.: 1. Mobilfunknetz (öffentlicher beweglicher Landfunkdienst)

Mobile Netze – Geschichte2

- 1978 USA: 1. Zellulares Mobilfunknetz
- 1981 1. Europäisches Zellulares Mobilfunknetz (N,S,DK)
- 1984 Öst.: 1. Mobilnetz mit Selbstwahl (D-Netz; aktiv bis 1997)
- 1991 Öst.: GSM
- 2002 Öst.: UMTS
- 2013 Öst.: LTE

Mobile Netze - Überblick

- Analoge Netze (nicht weiter behandelt)
- GSM (2. Generation)
- GPRS/EDGE
- UMTS (3. Generation)
- HSDPA und HSUPA
- LTE (4. Generation)
- 5G (5. Generation)

GSM 1

- **G**lobal **S**ystem for **M**obile Communications
- 9600 Bit/s Übertragungsrate
- Digitaler zellularer Mobilfunkstandard
- Abhörsicherheit durch Verschlüsselung
- Weltweit einheitlicher Standard
- Mobiles Telephonieren auch im Ausland

GSM 2

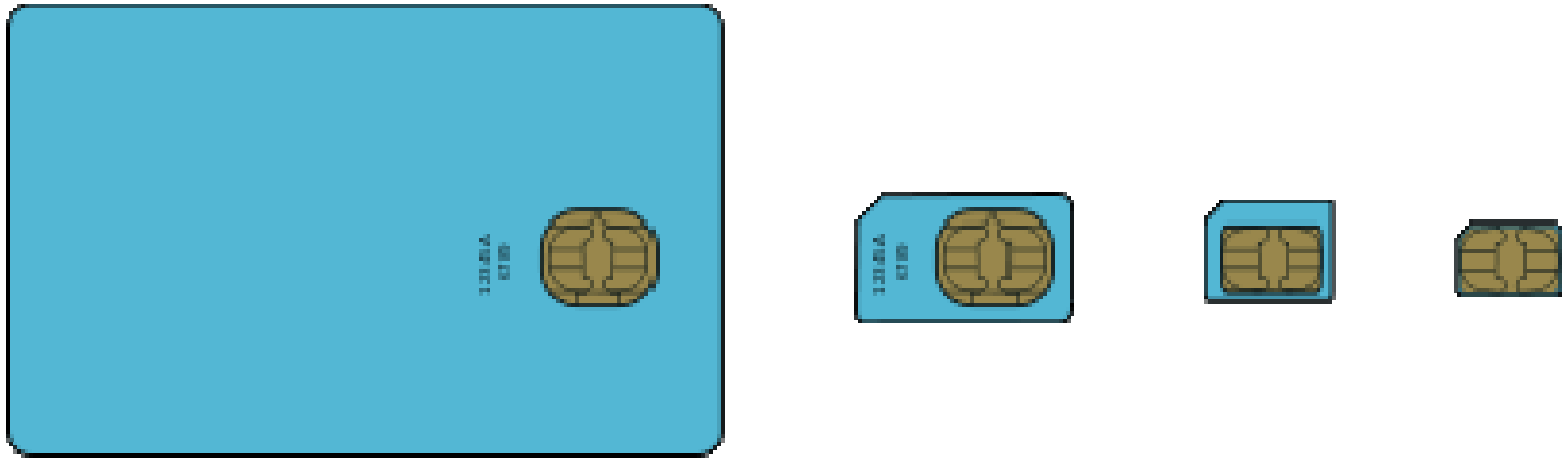
- SIM-Karte
  - Geräteunabhängigkeit
  - Sicherheitsabfrage (PIN-Code)
  - Teilnehmerdaten
  - IMSI (International Mobile Subscriber Identity)

GSM 3

- SIM-Format
  - Full Size (ISO/IEC 7810:2003, ID-1; 85,6*53,98mm)
  - Mini SIM (ISO/IEC 7810:2003, ID-000; 25*15mm)
  - Micro SIM (ETSI TS 102 221 V9.0.0, Mini-UICC; 15*12mm)
  - Nano SIM (ETSI TS 102 221 TS 102 221 V11.0.0; 12,3*8,8mm)
  - Embedded (JEDEC Design Guide 4.8 , SON-8, 6*5mm)

GSM 4

SIM bis NanoSIM

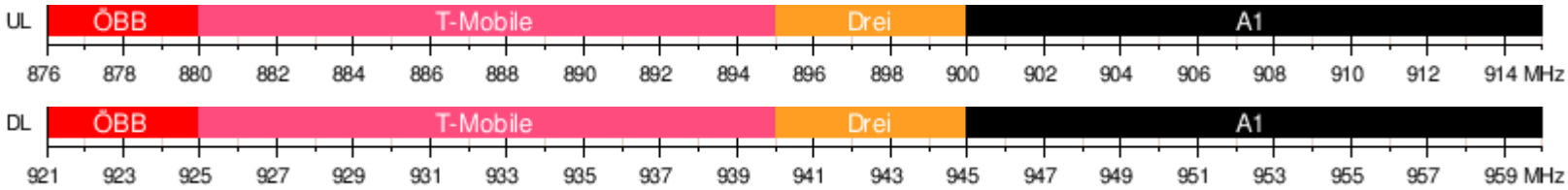


Quelle: http://upload.wikimedia.org/wikipedia/commons/e/e0/GSM_SIM_card_evolution.svg

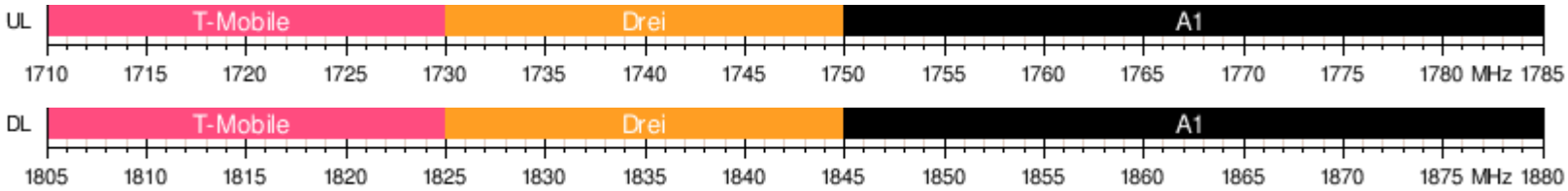
GSM 5

Frequenzaufteilung in Österreich

GSM-900



DCS-1800



Quelle: https://de.wikipedia.org/wiki/Global_System_for_Mobile_Communications

GPRS und EDGE

- **G**eneral **P**acket **R**adio **S**ervice
  - 56 kBit/s Übertragungsrate
  - Bündelung von bis zu 8 Timeslots
- **E**nhanced **D**ata Rates for **G**SM **E**volution
  - 220 kBit/s Übertragungsrate

UMTS 1

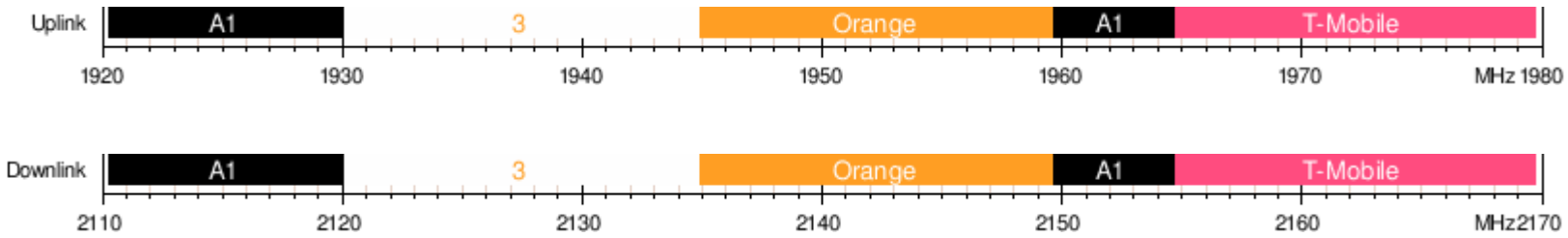
- **U**niversal **M**obile **T**elecommunications **S**ystem
- 3. Generation der Mobilfunknetze (3G)
- 384 kBit/s Übertragungrate
- Neue Funkzugriffstechnik (Breitband CDMA)
- Mehrere Datenströme gleichzeitig

UMTS 2

- Angebotene Dienste
  - Audio- und Videotelephonie
  - Unified Messaging
  - Internetzugang
  - Standortbezogene Dienste
  - Fernsehen

UMTS 3

Frequenzaufteilung in Österreich



Quelle: https://de.wikipedia.org/wiki/Universal_Mobile_Telecommunications_System

HSDPA und HSUPA

- **H**igh **S**peed **D**ownlink **P**acket **A**ccess
  - 3,6 bzw. 7,2 MBit/s Übertragungsrate
  - 3,5G oder 3G+ (G=Generation)
  - HSDPA+ bis 42 MBit/s Übertragungsrate
- **H**igh **S**peed **U**plink **P**acket **A**ccess
  - 5,76 MBit/s Übertragungsrate
  - HSUPA+ bis 23 MBit/s Übertragungsrate

LTE 1

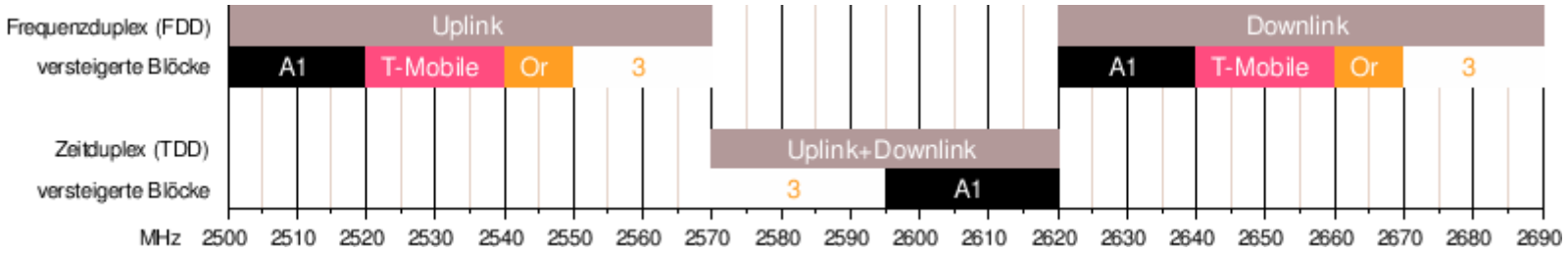
- **L**ong **T**ermin **E**volution
- 3,9/4. Generation der Mobilfunknetze
- 300 MBits/s Übertragungsrate
- Nutzung der UMTS-Infrastruktur
- Höhere Datenraten durch
  - QAM (Quadraturamplitudenmodulation)
  - MIMO (Multiple Input/Multiple Output)

LTE 2

- Verwendete Kodierung
  - OFDMA (Orthogonal Frequency Division Multiple Access; Downlink)
  - SC-FDMA (Sub Carrier Frequency Division Multiple Access; Uplink)

LTE 3

Frequenzaufteilung in Österreich



Quelle: https://de.wikipedia.org/wiki/Long_Term_Evolution

5G

- 5. Generation der Mobilfunknetze
- Bis zu 20 GBits/s Übertragungsrate
- Latenzzeiten unter 1ms
- IoT-Tauglichkeit (auch für Echtzeitanwendungen geeignet)
- In Österreich wurden erste Frequenzen (3,4-3,8 GHz) Anfang 2019 versteigert

Realisierung 1

- In jeder Zelle existiert eine BTS (Base Transceiver Station)
- Innerhalb einer Zelle nehmen die Mobilgeräte Verbindung zur BTS auf
- Die BTS versorgt über einen Funkkanal alle Geräte innerhalb der Zelle mit allgemeinen Funktionen (Rundfunk)

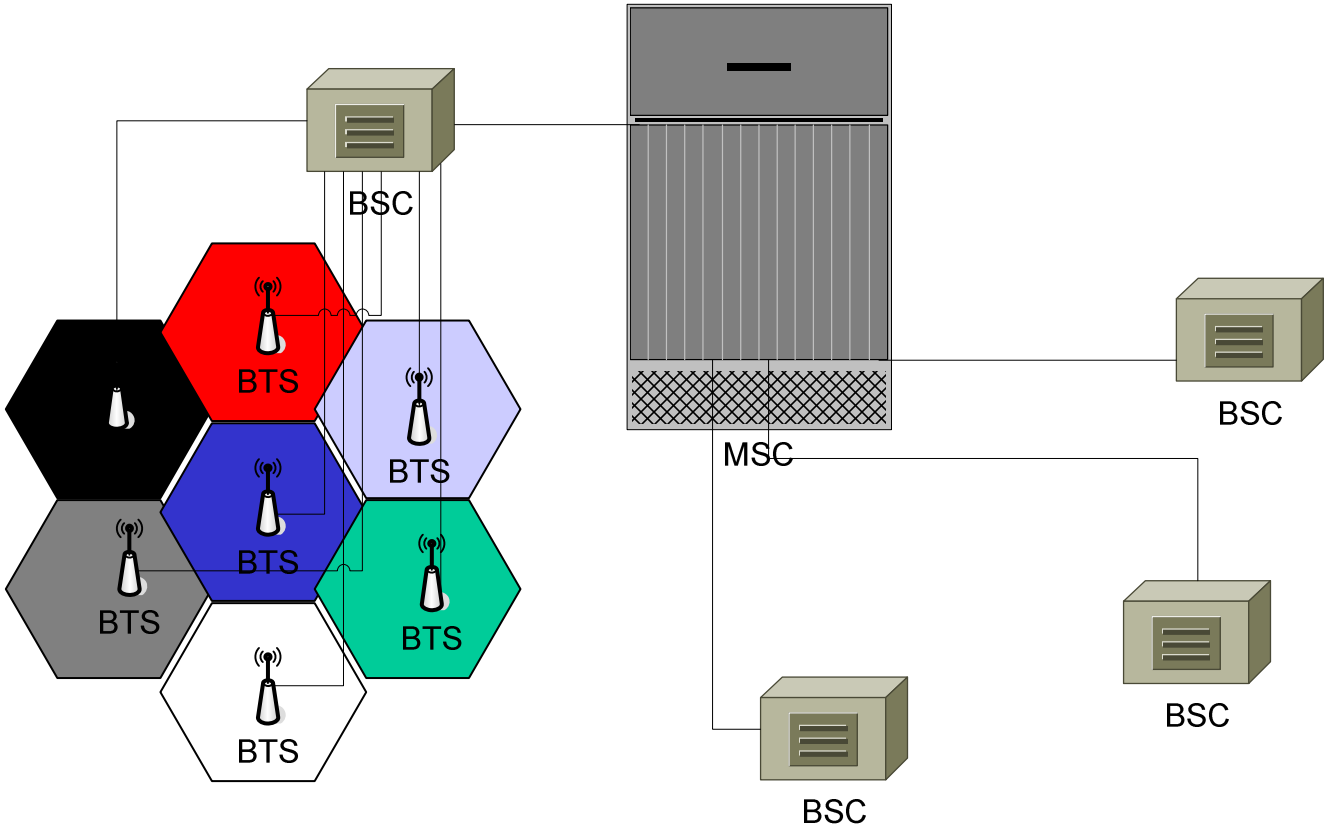
Realisierung 2

- Die Zellen müssen sich überlappen, damit genügend Zeit zum „Handover“ (Weiterreichen der Verbindung) besteht.
- Überlappungsbereich ist abhängig von der Geschwindigkeit des Mobilgerätes und der Zeit, die für das Handover benötigt wird (dzt. bis ca. 180km/h).

Realisierung 3

- Mehrere Zellen werden zu einer LA (Location Area) zusammengefaßt, damit der Aufenthaltsort des Mobilgerätes nicht zu oft aktualisiert werden muß
- Die LAs müssen an die topologischen Gegebenheiten angepaßt werden (Berge, Tunnels, …)

Realisierung 4



Realisierung 5

- BTS (Base Transceiver Station)
- BSC (Base Station Controller)
- MSC (Mobile Services Switching Center)
- GMSC (Gateway Mobile Services Switching Center)

Base Transceiver Station

- Funkversorgung einer Zelle
- Anschluß an BSC (meist per Leitung)
- Funktechnische Einrichtungen am Senderstandort
- Unmittelbare Kommunikation mit den mobilen Endgeräten

Base Station Controller

- Steuerung mehrerer BTS
- Steuerung des Verbindungsaufbaus
- Anschluß an MSC (Festnetz)
- Weiterreichen der Verbindung an andere BTS (soferne mit neue BTS am selben BSC angeschlossen ist)

Mobile Services Switching Center

- Verbindungsaufbau im Netz bzw. zu anderen Netzen (Gateway MSC)
- Verbindung des Vermittlungssystems mit der Basisstation
- Aufzeichnung der abrechungsrelevanten Gesprächsdaten

Anwendungsbeispiele

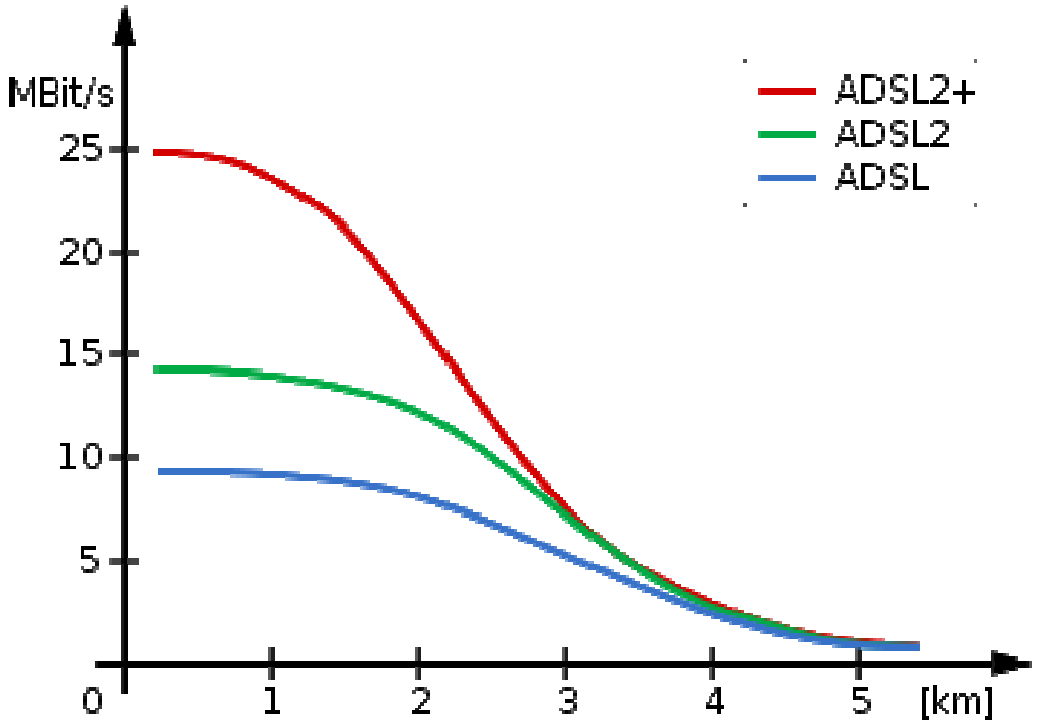
- ADSL
- Standleitungen
- MPLS
- Mobiles Internet

ADSL 1

- Asymmetric Digital Subscriber Line
- Datenrate entfernungsabhängig
- Kombinierbar mit POTS und ISDN
- Schmale Frequenzbänder, die je nach Störungssituation kombiniert werden
- Gegenstelle digital (DSLAM=DSL Acess Multiplexer)

ADSL 2

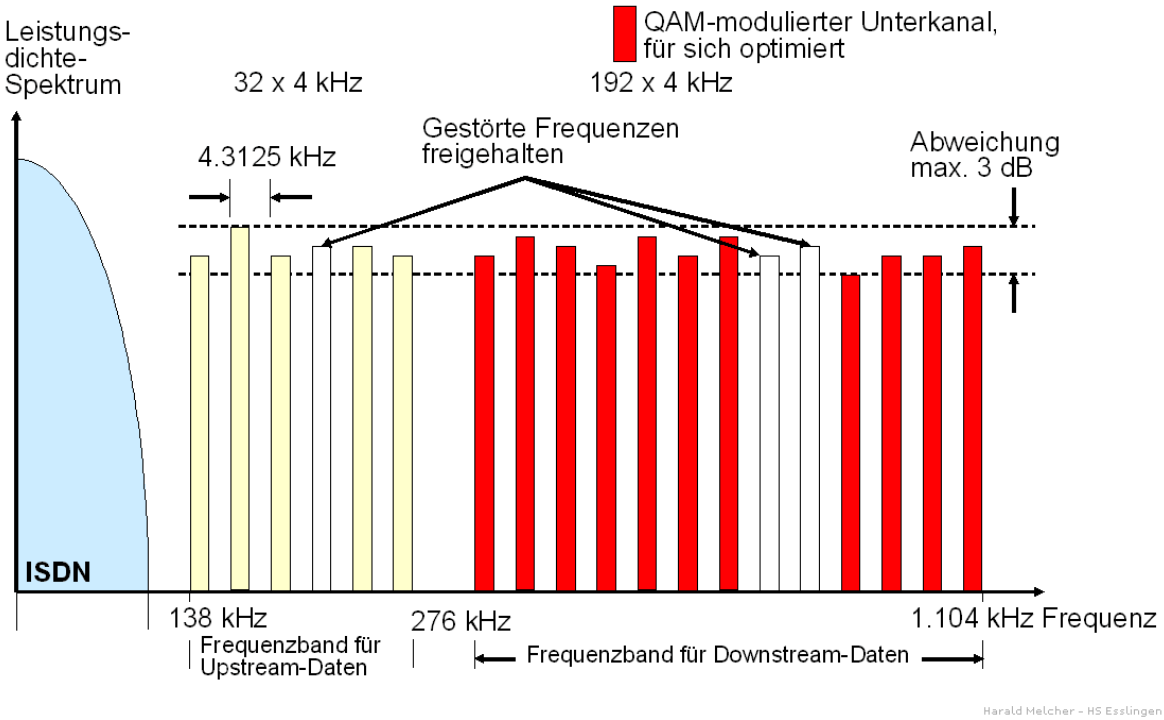
- Entfernungsabhängigkeit vom DSLAM



Quelle: http://de.wikipedia.org/wiki/ADSL

ADSL 3

Kanalwahl



Quelle: http://de.wikipedia.org/wiki/ADSL

Standleitung

- „Leased Line“
- Gemietete Leitung zwischen dem eigenen Standort und dem Provider
- Alleinige Benutzung durch den Kunden
- Kostenintensiv
- Heute oft durch VPN-Tunnels über das Internet ersetzt

MPLS

- Multiprotocol Label Switching
- Verbindungsorientierte Datenübertragung über verbindungslose Netze
- Zwischen ISO-Layer 2 und 3
- Layer 2 MPLS und Layer 3 MPLS
- Löst FrameRelay-Netze ab

Mobiles Internet

- z.B.: UMTS-Modem in Laptop, Tablet, Smartphone
- Standortunabhängig solange im Bereich des Mobilfunkanbieters und seiner Roamingpartner
- Weltweit möglich (trotz „weißer“ Flecken)

III.1 Internetdienste

- DNS
- DHCP
- WWW
- e-Mail
- Listen
- FTP, SFTP
- Telnet, SSH
- News

Dienste – DNS

- Domain Name System/Service
- RFC 1034 und 1035 + Updates dazu
- Symbolische Adressierung
- Bekannteste Realisierung:
  - BIND
- Oft auch in Verzeichnisdienste eingebunden

Internetadressierung

- Symbolische Adressen (DNS-Adressen)
- Logische Adressen (IP-Adressen)
- Physische Adressen (MAC-Adressen)
- Subadressen (Ports)
- e-Mail-Adressen
- URL

Symbolische Adressen

- Dienen in erster Linie dazu, die Adressen für uns leichter merkbar zumachen.
- z.B.:
  - WWW.ADV.AT
  - WWW.ORF.AT
  - MIRACULIX.HTL-TEX.AC.AT

Symbolische Adressen 2

- Bestehen aus zwei Teilen, dem Rechnernamen und dem Domainnamen und muß weltweit eindeutig sein.
- Die symbolischen Adressen werden mittels DNS (Domain Name System) in logische Adressen umgewandelt.
- Das DNS ist hierarchisch (nicht jeder Nameserver kennt alle Adressen).

Symbolische Adressen 3

- Rechner arbeiten nie mit symbolischen Adressen.
- Der nächstgelegene DNS-Server muß dem Rechner mit seiner logischen Adresse bekannt sein.

Symbolische Adressen 4

- Die Domainnamen sind strukturiert aufgebaut.
- Eigentlicher Domainname (häufig der Firmenname)
- SLD (Second level domain)
- TLD (Top level domain)

Symbolische Adressen 5

- Gängige SLDs
  - ac — academic
  - co, com — commercial
  - ed, edu — education
  - gv, gov — government
  - mil — military
  - or, org — organisations

Symbolische Adressen 6

- gängige TLDs
  - gTLDs Generic Topleveldomains

    Aus der Anfangszeit des Internets weltweite zentrale Vergabe durch von der ICANN beauftragte Institutionen
  - ccTLDs country code TLDs

    Für jedes Land ein Kürzel nach ISO 3166-1

Symbolische Adressen 7

- gTLDs
  - .aero Luftfahrtunternehmen
  - .biz Firmen
  - .com Kommerzielle Angebote
  - .coop Cooperatives
  - .edu Ausbildungsorganisation
  - .gov US Government
  - .info Informationsangebote

Symbolische Adressen 8

- gTLDs
  - .int Internationale Organisationen
  - .mil US Militär
  - .museum Museen
  - .name Für Einzelpersonen
  - .net Netzwerkbetreiber (ISPs)
  - .org Non-Profit Organisationen
  - .pro Gedacht für freie Berufe

Symbolische Adressen 9

- ccTLDs (Beispiele)
  - .at Austria
  - .au Australien
  - .ca Kanada
  - .de Deutschland
  - .fr Frankreich
  - .it Italien

Symbolische Adressen 10

- Beispiel 1

www.may.co.at

www	Name des Rechners
.may	Name der Firma
.co	commercial
.at	austria

Symbolische Adressen 11

- Beispiel 2

www.univie.ac.at

www	Name des Rechners
.univie	Name der Firma
.ac	academic
.at	austria

Dienste – DNS Ablauf

- Client schickt einen DNS-Request an seinen DNS-Server
- DNS-Server „frägt“ einen Root-Server, welche DNS-Server für die TLD zuständig sind
- …(SLD, bis zur IP des Rechners)
- DNS-Server schickt den DNS-Reply zum Client

Dienste – DHCP

- Dynamic Host Configuration Protocol
- RFC 2131
- UDP, Port 67 und 68
- Protokoll zur automatischen Vergabe von IP-Adressen in einem LAN
- Sicherheitsrisiko!

Dienste – DHCP Ablauf1

- Client schickt einen Anfrage als Broadcast in das LAN (DHCPDISCOVER)
- DHCP-Server antwortet mit den Netzwerkparametern (IP, Default Gateway, DNS, …) für den Client (DHCPOFFER)

Dienste – DHCP Ablauf2

- Client schickt einen Request mit den gewählten Parametern (DHCPREQUEST)
- Server schickt eine Bestätigung (DHCPACK) oder eine Ablehnung (DHCPNACK)

IPv6 SLAAC

- StateLess Address Auto Configuration
- Keinerlei manuelle Konfiguration
- Kein Serverdienst notwendig
- Clients konfigurieren ihre IPv6-Adresse an Hand von Router Advertisments
- Vorgabe des Präfixes durch den Router
- Rest aus der Interface ID

Stateful DHCPv6

- Die Adresszuordnung erfolgt zentral
- 2 Varianten
  - Rapid Commit (nur „Solicit“ und „Reply“)
  - Normal Commit (alle 4 Nachrichten)
- Default: Normal Commit
- Rapid Commit muß am Server und am Client konfiguriert werden

DHCPv6 Message Types 1

DHCPv6 Message Type	DHCPv4 Message Type
SOLICIT	DHCPDISCOVER
ADVERTISE	DHCPOFFER
REQUEST, RENEW, REBIND	DHCPREQUEST
REPLY	DHCPACK/DHCPNAK
RELEASE	DHCPRELEASE
INFORMATION-REQUEST	DHCPINFORM
DECLINE	DHCPDECLINE
CONFIRM	-
RECONFIGURE	DHCPFORCERENEW
RELAY-FORW, RELAY-REPLY	-

DHCPv6 Message Types 2

- SOLICIT — Client: Locate DHCP Servers
- ADVERTISE — Server: Hier ist ein DHCP Server
- REQUEST — Client: Brauche Information
- RENEW — Client: Informationserneuerung
- REBIND — Client: Brauche Infos weiterhin
- REPLY — Server: Hier die Informationen
- RELEASE — Client: Brauche Infos nicht mehr

DHCPv6 Message Types 3

- INFORMATION-REQUEST: Client: Brauche Infos aber keine IPv6 Adresse
- DECLINE Client: Verweigere Updateinfo
- CONFIRM Client: Infos werden verwendet
- RECONFIGURE Server: Infos haben sich geändert
- RELAY-FORW Relay: Nachrichtenweiterleitung
- RELAY-REPLY Server: Nachricht zum Weiterleiten

Stateless DHCPv6

- Für den SLAAC-Prozeß können Zusatzinformationen bereitgestellt werden (z.B.: DNS Server)

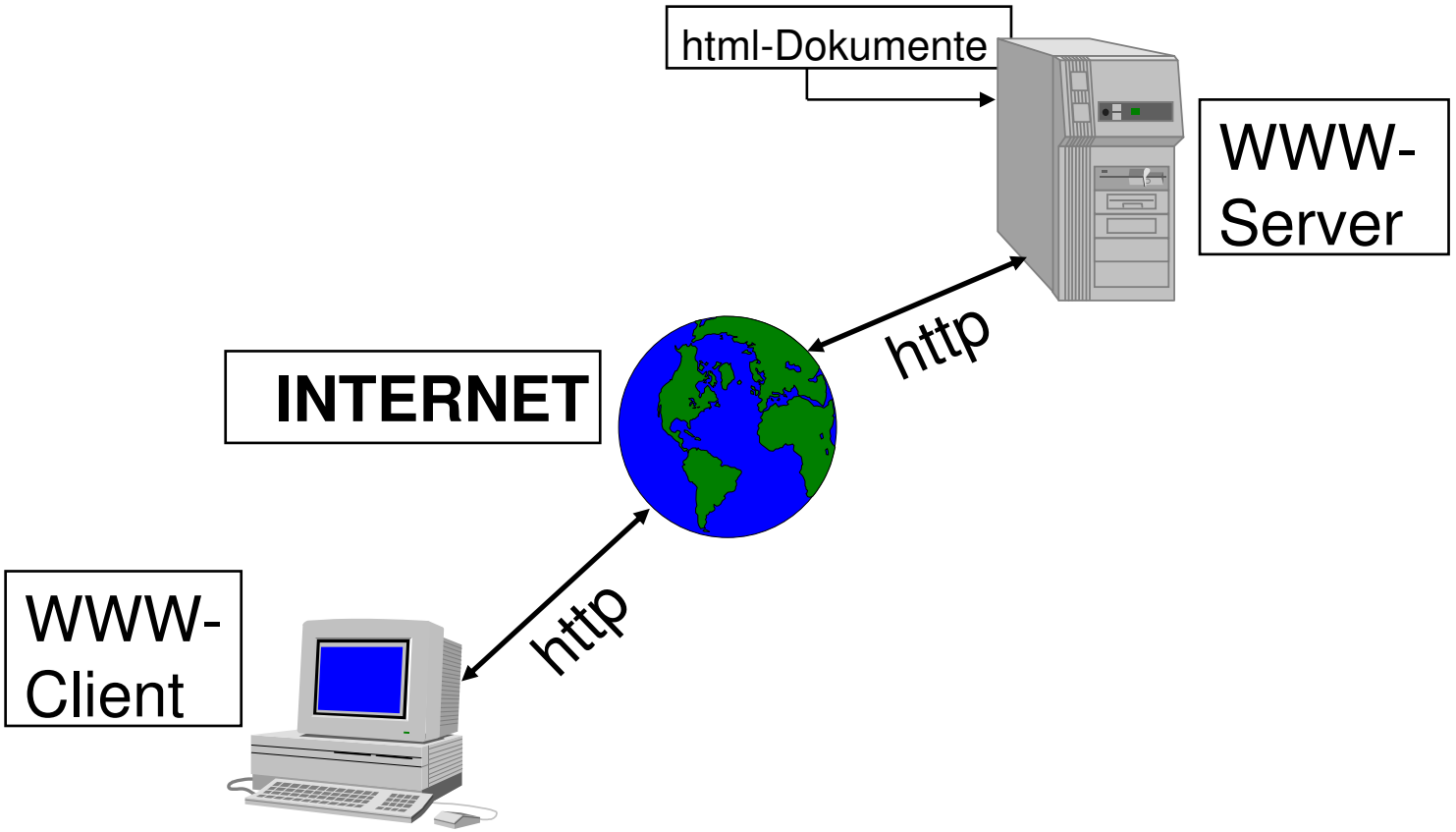
Dienste – WWW

- Grundbegriffe
  - Hypertext
  - Hyperlink
  - Hypermedia
- 1989 am CERN entwickelt
- 1. Browser MOSAIC $\rightarrow$ Navigator
- HTTP – HyperText Transfer Protocol
- RFC 1945 (V1.0) und 2616 (V1.1)

Dienste – WWW

- Webserver stellen über HTTP Informationen in standardisierter Form (HTML) zur Verfügung
- Webbrowser stellen diese dar
- Layoutkontrolle grundsätzlich am Client (Browser), d.h. Angepaßt an die Fähigkeiten des Clients

Dienste – WWW - Überblick



Dienste – WWW-Server

- Apache HTTP Server
  - Apache Software Foundation
- IIS (Internet Information Server)
  - Microsoft
- …
  - CERN httpd
  - lighttpd

Dienste - Webbrowser

- Browser
  - Mozilla Firefox (Open Source)
  - Google Chrome
  - Microsoft Internet Explorer (Microsoft)
  - Safari (Apple)
  - Opera (Opera)
  - Lynx (Open Source, textbasierend)
  - …
- Apps

Dienste – WWW – Dynamik

- Dynamische Inhalte Serverseitig
  - SSI
  - Scripts (CGI, Perl, PHP, ASP, JSP, ...)
  - Datenbankanbindung
- Dynamische Inhalte Clientseitig
  - Scripts (Javascript, Active X)
  - Bilder (Animated GIFs, Flash, ...)

Dienste – WWW – Proxy

- Zweck: Bessere Nutzung der Bandbreite durch Zwischenspeicherung
- Nur bei statischen Seiten effizient
- Sicherheitsüberlegungen können ebenfalls zum Einsatz führen
- Überwachung des Surfens und Sperre von Seiten möglich

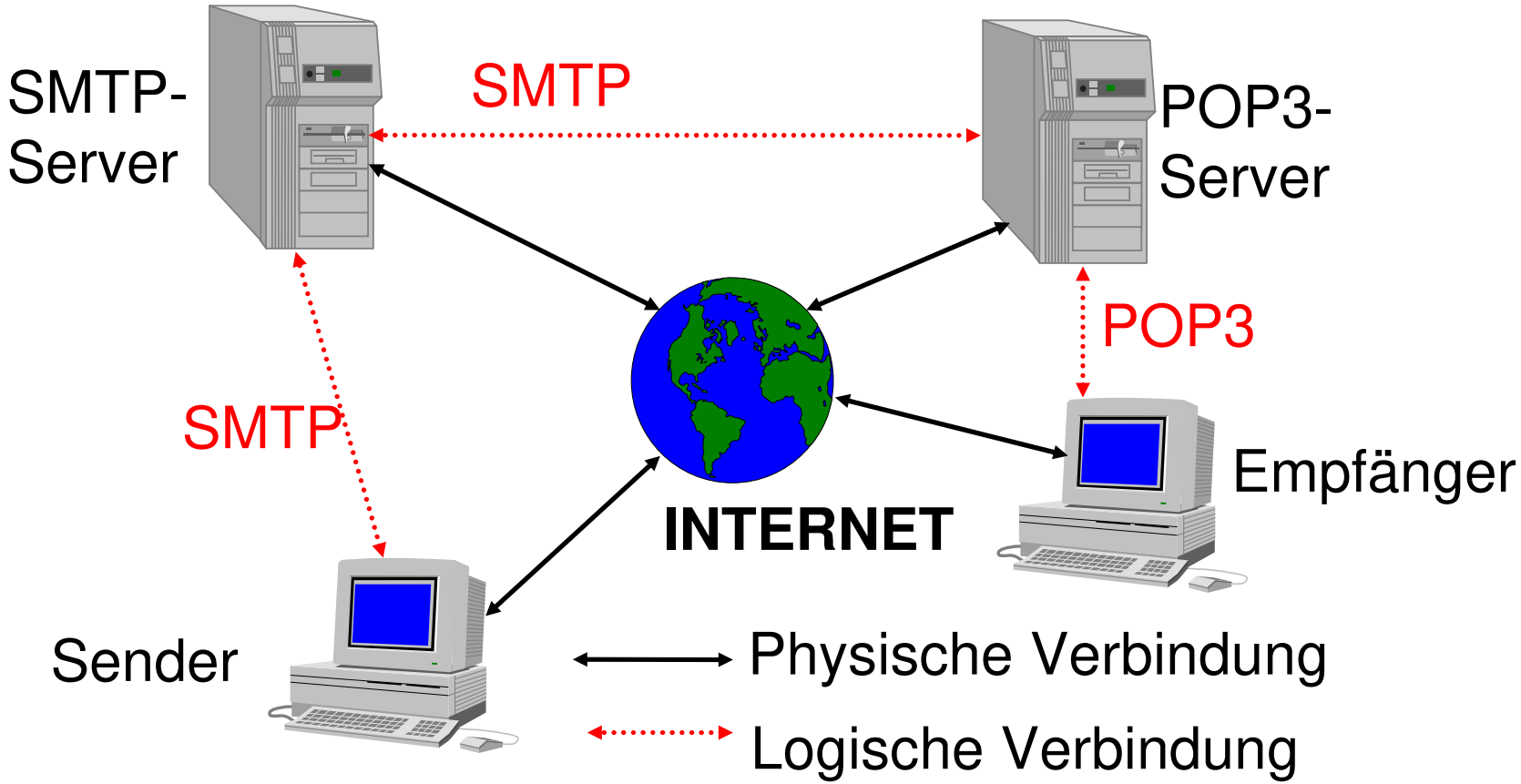
Dienste – WWW VT/NT

+ Benutzerfreundliche Oberfläche
+ Nutzung verschiedenster Dienste mit einem Client
+ Einfache Suchmöglichkeit
- Kein Vorausschau auf zu erwartende Wartezeit
- „Verlaufen“ im Cyberspace

Dienste – e-Mail

- Ältester Dienst im Internet
- Ursprünglich nur ASCII-Texte (7-Bit-Code)
- Formatierungen problematisch
- Ausführlicher Mailheader
- MIME-Codierung

Dienste – e-Mail Funktionsweise



Dienste – e-Mail

- Senden immer per SMTP von e-Mail-Client zum eigenen SMTP-Server (vom Provider)
- Empfangen auf mehrere Varianten vom Postfach beim eigenen Mailserver
  - POP3 (APOP)
  - IMAP4

Dienste – e-Mail Daten

Notwendige Informationen zum Einrichten des Dienstes:

- Generelle Informationen
- Empfangsinformationen
- Sendeinformationen

Dienste – e-Mail Daten 2

- Generelle Information
  - die eigene e-Mail-Adresse
  - Optional Name
  - Optional Firmen-/Organisationsinformationen
  - Optional Rückantwortadresse
  - Optional Unterschriftendatei

Dienste – e-Mail Daten 3

- Empfangsinformationen
  - Empfangsart (POP, IMAP)
  - POP/IMAP-Server
  - Accountname und Passwort
  - Sicherheitseinstellungen
  - Optionale weitere dienstabhängige Parameter

Dienste – e-Mail Daten 4

- Sendeinformationen
  - SMTP-Server
  - Sicherheitsparameter (TLS, SSL, Port)
  - Eventuell notwendige Zugangsdaten (Name/Passwort)
  - Optionale weitere Parameter (versetztes Senden, ...

Dienste – e-Mail Programme

- Outlook (Microsoft)
- Thunderbird (Mozilla)
- Pegasus (David Harris)
- elm (Open Source)
- pine (Open Source)
- Mutt (Open Source)
- …

Dienste – e-Mail TCP-Ports

- SMTP
  - 25 Standardport
  - 465 SMTP over SSL
  - 587 SMTP TLS
- POP3
  - 110 Standardport
  - 995 POP3 over SSL
- IMAP4
  - 143 Standardport
  - 993 IMAP over SSL

Dienste – e-Mail VT/NT

+ Schnelle Nachrichtenübermittlung (im Vergleich zu snail-Mail)
+ Einfache Weiterverarbeitung der Nachrichten möglich
- Unzureichender Datenschutz
- Keine zentralen e-Mail-Verzeichnisse

Dienste – Listserver

- Verwaltet Listen von e-Mail-Adressen zu verschiedenen Themen
- Offene Listen
- Moderierte Listen
- E-Mail an die Liste bewirkt Versendung an alle Teilnehmer der Liste

Dienste – Listserver - Eintragen

- Nachrichtenformat muß strikt eingehalten werden , da automatische Verarbeitung erfolgt.
- Mail an den Verwalter der Liste (meist majordomo)
- Betreff: i.a. leer
- Text der Nachricht: subscribe <liste>

Dienste – Listserver - Austragen

- Nachrichtenformat muß strikt eingehalten werden , da automatische Verarbeitung erfolgt.
- Mail an den Verwalter der Liste (meist majordomo)
- Betreff: i.a. leer
- Text der Nachricht: unsubscribe <liste>

Dienste – FTP, SFTP

- (Secure) File Transfer Protocol/Program
- Dateitransfer über das Netz
- Eigentliche Benutzername und Passwort notwendig
- Meist aber mit Benutzername anonymous und als Passwort die eigene e-Mail-Adresse möglich

Dienste – FTP Funktion

- RFC 354
- Steuerkanal (Port 21) zum Aushandeln des Transfers
- Datenkanal vom Server gesteuert (außer im PASSIV-Mode; Port 20), daher im Zusammenhang mit Firewalls und NAT problematisch

Dienste – FTP, SFTP 2

- Bei den Betriebssystemen nur Commandline-Programm enthalten
- Z.B.: <START> <AUSFÜHREN>

  FTP <rechnername>
- Graphische Varianten von Drittanbietern verfügbar
- Für den privaten Gebrauch oft kostenlos

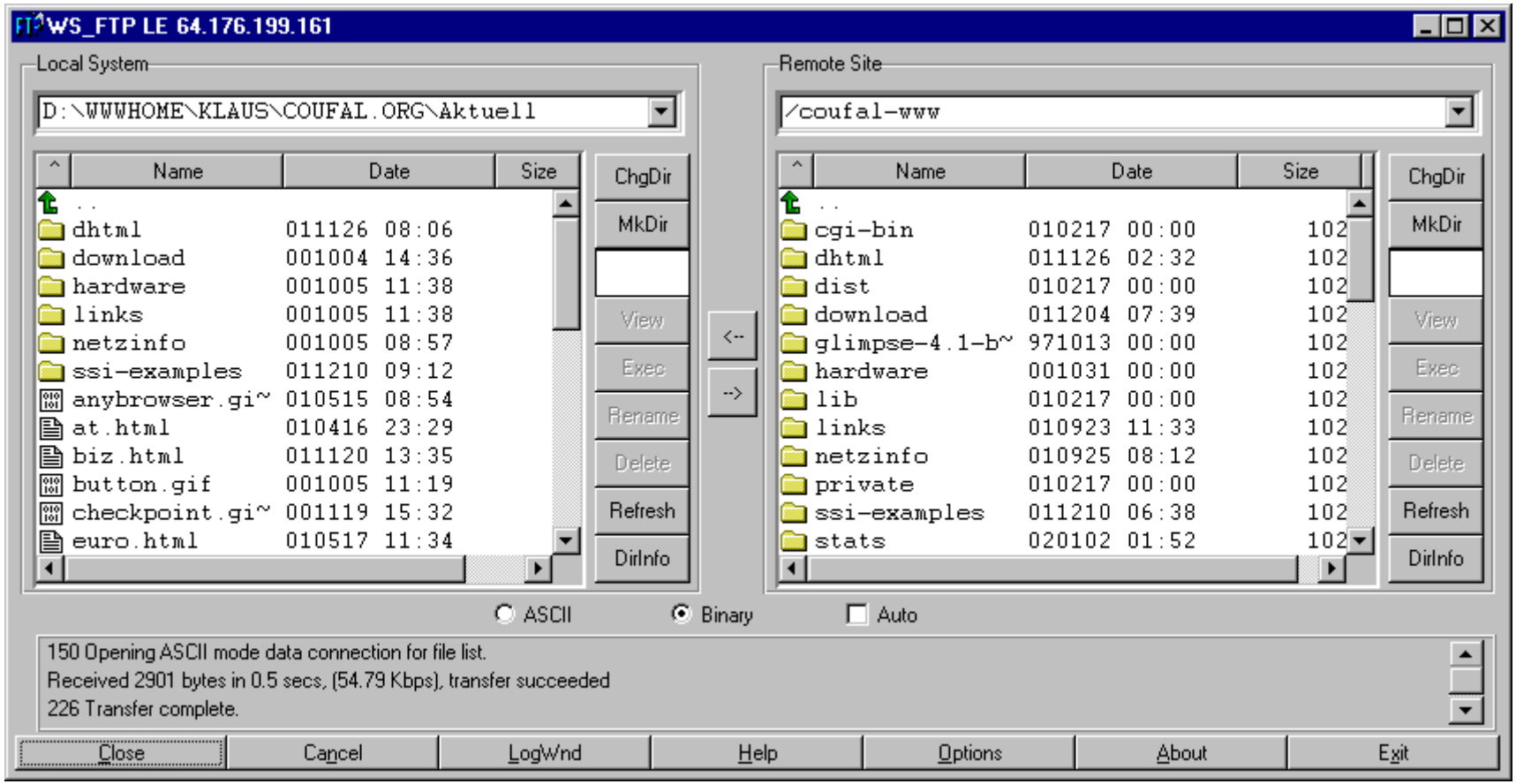
FTP-Commands

- OPEN <server>
- USER <user> (Abfrage nach Passwort)
- GET remote-filename local-filename
- PUT local-filename remote-filename
- BINARY/ASCII
- CLOSE/QUIT/BYE
- DIR/LS

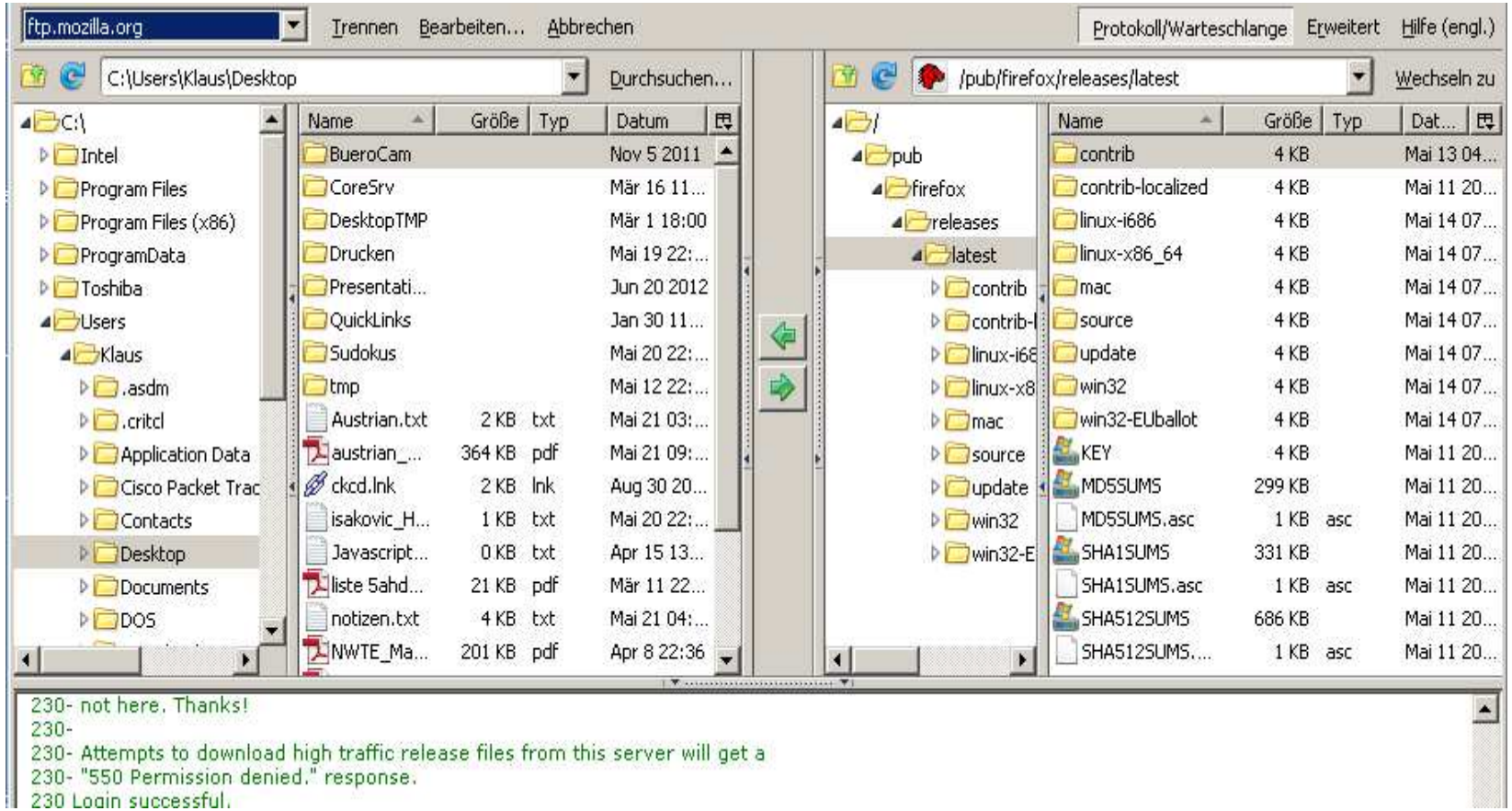
Dienste – FTP graphisch

- Vorkonfigurierbare Sitzungen
  - Servername, Username und Password
  - Startverzeichnis lokal und remote
  - Automatische Übertragungsmodi
- Komplett Mausbedienbar
- Diverse Zusatzfunktionen (Ansehen von remote Dateien)

Dienste – FTP graphisch



Dienste – FTP Browser



Dienste – FTP Übertragung

ASCII	Für Text, dabei werden Anpassungen in der Zeilenschaltung vorgenommen
BINARY	Für Binärdateien, hier werden keine Anpassungen vorgenommen
PASSIV	Verbindung wird vom Client aufgebaut

Dienste – FTP → SFTP

- Die leichte Abhörbarkeit einer FTP-Verbindung hat dieses Protokoll in Verruf gebracht
- Secure FTP verwendet eine SSH (siehe unten)-Verbindung für die Übertragung und erreicht damit eine wesentlich höhere Sicherheit.

Dienste – FTP VT/NT

+ Einfache Art Dateien zu kopieren
+ Wenige Befehle
+ Riesige Datenbestände
+ Oft lokaler Mirror eines interessanten Datenbestandes vorhanden
- Unzureichender Datenschutz, daher nur anonym zu empfehlen bzw. SFTP

Dienste – Telnet, SSH

- Anmelden an einen entfernten (remote) Rechner
- Danach verläuft die Arbeit, so als würde direkt an diesem Rechner gearbeitet werden
- Daher auch die Bedienung des Rechner mit dessen Befehlen (häufig UNIX)

Dienste – Telnet

- Die Daten inklusive der Anmeldedaten werden im Klartext übertragen und können daher leicht abgehört werden.
- Fernadministration von praktisch allen Multiusersystemen möglich.
- Z.B.: <START> <AUSFÜHREN> TELNET <rechnername>

Dienste – SSH

- Schutz der übertragenen Daten durch Verschlüsselung
- In den WIN32-Systemen nicht standardmäßig implementiert
- Free Client für Win32: PuTTY
- Nur zu Rechnern mit einem SSH-Server möglich

Dienste – Telnet VT/NT

+ Einfacher Zugang auf einen entfernten Rechner
+ Auf den Zielrechner die auf diesem Rechner gewohnten Befehle
- Unzureichender Datenschutz

Dienste – News

- Weltweites Diskussionsforum
- Analog den schwarzen Brettern, daher einfach in der Bedienung, häufig in die e-Mail-Clients integriert
- Durch den hierarchischen Aufbau kann der Überblick über die Themenvielfalt bewahrt werden

Dienste – News

- NNTP
- Newsgroup
- News-Reader
- Posten, Posting
- Followup

Dienste – News VT/NT

+ Weltweit Artikel zu fast allen Themen vorhanden
+ Verteilte Speicherung, daher sinnvolle Zugriffszeiten
- „Spreu vom Weizen zu trennen“ nahezu unmöglich

III.2. Verzeichnisdienste

- Verzeichnisdienst - Was ist das?
- Warum?
- Vorteile für den Benutzer
- Vorteile für den Administrator
- Standards

Was ist ein Verzeichnisdienst?

- Ein zentraler Informationsspeicher der Netzwerkumgebung
- Nicht gebunden an einen oder mehrere physikalische Standorte
- Hierarchisch aufgebaut
- Plattformunabhängig
- Standardisiertes Zugriffsprotokoll

Beispiel DNS

- Im Internet wird – meist transparent – der DNS-Dienst für die Zuordnung von DNS-Namen zu IP-Adressen verwendet.
- Plattformunabhängig, hierarchisch, standardisiert
- Nur eine Aufgabe

Aufbau

- Container
  - Firma, Abteilung, ...
- Objekte
  - Benutzer, Server, ...
- Eigenschaften
  - Werte der Objekte (z.B.: e-Mailadresse eines Benutzers, ...)

Anforderungen

- anpaßbar an Firmenstruktur
- Integration aller Netzwerkkomponenten
- Standardobjekttypen (User, Drucker, ...)
- freie Objekttypen
- Sinnvolle Standardattribute (e-Mail, ...)
- Definition freier Attribute

Warum Verzeichnisdienste?

- Reduktion der Benutzer- bzw. Ressourcenverwaltung
  - e-Mail-Systeme
  - Netzwerbetriebssysteme
  - Anwendungsprogramme
- Vereinheitlichung der Parameter und der Suche danach

Ressourcen

- Dateien
- Verzeichnisse
- Datenbanken
- Dienste
- Druckerwarteschlangen
- Drucker
- Speichereinheiten
- Gateways
- Server
- Arbeitsstationen
- Anwendungen
- ...

Angaben (Beispiele)

- Mitarbeitern
  - (Name, Adresse, Telephonnummer, ...)
- Ressourcen
  - (Drucker: Standort, Fähigkeiten, ...)
- Zugriffsmöglichkeiten
- Zugriffsrechte
- Verfügbare Anwenderdienste

Einsatzmöglichkeiten

- Wie ist die Telephonnummer von X?
- Wie lautet die e-Mail-Adresse von y?
- Wo ist die Anwendung z?
- Wie melde ich mich an die Datenbank abc an?
- Wo ist der aktuelle Geschäftsbericht?
- Wo ist ein Farbdrucker?
- ...

Nachteile für den Benutzer

- Umstellung auf ein neues System
- Namen gewohnter Dienste können länger werden, da sie in einem Kontext gesehen werden müssen

Vorteile für den Benutzer

- Einfache Abfrage von Informationen zu einem Objekt
- Nur ein(?) Passwort
- Keine Notwendigkeit über Änderungen im Netz informiert zu werden (Änderung von Speicherplätzen, Faxdiensten, ...)
- Transparenter Zugriff auf Objekte

Nachteile für den Administrator

- Umstellung

Vorteile für den Administrator

- „Single Point of Administration“
- Änderungen in der Netzwerkinfrastruktur bleiben für den Benutzer transparent
- Weniger Benutzerunterstützung notwendig

Standards

- ISO/IEC 9594/ITU-TS X-500
  - Basisnorm für alle Verzeichnisdienste
- ENV 41210
  - DAP (Directory Access Protocol)
- LDAP (Lightweight DAP)
  - Derzeitiger Defacto-Standard mit dem verschiedene Verzeichnisdienste kommunzieren

X.500

- DIT (Directory Information Tree)
- DN (Distinguished Name)
  - global eindeutig
- RDN (Relative Distinguished Name)
- CN (Common Name)
- @c=AT@o=SPG@ou=EDV@cn=xyz

LDAP

- Defacto-Standard für die Kommunikation verschiedener Verzeichnisdienste
- RFC 1777 (März 1995) LDAPv2
- RFC 2251 (Dezember 1997) LDAPv3
- cn=xyz, ou=EDV, o=SPG, c=AT

Übersicht – Verzeichnisdienste

- Laut der US-Vereinigung Network Applications Consortium gibt es nur zwei die den Namen Verzeichnisdienst verdienen:
  - Banyan Streettalk
  - Novell NDS/e-Directory

Übersicht – Verzeichnisdienste 2

- Daneben noch:
  - IBM Secure Directory
  - IBM/Lotus NAB (Namen- und Adressbuch)
  - Microsoft ADS