DHBW Stuttgart

Technik der digitalen Netze
Teil 1 - Einführung

Stephan Rupp
Nachrichtentechnik

www.dhbw-stuttgart.de

Inhalt

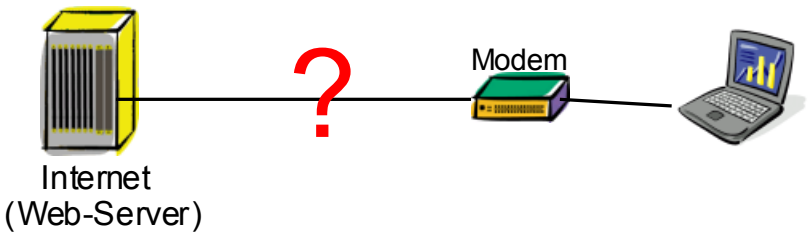
DHBW Stuttgart

Technik der Netze - Einführung

- Netze
- Leitungsvermitlung, Paketvermittlung
- geografische Ausprägung: Lokales Netz und Weitverkehrsnetz (Zugangsnetz, Metronetz, Kernnetz)
- Netztypen: Telefonnetz, CaTV-Netz, Mobilfunknetz, Satelliten

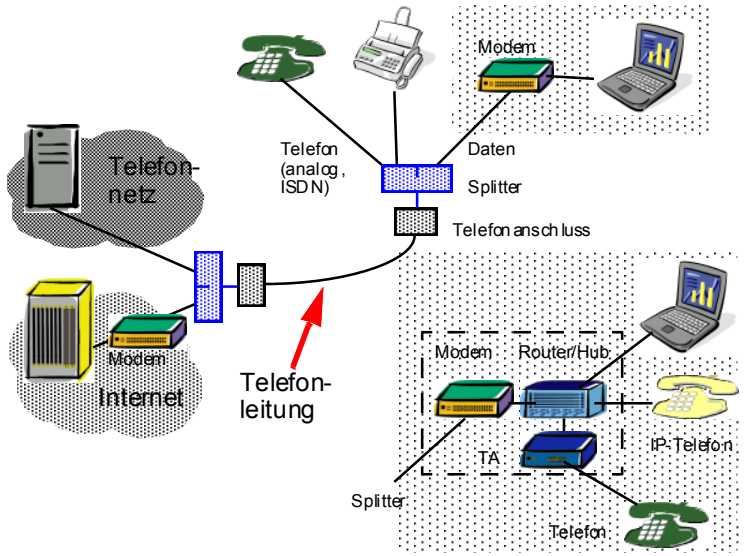
Was wissen wir über Netze?

DHBW Stuttgart



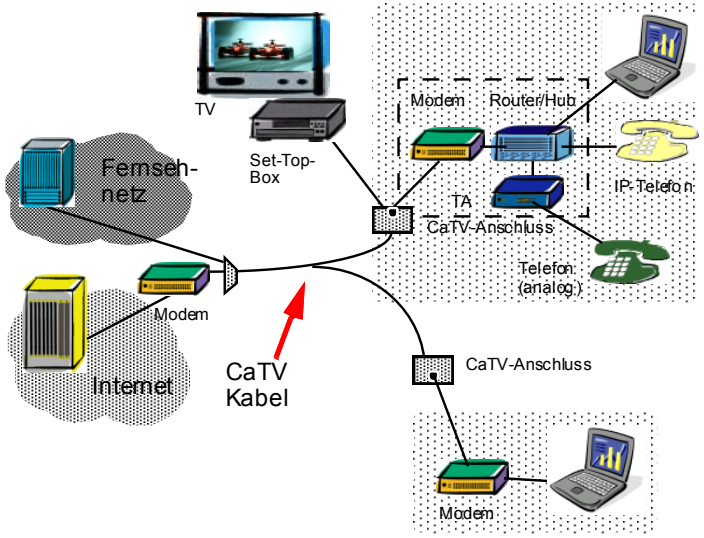
DSL - Was steckt dahinter?

DHBW Stuttgart



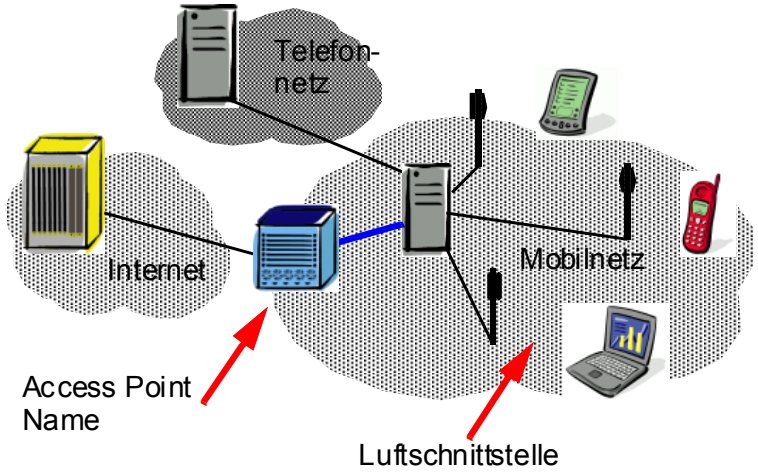
CaTV - Was steckt dahinter?

DHBW Stuttgart



Händi - Was steckt dahinter?

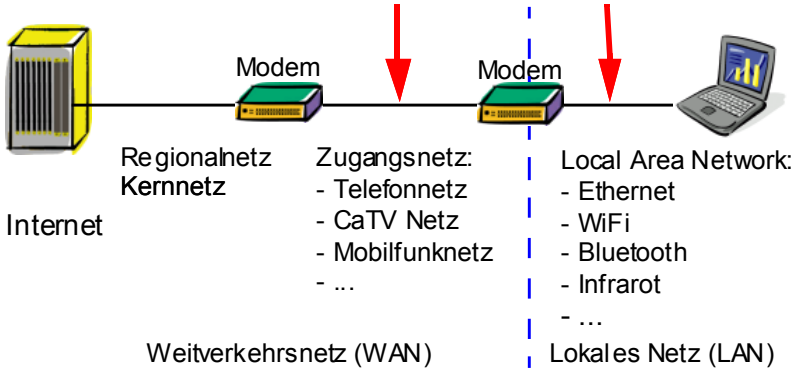
DHBW Stuttgart



Das Strickmuster erkennen

DHBW Stuttgart

Vereinfachung durch Abstraktion



Strickmuster

DHBW Stuttgart

Adressräume als Netze

Schichtenmodell

- Leitungen und Luft
- Modem-Schicht: Punkt-zu-Punkt Verbindungen
- Netzschicht: Zustellung von Paketen bzw. Vermittlung von Verbindungen
- Anwendungsschicht: Ende-zu-Ende Beziehung, vom Netz sieht man nichts mehr

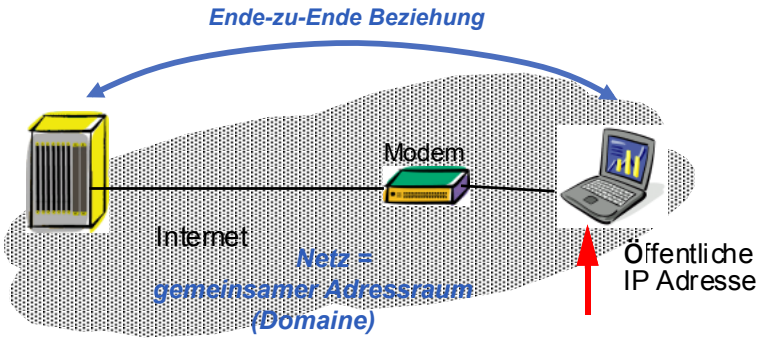
Funktionen, z.B. Mobilitätsverwaltung

- gleiche Funktionen
- viele unterschiedliche Implementierungen

Geografische Netzausprägung

Netze als Wölkchen

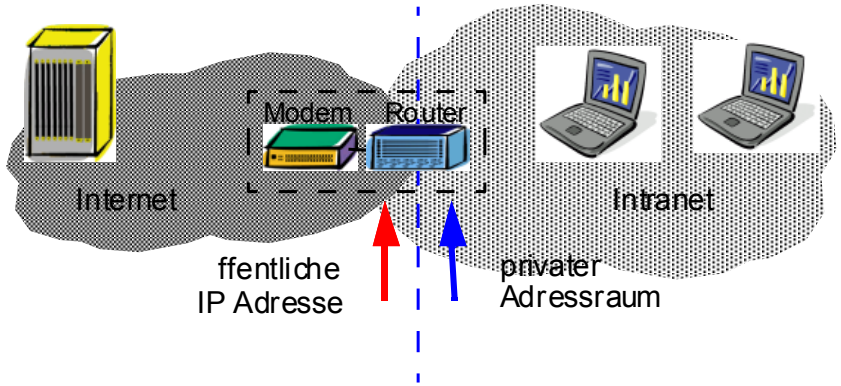
DHBW Stuttgart



Alternative Definition: Netz = Eigentum des Betreibers bzw. einer Firma oder Privatperson (Domaine)

Adressräume spannen Netze auf

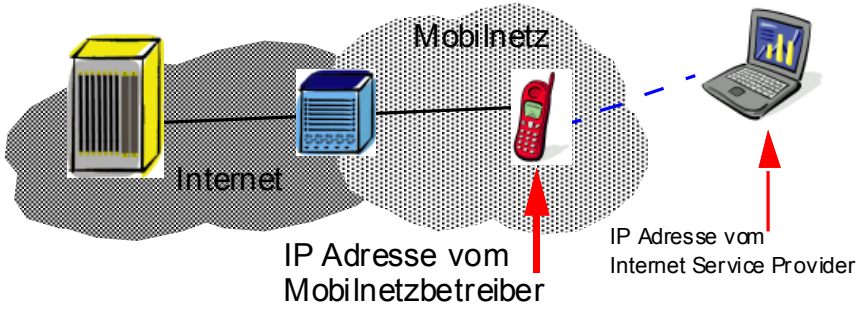
DHBW Stuttgart



Das Händi als Modem

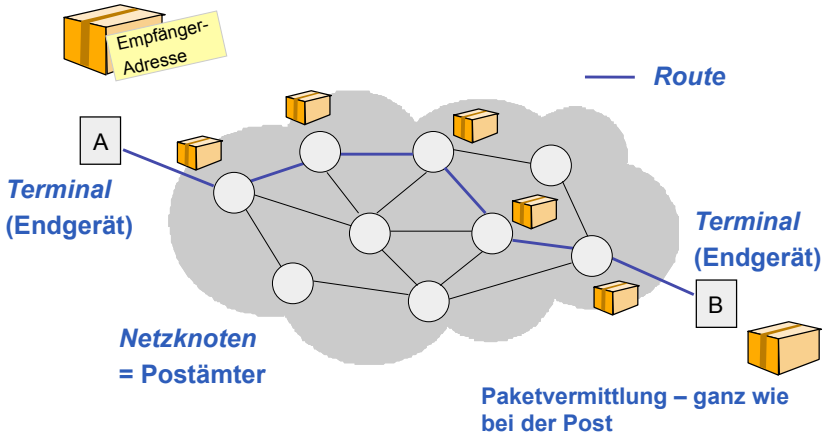
DHBW Stuttgart

In welchem Netz befindet sich das Gerät?



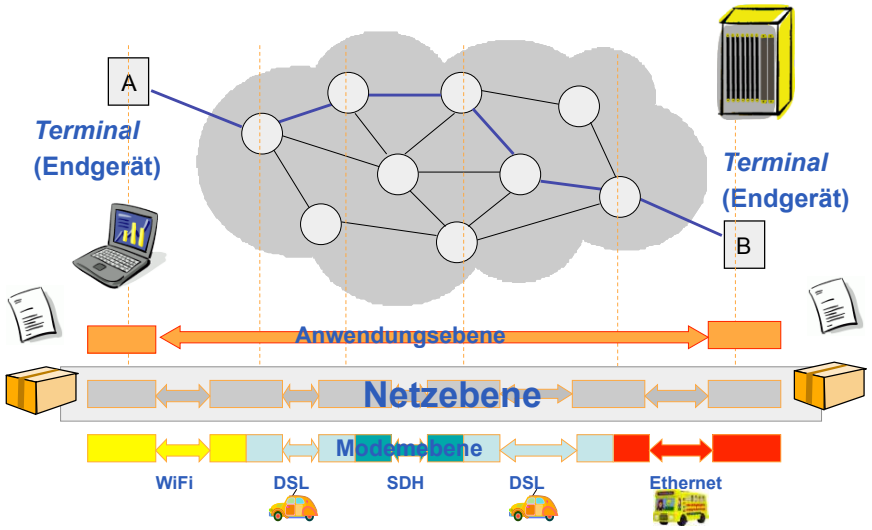
Schichtenmodell – Netzebene

DHBW Stuttgart



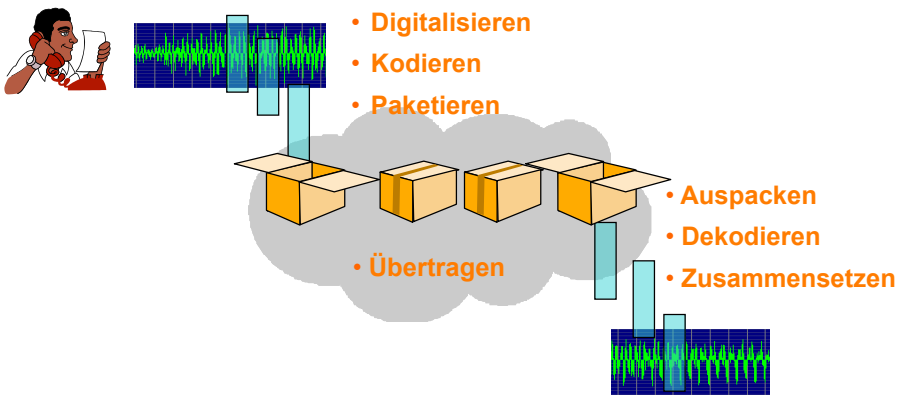
Schichtenmodell

DHBW Stuttgart



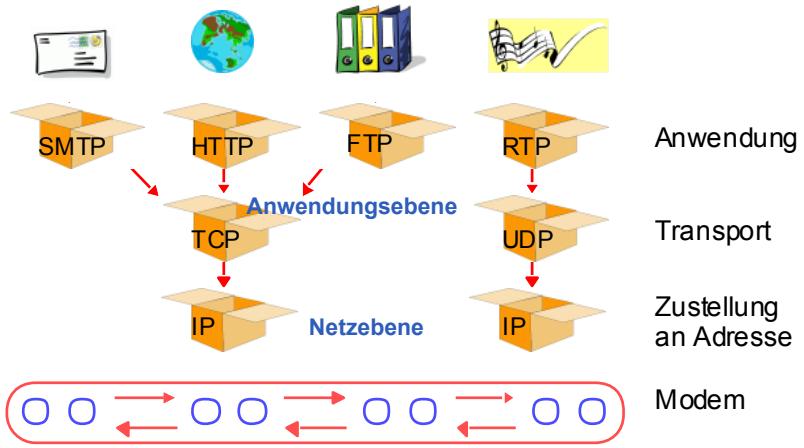
Anwendungsebene - Sprachpakete

DHBW Stuttgart



Schichtenmodell - Internet

DHBW Stuttgart



Ganz unten durch: Leitungen und Luft

Schichtenmodell

DHBW Stuttgart

Pizzaservice oder Containerdienst?

Paketvermittlung

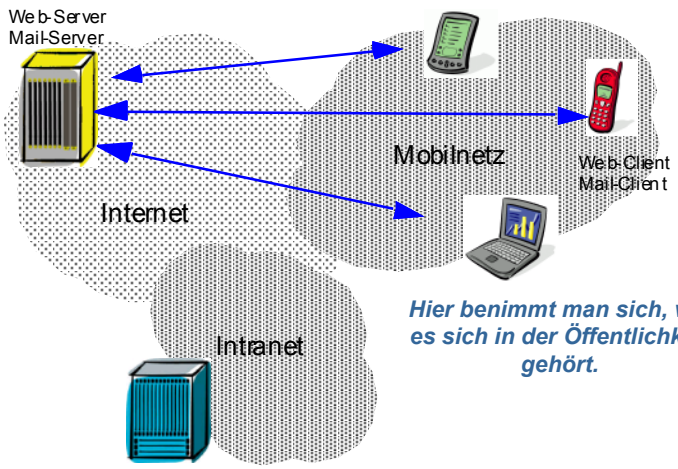
Container Service

Containerdienst

Wege:
Leitungen oder Luft

Öffentlicher Verkehr

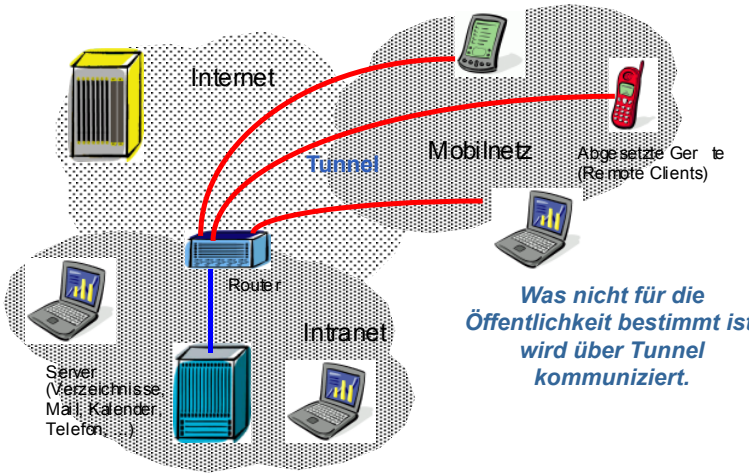
DHBW Stuttgart



Hier benimmt man sich, wie es sich in der Öffentlichkeit gehört.

Privater Verkehr: Tunnel (VPN)

DHBW Stuttgart



Was nicht für die Öffentlichkeit bestimmt ist, wird über Tunnel kommuniziert.

Das kennen wir jetzt:

DHBW Stuttgart

Schichtenmodell

Netze als Wölkchen

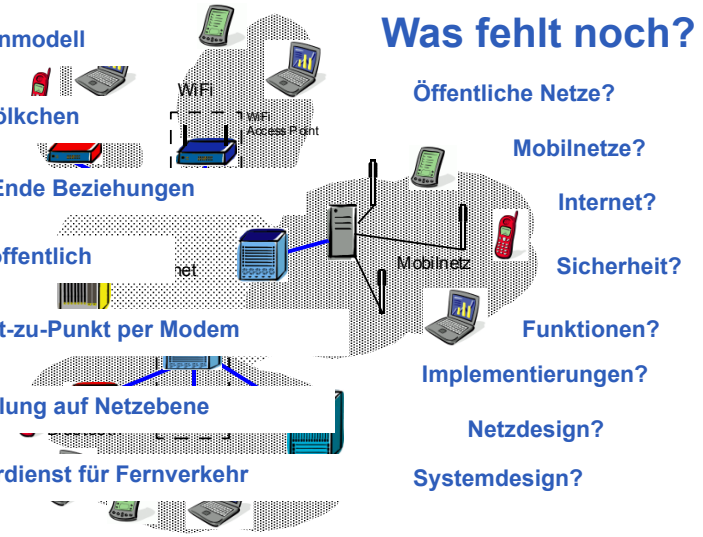
Ende-zu-Ende Beziehungen

Privat und öffentlich

Punkt-zu-Punkt per Modem

Paketvermittlung auf Netzebene

Containerdienst für Fernverkehr



Was fehlt noch?

Öffentliche Netze?

Mobilnetze?

Internet?

Sicherheit?

Funktionen?

Implementierungen?

Netzdesign?

Systemdesign?

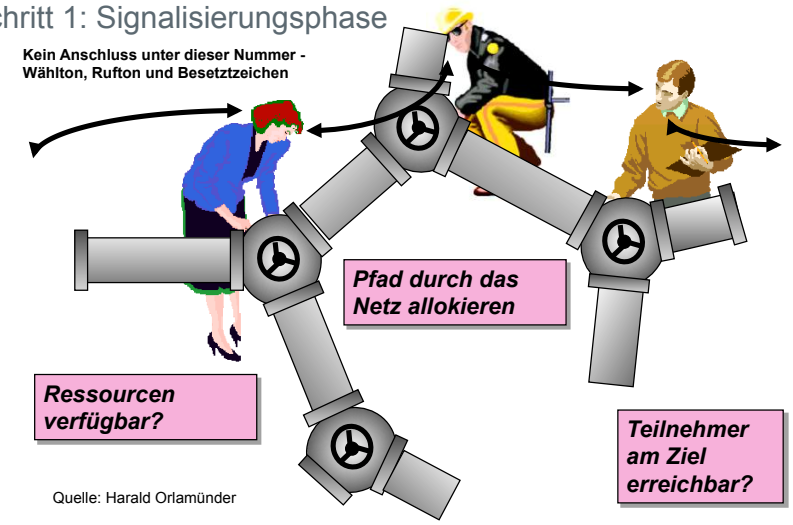
Inhalt

DHBW Stuttgart

Technik der Netze - Einführung

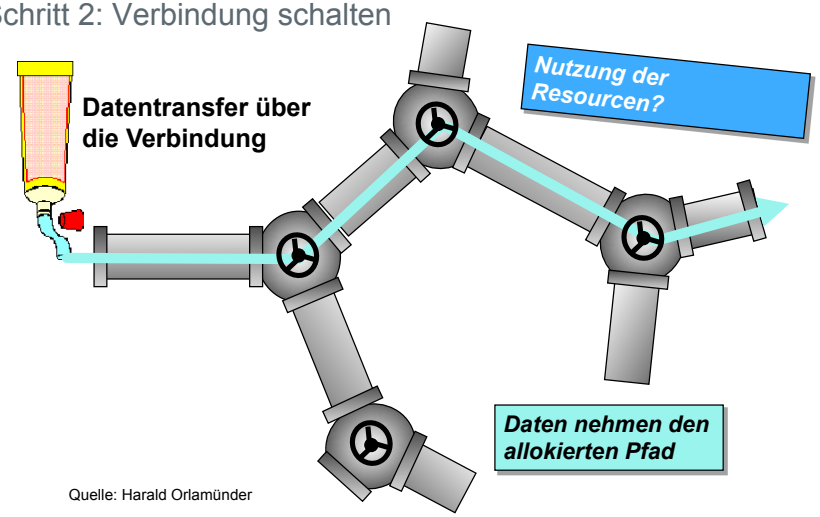
- Netze
- Leitungsvermitlung, Paketvermittlung
- geografische Ausprägung: Lokales Netz und Weitverkehrsnetz (Zugangsnetz, Metronetz, Kernnetz)
- Netztypen: Telefonnetz, CaTV-Netz, Mobilfunknetz, Satelliten

Schritt 1: Signalisierungsphase



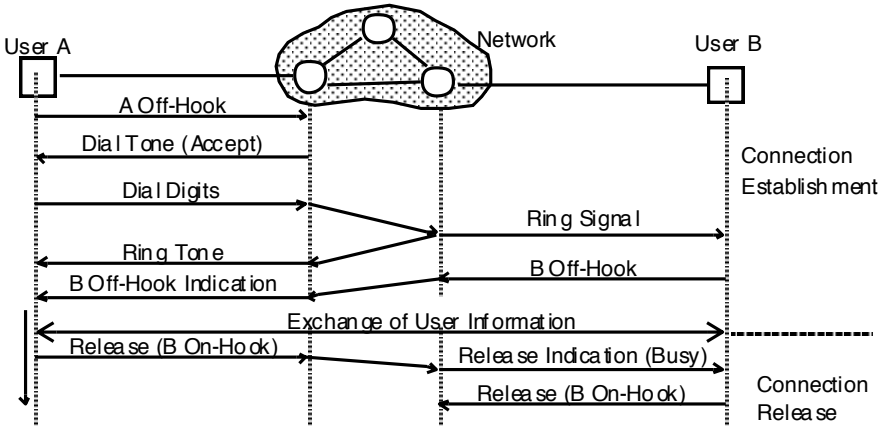
Quelle: Harald Orlamünder

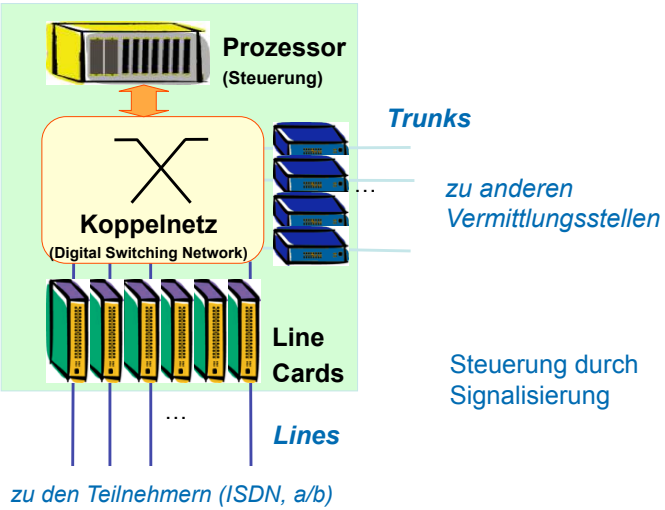
Schritt 2: Verbindung schalten



Quelle: Harald Orlamünder

Noch einmal: Schritt 1 und Schritt 2

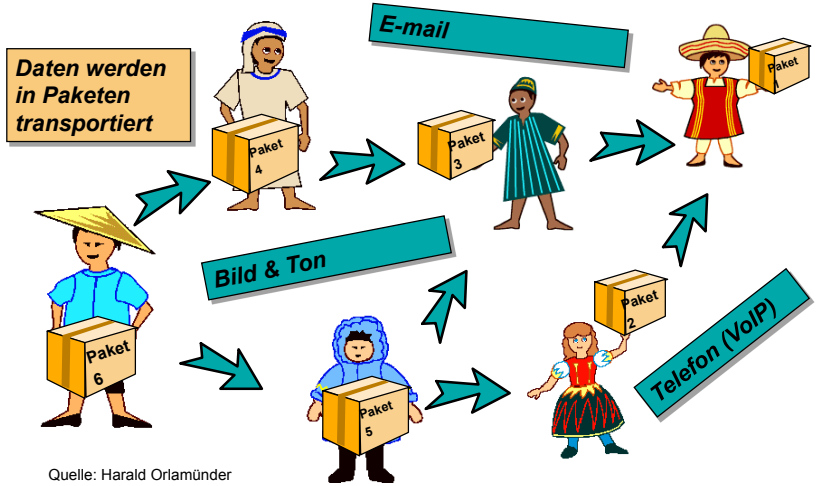




Paketvermittlung

DHBW Stuttgart

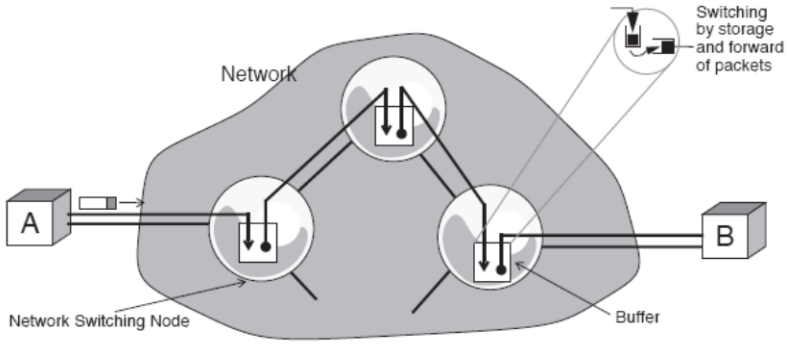
„Fein geschnitten und in Stücken“



Quelle: Harald Orlamünder

Postamt: Storage & Forward Routing

DHBW Stuttgart



Quelle: Gerd Siegmund

Inhalt

DHBW Stuttgart

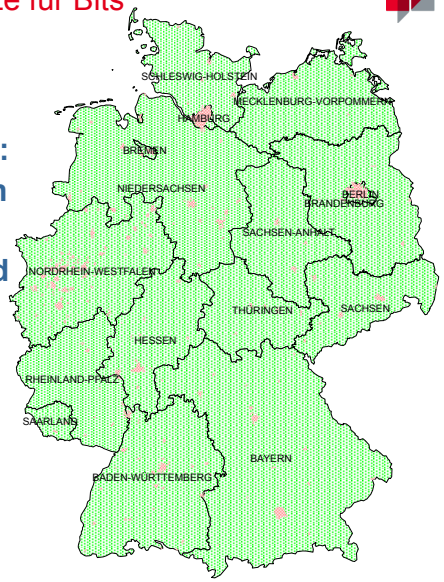
Technik der Netze - Einführung

- Netze
- Leitungsvermitlung, Paketvermittlung
- geografische Ausprägung: Lokales Netz und Weitverkehrsnetz (Zugangsnetz, Metronetz, Kernnetz)
- Netztypen: Telefonnetz, CaTV-Netz, Mobilfunknetz, Satelliten

Verkehrsnetze für Bits

DHBW Stuttgart

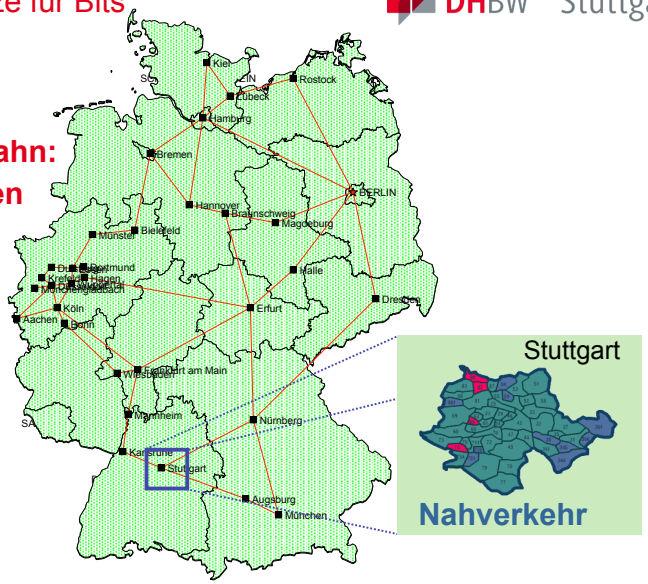
Ein Beispiel: die grössten Städte in Deutschland



Verkehrsnetze für Bits

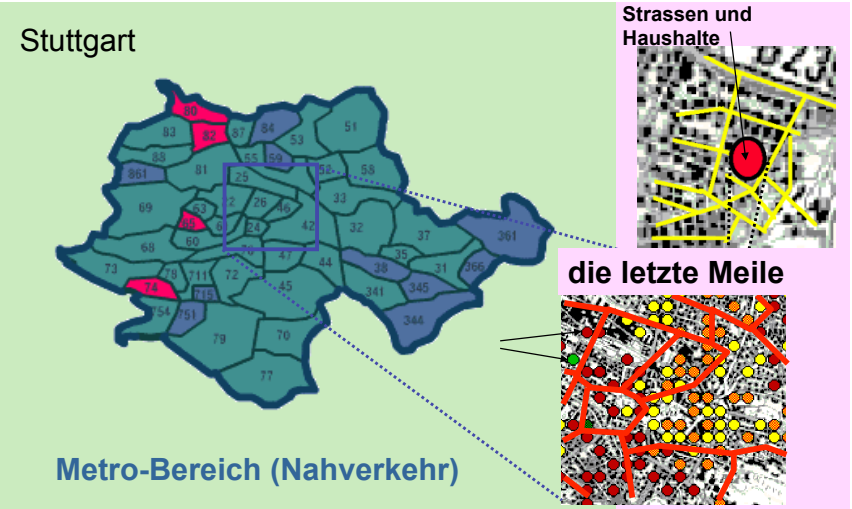
DHBW Stuttgart

Datenautobahn: zwischen den grössten Städten



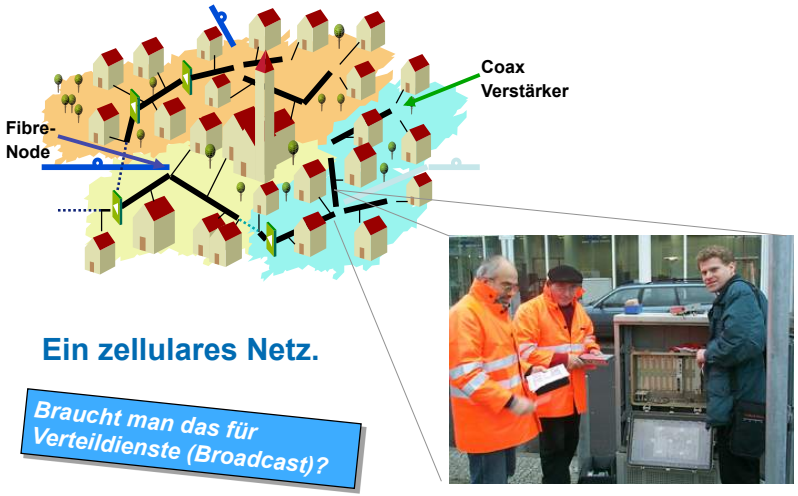
Nahverkehr und letzte Meile

DHBW Stuttgart



Zum Beispiel Kabel-TV Netze

DHBW Stuttgart



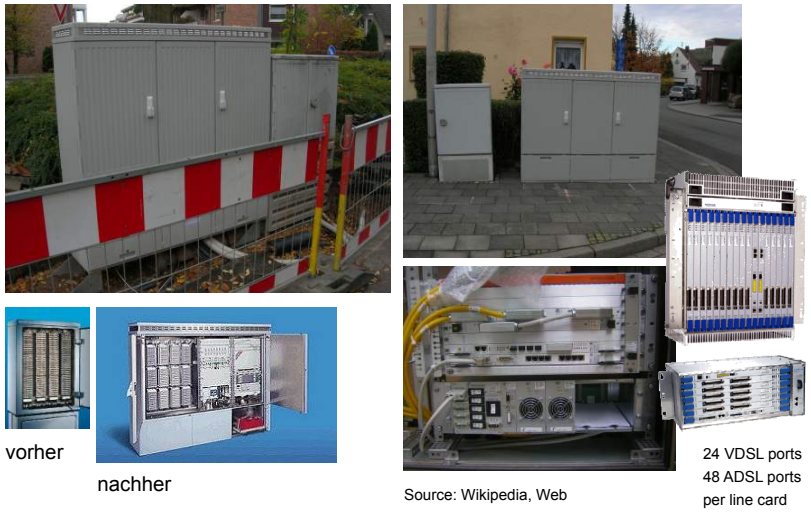
Ein zellulares Netz.

Braucht man das für Verteildienste (Broadcast)?

Quelle: Alcatel

Zum Beispiel DSL-Netze

DHBW Stuttgart



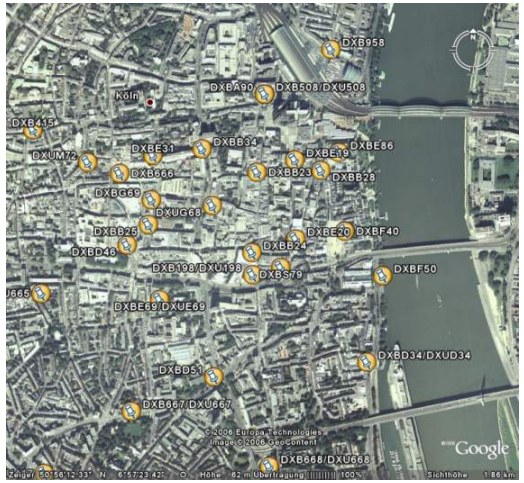
Source: Wikipedia, Web

Zum Beispiel Mobilfunk

DHBW Stuttgart

BTS

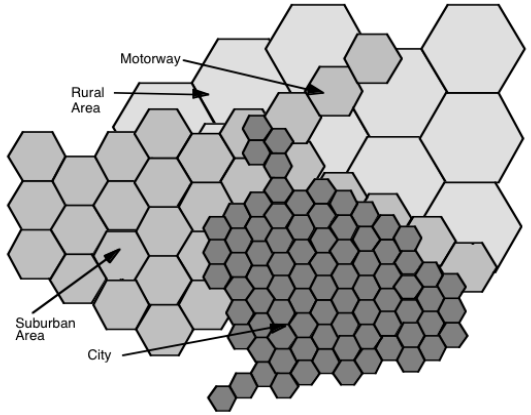
Node B
(BTS)



Quellee: www.duwen.de; vodafone Node B Standorte

Zellulare Netzstruktur

DHBW Stuttgart



Grösse der Zellen ist abhängig von der Verkehrsdichte (bzw. Teilnehmerdichte)

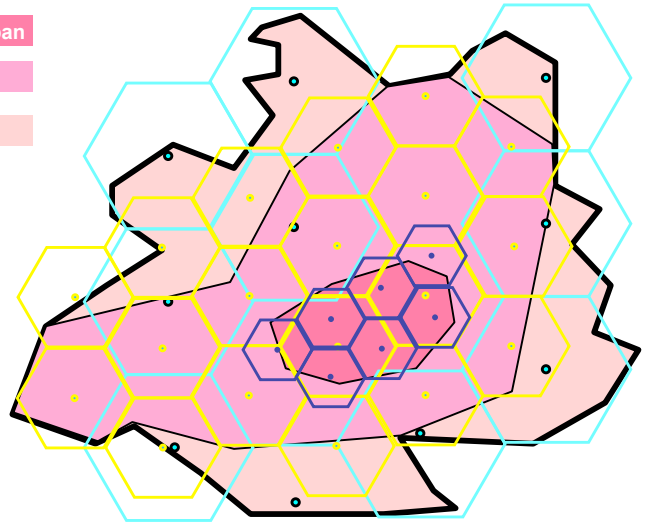
Beispiel: Verkehrsdichte im Metronetz

DHBW Stuttgart

dense urban

urban

rural

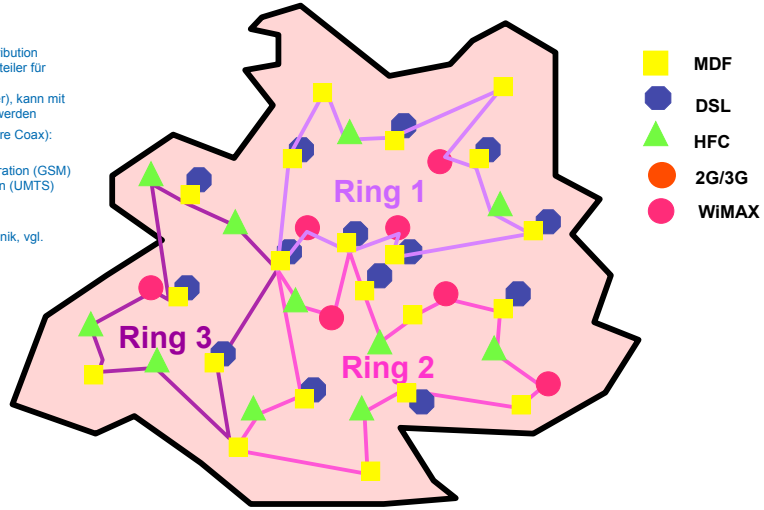


Glasfaserringe als Zubringer

DHBW Stuttgart

Legende:

- MDF (Main Distribution Frame): Hauptverteiler für Telefonleitungen (Kupferdoppelader), kann mit DSL aufgerüstet werden
- HFC (Hybrid Fibre Coax): CaTV Verteilnetz
- 2G/3G: 2. Generation (GSM) bzw. 3. Generation (UMTS) Mobilfunk
- WiMAX: neue Funkzugangstechnik, vgl. WLAN



Beispiel: Metronetz Stuttgart

DHBW Stuttgart

Inhalt

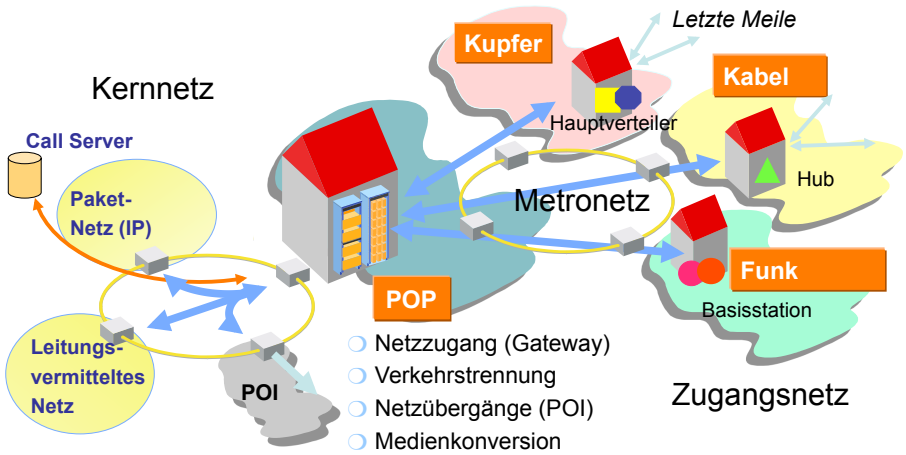
DHBW Stuttgart

Technik der Netze - Einführung

- Netze
- Leitungsvermitlung, Paketvermittlung
- geografische Ausprägung: Lokales Netz und Weitverkehrsnetz (Zugangsnetz, Metronetz, Kernnetz)
- Netztypen: Telefonnetz, CaTV-Netz, Mobilfunknetz, Satelliten

Aufbau der Weitverkehrsnetze

DHBW Stuttgart



POI Point of Interconnect

Von der Datenautobahn bis ins Haus

DHBW Stuttgart

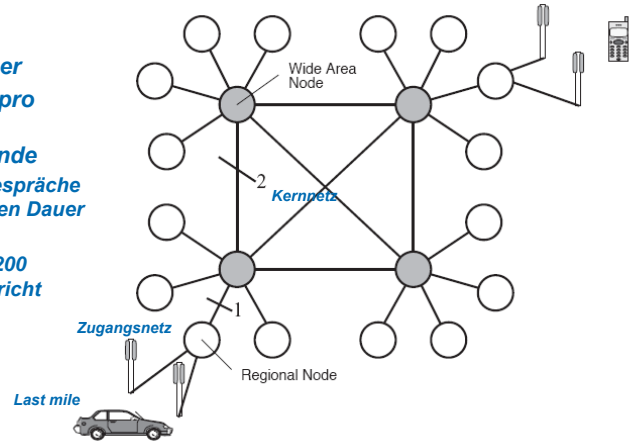
- Die Netze sind sehr unterschiedlich ausgebaut.
- Datenautobahnen (Back-Bones) sind reichlich vorhanden.
- Im Nahverkehr (City-Ringe, Metronetze) gibt es Glasfaser-Infrastruktur in allen größeren Städten.
- In der letzten Meile gibt es unterschiedliche Technologien, die in Deutschland sehr unterschiedlich genutzt werden:
  - Kupferdoppelader (Telefon, DSL): über 12 Millionen Breitbandanschlüsse, ca. 40 Millionen Telefone.
  - CaTV-Netze (Kabelmodem, Kabeltelefon): fast nur als Fernsehverteilnetz genutzt (18 Millionen Haushalte).
  - Mobilfunk der 2. und 3. Generation (GSM/GPRS, UMTS): über 80 Millionen Mobiltelefone, weiteres Wachstum durch Telematik und Maschinen.
  - Hot-Spots (WiFi) und Hot-Zones (WiMAX) für massives Datenaufkommen bzw. hohe Verkehrsdichten

Gymnastik

Netzdesign

Nutzung:

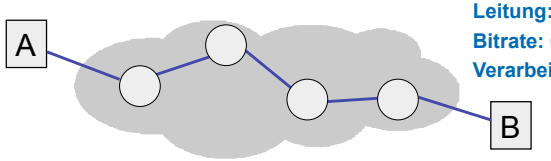
- ***50 Mio. Teilnehmer***
- ***2 Transaktionen pro Teilnehmer in der Hauptverkehrsstunde***
  - ***50% Telefongespräche mit 100 Sekunden Dauer und 64 kBit/s***
  - ***50% SMS mit 200 Bytes pro Nachricht***



Struktur:

- 16 Regionen mit eigenem regionalen Access Point (Regional Node)
- 4 Regionale Access Points pro Weitverkehrsknoten (Wide Area Node)

- Wie viele Daten pro Teilnehmertransaktion?
- Wie viel Verkehr pro Teilnehmer im Mittel?
- Wie viel Verkehr an den Schnittstellen 1 und 2? (Annahme: geschlossenes System mit gleichmässiger Verteilung)
- Bonus-Stretch: “Der hat aber eine lange Leitung”
  - Verzögerungen und Reaktionszeiten (Latency, Round-Trip-Delays) bedingt durch Propagation Delay (Ausbreitungsgeschwindigkeit), Transmission Delay (Bitrate) und Processing Delay (Storage & Forwarding bzw. allgemein die Bearbeitung von Transaktionen).



Leitung: 3.000 km
Bitrate: 64 kBit/s
Verarbeitung: 10 ms pro Hop

Fall 1: 64 Bits an B mit Rückmeldung
Fall 2: 2 MBytes download von B

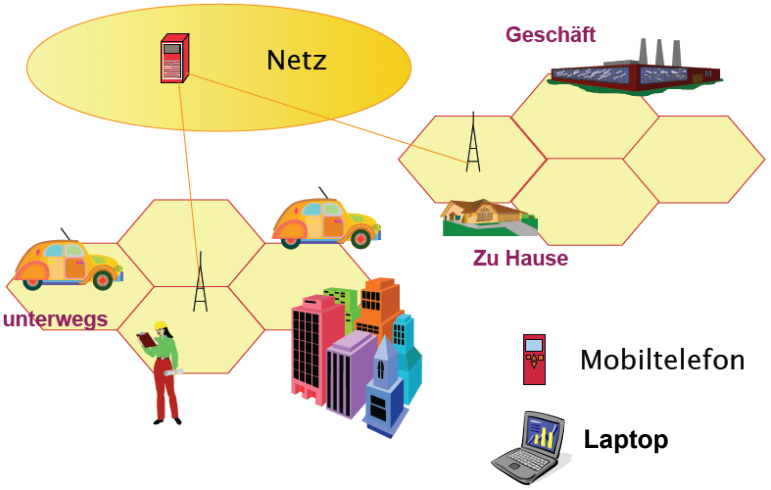
Gymnastik

Mobilität

Mobilität:

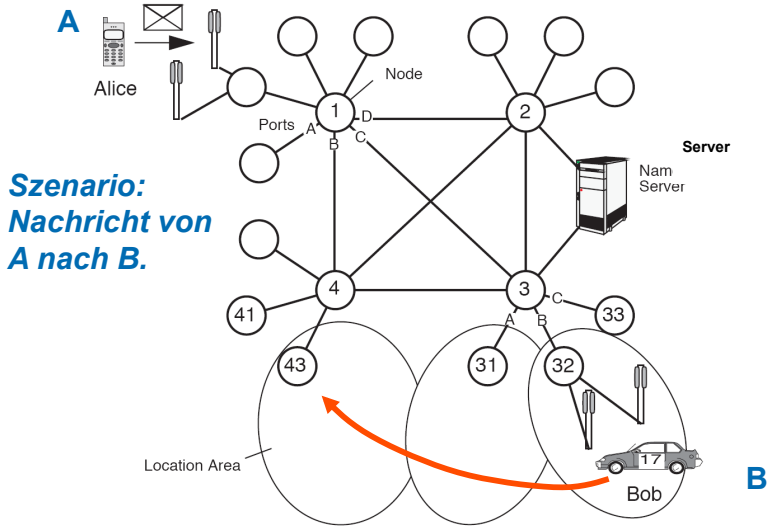
DHBW Stuttgart

Mit dem Laptop bin ich doch auch mobil - was ist daran besonders?



Mobilitätsverwaltung

DHBW Stuttgart



Szenario: Nachricht von A nach B.

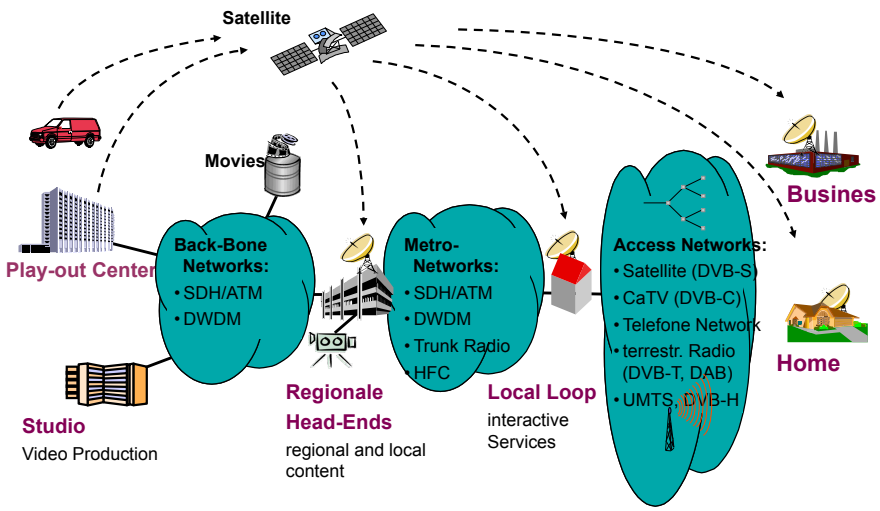
Mobile Teilnehmer im Netz - Fragen

DHBW Stuttgart

- A (Alice) schickt eine Nachricht an B (Bob, Adresse 17 an Knoten 32) – Was passiert im Netz (Routing-Tabellen in den Knoten)?
- B ist mobil und hat sich zum Knoten 43 bewegt – Was passiert nun?
- Wie kann man Nachrichten an mobile Nutzer zustellen? Was sind die Unterschiede zum Festnetz?
- B hat sein Händi ausgeschaltet – Was passiert nun mit an ihn verschickten Nachrichten?
- Wie kann man ausgeschaltete Geräte berücksichtigen und Nachrichten trotzdem zustellen?
- Der falsche Bob: Mallory kennt die Adresse von Bob, empfängt dessen Nachrichten und verschickt Nachrichten auf dessen Kosten. Warum ist das im Festnetz kein Problem? Was kann man dagegen tun?
- Das falsche Netz: Eine Basisstation in der Aktentasche ist der stärkste Sender in der Nähe und nimmt Nachrichten von Alice entgegen. Was kann man dagegen tun?

Satelliten im Weitverkehrsnetz

DHBW Stuttgart



Netze und Benutzer

DHBW Stuttgart

inkl. Nahbereich (Bluetooth, WiFi, …)

Netze:
- öffentliche Kommunikationsnetze
- Heimnetze
- Gebäude
- industrielle Fertigung
- Fahrzeuge

Benutzer:
- Leute
- Maschinen
- Geräte & Consumer Elektronik
- Sensoren & Aktuatoren

Technik der digitalen Netze

DHBW Stuttgart

ENDE Teil 1 – Einführung

Literaturempfehlung: Gerd Siegmund, Technik der Netze, Band 1 und 2, Band 1: Klassische Kommunikationstechnik: Grundlagen, Verkehrstheorie, ISDN/GSM/IN - Band 2: Neue Ansätze: SIP in IMS und NGN; VDE-Verlag; Auflage: 6., vollst. neu bearbeitete und erweiterte Auflage (2010); ISBN-13: 978-3800732203

DHBW Stuttgart

Technik der digitalen Netze

Teil 2 - Mobilität

www.dhbw-stuttgart.de

Inhaltsübersicht

DHBW Stuttgart

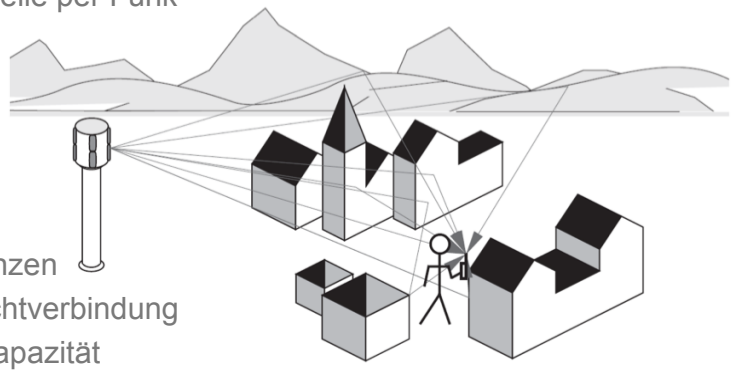
Was steckt hinter meinem Händi?

- Funk und Funkzellen
- Szenarien: Anrufen und angerufen werden
- Authentisierung
- Roaming und Hand-Over
- GSM-Netzarchitektur (2. Generation Mobilfunk)
- Datendienste der 2. Generation Mobilfunk

Funk und Funkzellen

DHBW Stuttgart

Die letze Meile per Funk



- Echos
- Interferenzen
- keine Sichtverbindung
- Uplink-Kapazität
- Downlink-Kapazität

Quelle: Gerd Siegmund (1)

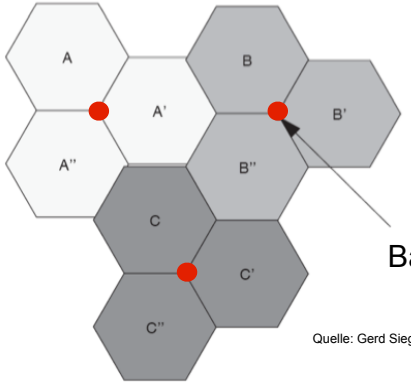
Ein Fall für die Funkspezialisten und für die Regulierung.

Zellulare Netzstruktur

DHBW Stuttgart

Funken auf der gleichen Frequenz gibt Ärger?

Muster wiederkehrender Frequenzen



Basisstation

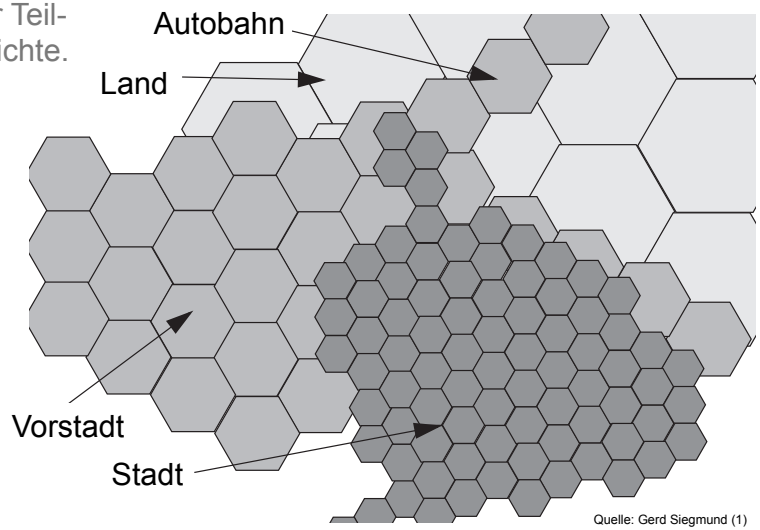
Quelle: Gerd Siegmund (1)

Die Größe der Funkzellen variiert ...

DHBW Stuttgart

... mit der Teilnehmerdichte.

Warum?



Quelle: Gerd Siegmund (1)

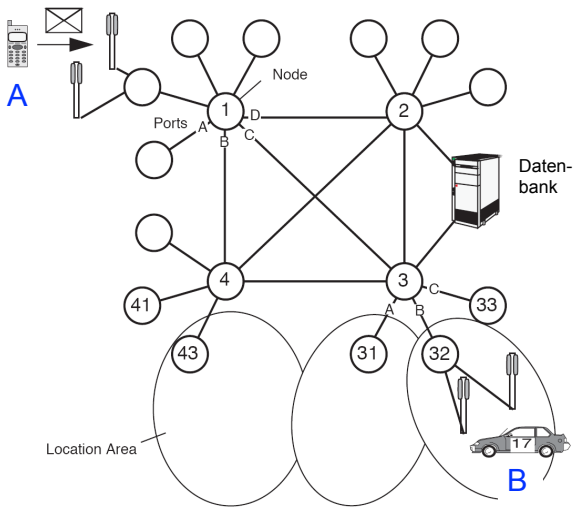
Was ein Mobilnetz können muss

DHBW Stuttgart

Szenarien:

(1) Anrufen aus dem Mobilnetz

(2) Angerufen werden im Mobilnetz



Anforderungen an das Mobilnetz

DHBW Stuttgart

Anrufen (Outgoing Call)

- Allokieren von Funkresourcen …
- … aber nur für Kunden (autorisierte Nutzer)
- Sonst nichts neues.

Authentisierung und Autorisierung

Angerufen werden (Incoming Call)

- Wo bin ich? – Das Netz muss meinen Standort ständig mitführen, wenn ich erreichbar sein möchte.
- Erfordert neue Funktion: Location Updates bzw. Roaming

Mobilitätsverwaltung

Zur Definition der Begriffe

DHBW Stuttgart

Authentisierung und Autorisierung: Zugang nur für Kunden

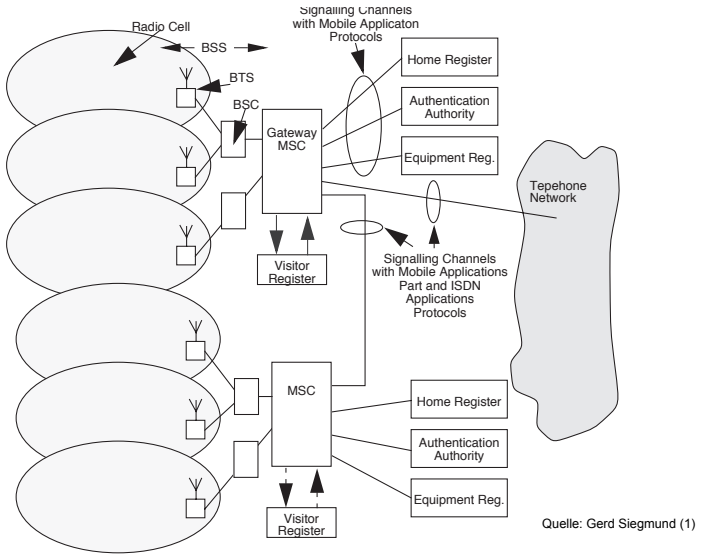
- authentisch: Identität ist überprüft
- autorisiert: Zugang ist erlaubt
- Diskussion: Identitätsdiebstahl, falsche Rechnungen, Abstreitbarkeit; wie implementiert man so etwas?

Mobilitätsverwaltung:

- Roaming: Ankommen, Händi einschalten, erreichbar sein
- Hand-Over: Ich bewege mich während eines Anrufes zwischen den Funkzelle, die Verbindung soll erhalten werden.
- Diskussion: wie implementiert man denn so etwas?

GSM Netzarchitektur

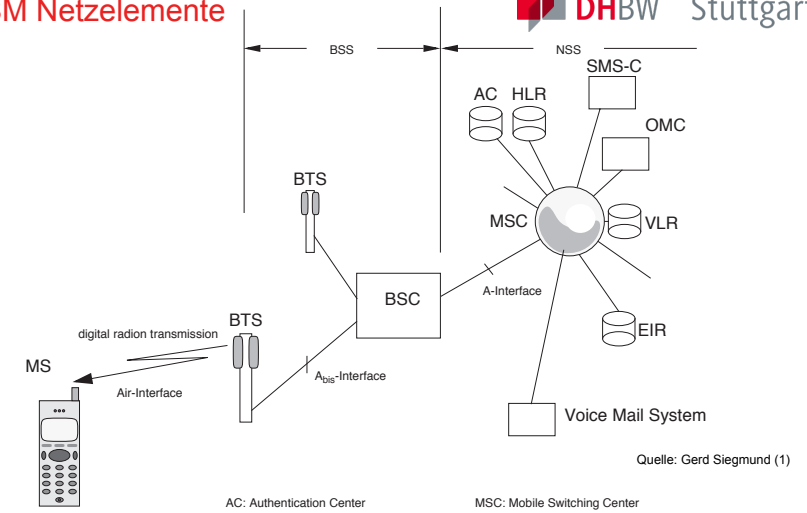
DHBW Stuttgart



Quelle: Gerd Siegmund (1)

GSM Netzelemente

DHBW Stuttgart



Quelle: Gerd Siegmund (1)

AC: Authentication Center
BSS: Base Station Subsystem
BSC: Base Station Controller
BTS: Base Transceiver Station
EIR: Equipment Identification Register
HLR: Home Location Register
MSC: Mobile Switching Center
MS: Mobile Station
NSS: Network Subsystem
OMC: Operation and Maintenance Center
SMS-C: Short Message Service Controller
VLR: Visitor Location Register

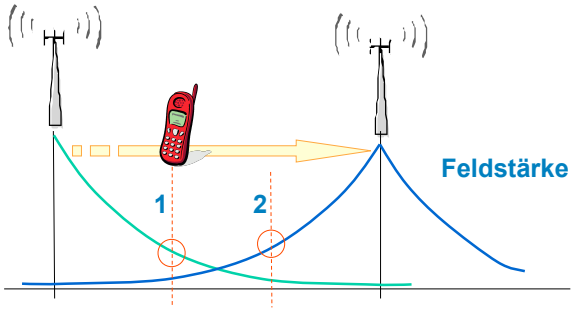
GSM Netzelemente

DHBW Stuttgart

- Mobiltelefon (Mobile Station, MS, dt. Händi)
- Basistation (Base Transceiver Station, BTS): Modem zur MS
- Vermittlunsanlage (Mobile Switching Centre, MSC): kombiniert mit Care-of-Postamt 1 (VLR, Visited Location Register)
- Home-Location Register, HLR: Care-of-Postamt 2, kombiniert mit Authentication Centre (AuC)
- Zusatzdienste:
  - Voice Mail Server
  - SMS Server
  - Equipment Register
- Operation & Maintenance Centre (Administration der Teilnehmer und der Netzinfrastuktur)

Hand-Over: Von Station zu Station

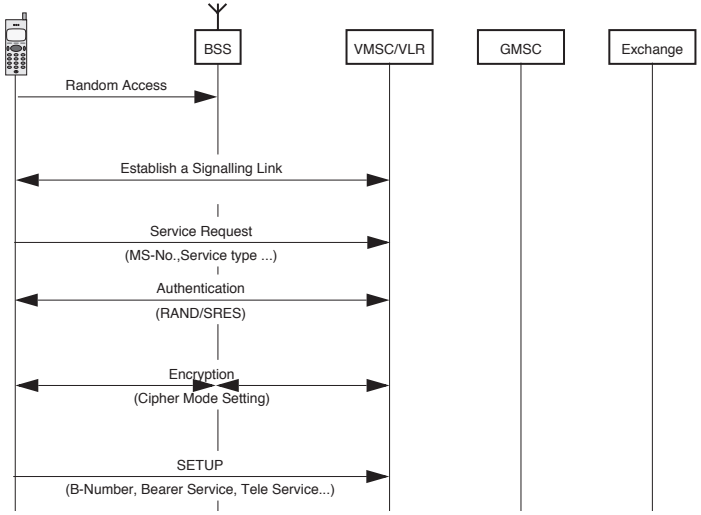
DHBW Stuttgart



- Das Mobiltelefon möchte während des laufenden Telefongesprächs zur stärkeren Station wechseln und beantragt den Wechsel beim Netz.
- Wenn der Antrag genehmigt wird, darf das Händi wechseln und die laufende Verbindung wird im Netz nachgeführt.

Mit dem Händi anrufen (1)

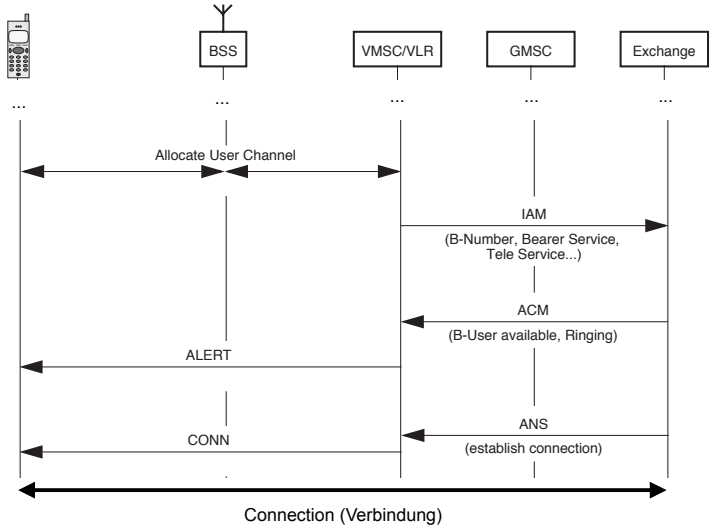
DHBW Stuttgart



Quelle: Gerd Siegmund (1)

Mit dem Händi anrufen (2)

DHBW Stuttgart



Quelle: Gerd Siegmund (1)

Aus dem Mobilnetz anrufen

DHBW Stuttgart

Sequenzdiagramm zur Darstellung des Ablaufs

Die einzelnen Schritte:

- Kanal beantragen
- Authentisierung
- Verschlüsselung vorbereiten

Speziell für den Mobilfunk

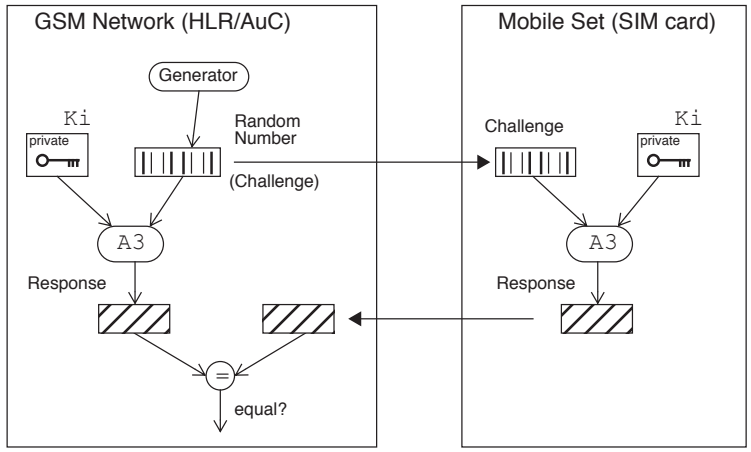
- Verbindung aufbauen

Wie beim Telefonnetz

Authentisierung

DHBW Stuttgart

Verhandlung zwischen Netz und Händi



Authentisierung - Fragen

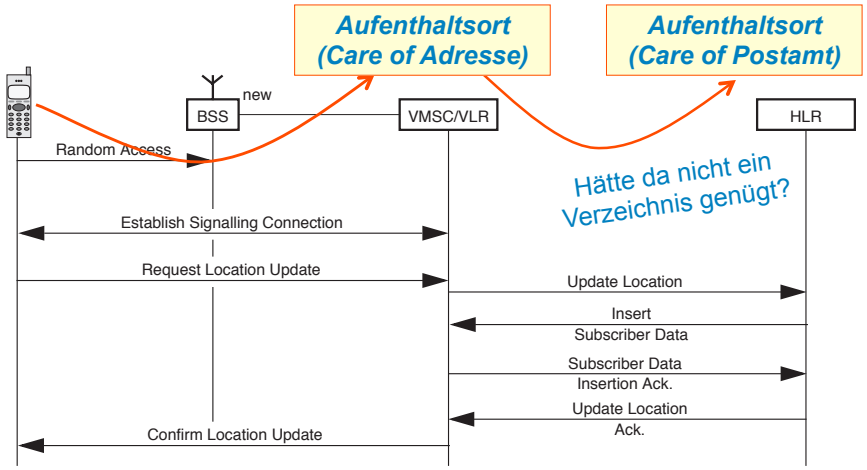
DHBW Stuttgart

- Beim Login in einen Server reichen doch auch User-ID und Passwort – warum macht man das bei GSM nicht genau so?
- Die GSM – Authentisierung beruht auf einem Geheimnis, das auf der SIM-Karte und im HLR/AuC abgelegt ist (dem geheimen Schlüssel Ki). Warum wird der geheime Schlüssel bei GSM bei der Authentisierung nie über das Netz übertragen?
- Wie funktioniert die in der Abbildung auf der letzten Folie gezeigte Authentisierung?
- Die SIM-Karte ist weg, was tun? Brauche ich jetzt eine neue Telefonnummer?
- Sicherheitslücke SIM-Karte: Wer SIM-Karten herstellt oder fälscht oder gefälschte SIM-Karten in Umlauf bringt …?

Roaming: Location Updates

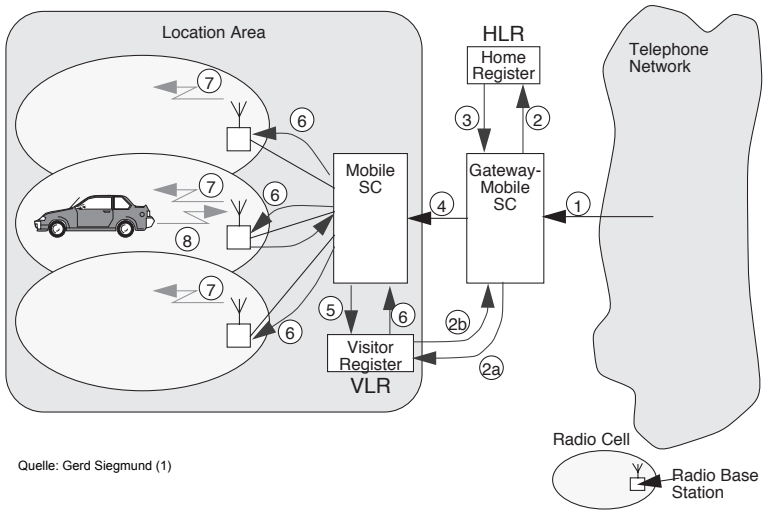
DHBW Stuttgart

Erreichbarkeit unterwegs



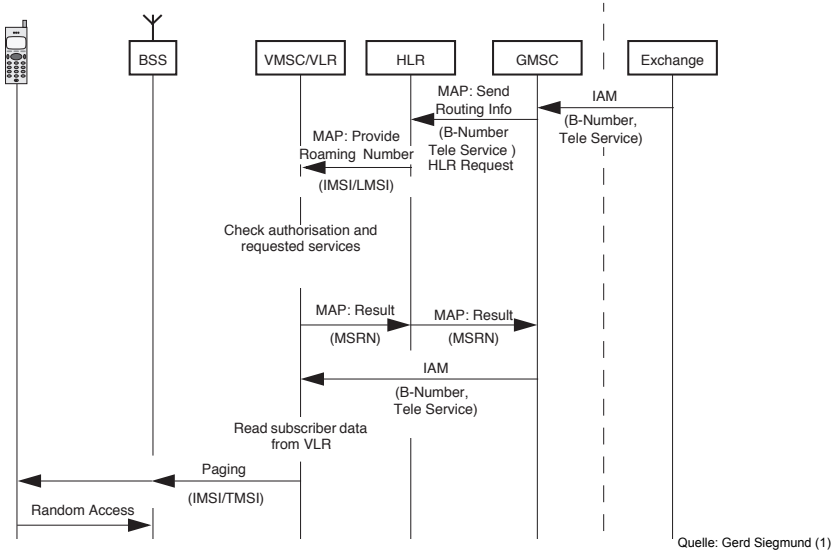
Quelle: Gerd Siegmund (1)

Sequenz eines Anrufs ins Mobilnetz



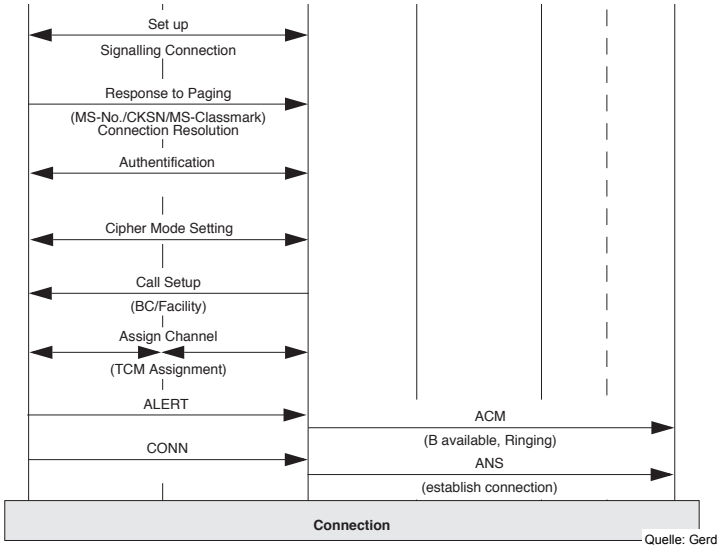
Quelle: Gerd Siegmund (1)

Anruf ins Mobilnetz (1)



Quelle: Gerd Siegmund (1)

Anruf ins Mobilnetz (2)



Quelle: Gerd Siegmund (1)

Anruf ins Mobilnetz - Ablauf

Sequenzdiagramm zur Darstellung des Ablaufs

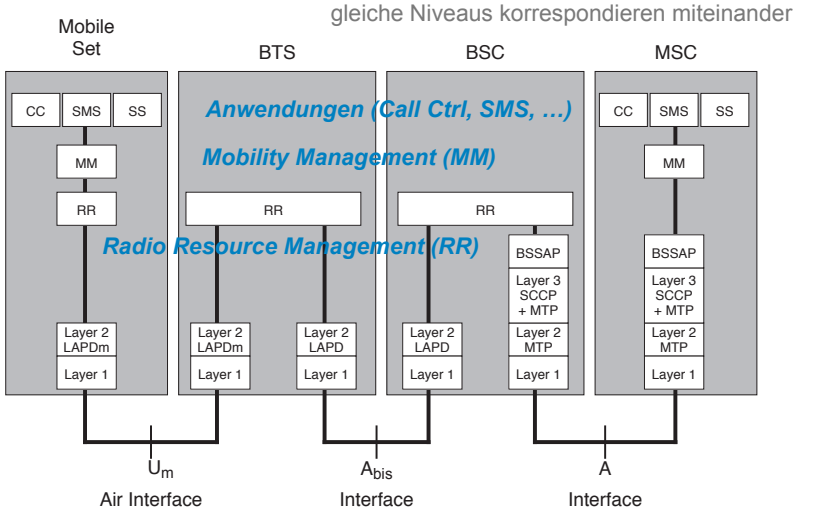
Die einzelnen Schritte:

- Verbindungswunsch signalisieren an Gateway-MSC
- Aufenthaltsort des gewünschten Teilnehmers nachschlagen in HLR und VLR
- Verbindungswunsch weiter signalisieren an Visited MSC
- Mobiltelefon wird in der Location Area ausrufen (Paging)

- Ausgerufenes Mobiltelefon meldet sich
- Ablauf wie beim Anruf vom Händi aus (Kanal beantragen, Authentisieren, Verbindung aufnehmen)

Beziehungen im Schichtenmodell

DHBW Stuttgart



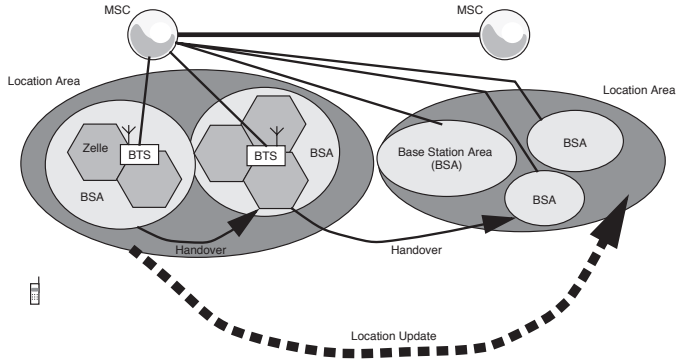
SS: Supplementary Services

Quelle: Gerd Siegmund (1)

Hand-over & Roaming

DHBW Stuttgart

Ganz unterschiedliche Dinge:

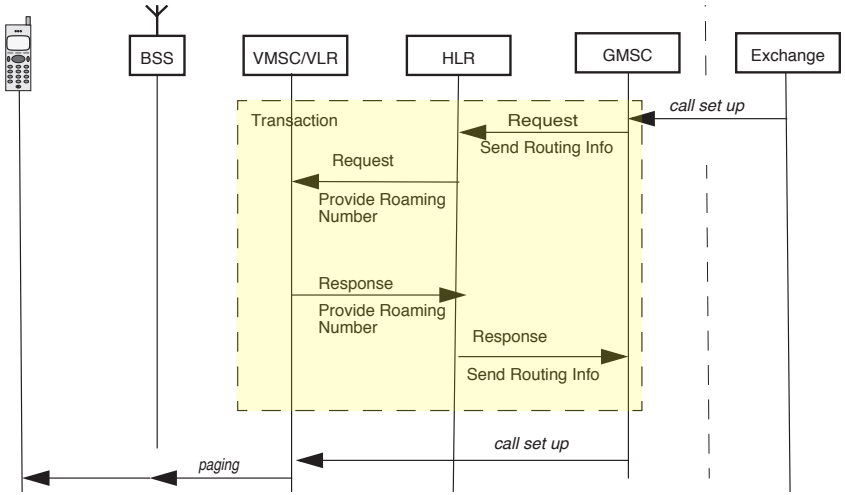


- Roaming: Netz führt Aufenthaltsort nach (sofern Händi eingeschaltet)
- Hand-over: Nachführen der laufenden Verbindung ohne Unterbrechung
- siehe auch: http://www.youtube.com/watch?v=UyWy4UBXadQ

Quelle: Gerd Siegmund (1)

Transaktionen an HLR und VLR (1)

DHBW Stuttgart



Transaktionen an HLR und VLR (2)

DHBW Stuttgart

Szenario:

- 50 Mio. Teilnehmer
- 4 Transaktionen pro Teilnehmer in der Hauptverkehrsstunde
- 50 ms Verarbeitungszeit für Look-up (HLR und VLR)
- 80% der Teilnehmer werden bereits im HLR gefunden
- 200 Bytes pro Nachricht

Transaktionen an HLR und VLR (3)

DHBW Stuttgart

Fragen:

- Transaktionen pro Sekunde insgesamt?
- Throughput (bits/s) an HLR und VLR
- Round-Trip Delay pro Transaktion?
- Welchen Vorteil hätte ein kombiniertes HLR/VLR?

Inhaltsübersicht

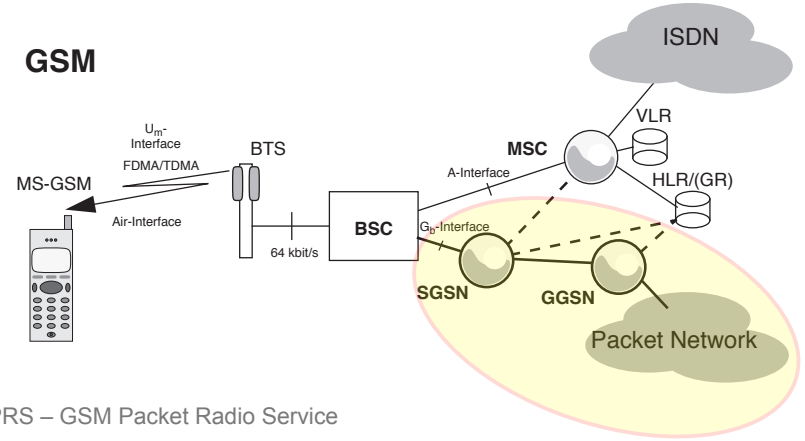
DHBW Stuttgart

Was steckt hinter meinem Händi?

- Funk und Funkzellen
- Szenarien: Anrufen und angerufen werden
- Authentisierung
- Roaming und Hand-Over
- GSM-Netzarchitektur (2. Generation Mobilfunk)
- Datendienste der 2. Generation Mobilfunk

GPRS – Der Datendienst in GSM

DHBW Stuttgart

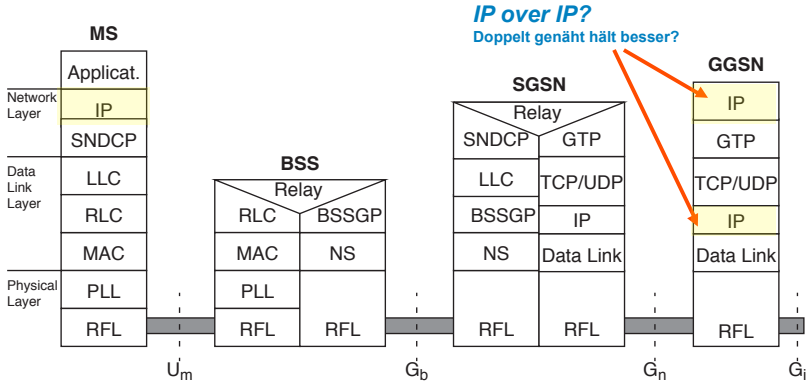


GPRS – GSM Packet Radio Service
SGSN – Serving GPRS Service Node (Access Control)
GGSN – Gateway GPRS Service Node (Übergang zum Internet)

Quelle: Gerd Siegmund (1)

Beziehungsgeflecht für GPRS

DHBW Stuttgart



SNDCP: Subnetwork Dependent Convergence Protocol
LLC: Logical Link Control
RLC: Radio Link Control
MAC: Medium Access Control
PLL: Physical Link Control
RFL: Physical RF Layer

BSSGP: BSS GPRS Application Protocol
GTP: GPRS Tunneling Protocol
TCP: Transmission Control Protocol
UDP: User Datagram Protocol
IP: Inernet Protocol
NS: Network Service

Quelle: Gerd Siegmund (1)

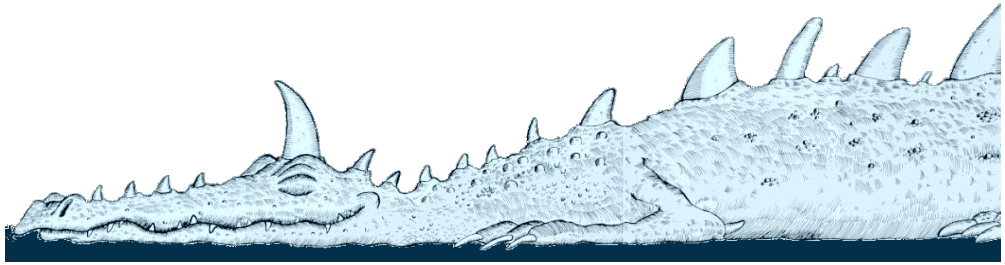
DHBW Stuttgart

ENDE Teil 2

Literaturempfehlungen:

(1) Gerd Siegmund, Technik der Netze, Band 1 und 2, Band 1: Klassische Kommunikationstechnik: Grundlagen, Verkehrstheorie, ISDN/GSM/IN - Band 2: Neue Ansätze: SIP in IMS und NGN; Vde-Verlag; Auflage: 6., vollst. neu bearbeitete und erweiterte Auflage (26. Mai 2010); ISBN-13: 978-3800732203

(2) Andrew S. Tanenbaum, Computer Netzwerke, Pearson Studium; Auflage: 4., überarb. A. (15. Juli 2003); ISBN-13 978-3827370464



DHBW Stuttgart

Technik der digitalen Netze
Teil 3 – Sicherheit

Stephan Rupp
Nachrichtentechnik

www.dhbw-stuttgart.de

Inhalt

DHBW Stuttgart

Sicherheit

- Begriffe: Vertraulichkeit, Integrität, Verfügbarkeit
- Bedrohungen
- Schutzmaßnahmen
- Identitätsnachweise
- Geheimniskrämerei
- Verfügbarkeit
- Hochverfügbare Systeme

Sichere Systeme – ganz abstrakt

DHBW Stuttgart

Vertraulichkeit (Confidentiality):

- Information sollte nicht unerwünscht an Dritte gelangen (z.B. Fernmeldegeheimnis, Schutz personenbezogener Daten, firmenvertrauliche Daten)
- Angriffe: Mithören, „Datendiebstahl“
- Lösungen: Zugangskontrolle, Authentisierung, Autorisierung, Verschlüsselung

Integrität (Integrity):

- Unversehrtheit
- Information sollte nicht verfälscht sein
- Angriffe: Identitätsdiebstahl; manipulierte Daten
- Lösungen: Prüfsummen, Signatur

Sichere Systeme – ganz abstrakt

DHBW Stuttgart

Verfügbarkeit (Availability):

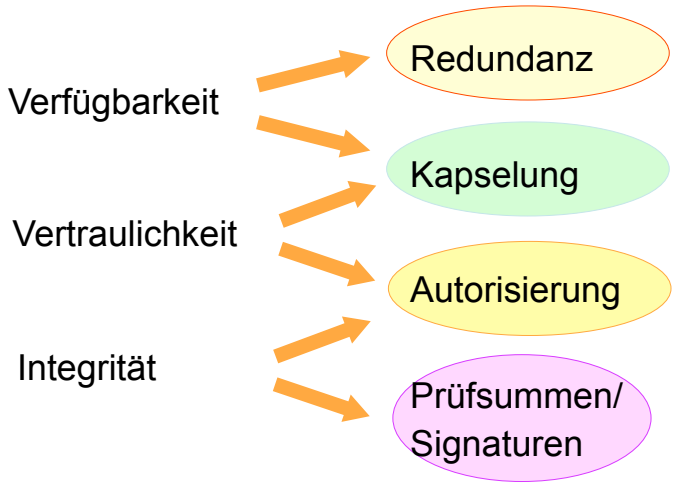
- Anwendungen bzw. Dienste sollten für autorisierte Nutzer jederzeit verfügbar sein
- Angriffe auf die Systemverfügbarkeit müssen verhindert oder abgewehrt können (Lastabwehr, Denial of Service, schädliche Software)
- Nicht jede Software ist vertrauenswürdig!
- Lösungen: Redundanz, Kapselung und Sicherheitsmodell (Rollen, Rechte und Pflichten definieren, umsetzen und einfordern)

CIA
(für die Fans von Eselsbrücken)

Englisch - Deutsch
Security = Sicherheit
Safety = funktionale Sicherheit

Sicherheitskonzepte

DHBW Stuttgart



Was ist Kapselung (Encapsulation)?

DHBW Stuttgart

Bob in einer unsicheren Umgebung

Alice in einer sicheren Umgebung

Inhalt

DHBW Stuttgart

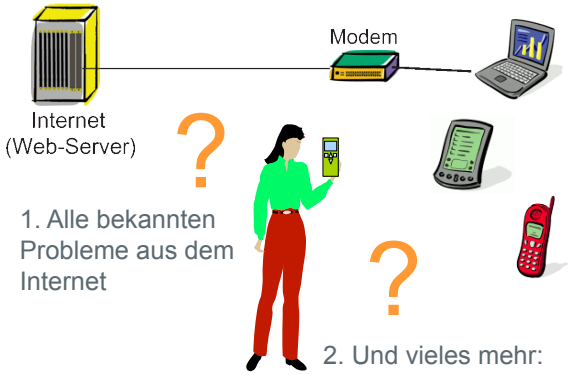
Sicherheit

- Begriffe: Vertraulichkeit, Integrität, Verfügbarkeit
- Bedrohungen: Risiken und Nebenwirkungen
- Schutzmaßnahmen
- Identitätsnachweise
- Geheimniskrämerei
- Verfügbarkeit
- Hochverfügbare Systeme

Vom Schreibtisch in die Westentasche

DHBW Stuttgart

Die Probleme wandern mit.



1. Alle bekannten Probleme aus dem Internet

2. Und vieles mehr:
- Bewegungsprofile
- persönliche Daten
- neue Verbreitungsmöglichkeiten für Schädlinge

Schreibtisch

(zuhause oder im Geschäft)

Mobile Dienste: unterwegs und überall dabei

Was kann mir passieren?

DHBW Stuttgart

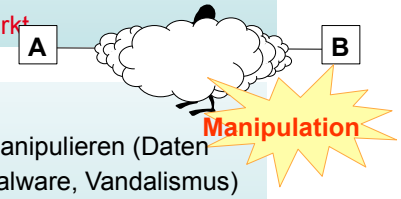
Passive Angriffe

- Mithören
- Passwörter ausspionieren
- Datenklau
- Identitätsdiebstahl
- Verhaltenmuster und Nutzerprofile erstellen
- bleiben völlig unbemerkt

Funktechnologien sind leicht zu belauschen!

Aktive Angriffe

- Eingriff in die Kommunikation
- Manipulation von Daten
- Verbindung entführen
- Boykott (Denial of Service)
- Geräte manipulieren (Daten stehlen, Malware, Vandalismus)
- mit falscher Identität agieren
- Übertölpeln von Nutzern (z.B. Passwörter stehlen)



Inhalt

DHBW Stuttgart

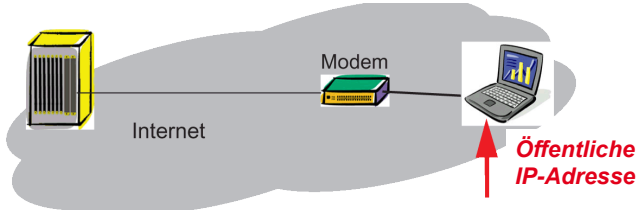
Sicherheit

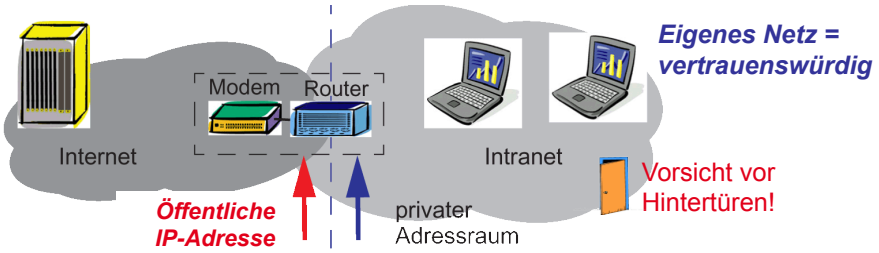
- Begriffe
- Bedrohungen
- Schutzmaßnahmen: Verhaltensregeln, die eigenen 4 Wände, der Vorraum
- Identitätsnachweise
- Geheimniskrämerei
- Verfügbarkeit, Hochverfügbare Systeme

Verhaltensregeln

DHBW Stuttgart

Öffentliches oder fremdes Netz = nicht vertrauens-würdig



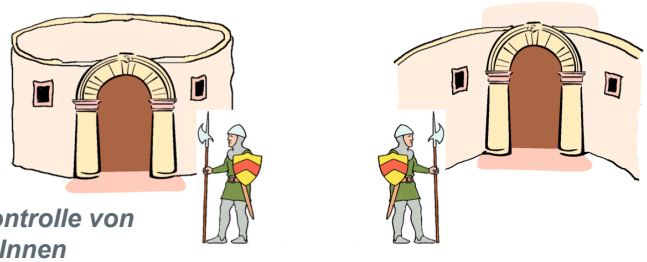


Eigenes Netz = vertrauenswürdig

Die eigenen 4 Wände

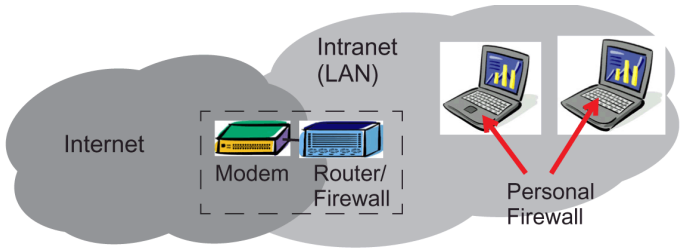
DHBW Stuttgart

Stadttor



= Zugangskontrolle von Aussen und Innen

Firewall



Mehrstufige Kapselung

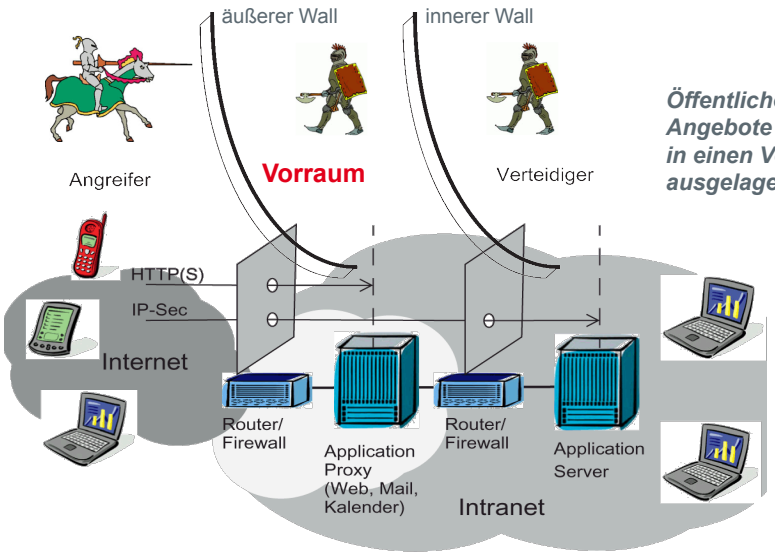
DHBW Stuttgart

Vorraum: Marktplatz und Lobby

Burg Falkenstein, Luftbild von Westen

Vorraum

DHBW Stuttgart

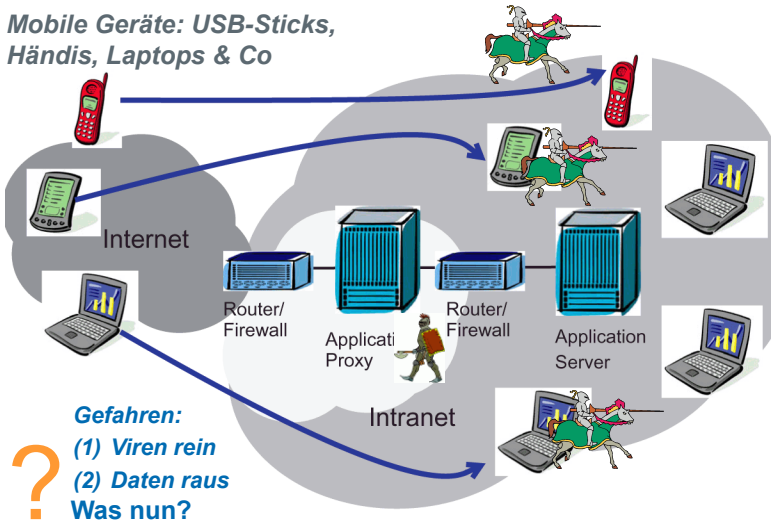


Öffentliche Angebote werden in einen Vorraum ausgelagert

An der Firewall vorbei ins Intranet

DHBW Stuttgart

Mobile Geräte: USB-Sticks, Händis, Laptops & Co



Gefahren:
(1) Viren rein
(2) Daten raus
Was nun?

Inhalt

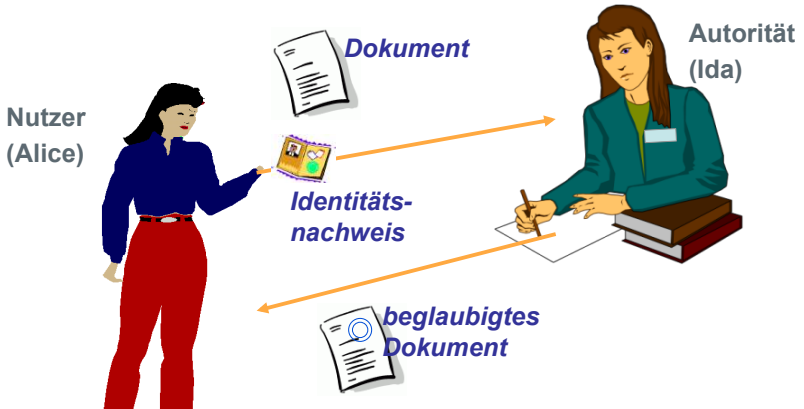
DHBW Stuttgart

Sicherheit

- Begriffe
- Bedrohungen
- Schutzmaßnahmen
- Identitätsnachweise: Authentisierung, Zertifikate, Signaturen
- Geheimniskrämerei
- Verfügbarkeit, Hochverfügbare Systeme

Identitätsnachweis, Ursprungsnachweis

DHBW Stuttgart

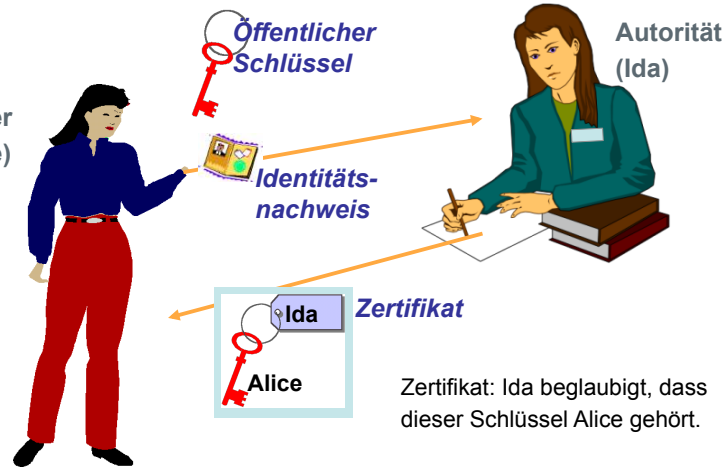


Identitätsnachweise:

- Geheimnis ("Ich weiss was", z.B. UserID/Passwort, ...)
- Token ("Ich hab was", z.B. Ausweis, Chipkarte, ...)
- Biometrische Merkmale ("ich bins")

Zertifikate

DHBW Stuttgart



Zertifikat: Ida beglaubigt, dass dieser Schlüssel Alice gehört.

Nutzung von Zertifikaten

DHBW Stuttgart

Ursprungsnachweise für

- Dokumente (digitale Signatur, verschlüsselte Dokumente)
- Software aus vertrauenswürdigen Quellen
- signierte E-Mail (Vermeidung von Spam und Manipulation)

Aufbau verschlüsselter Verbindungen

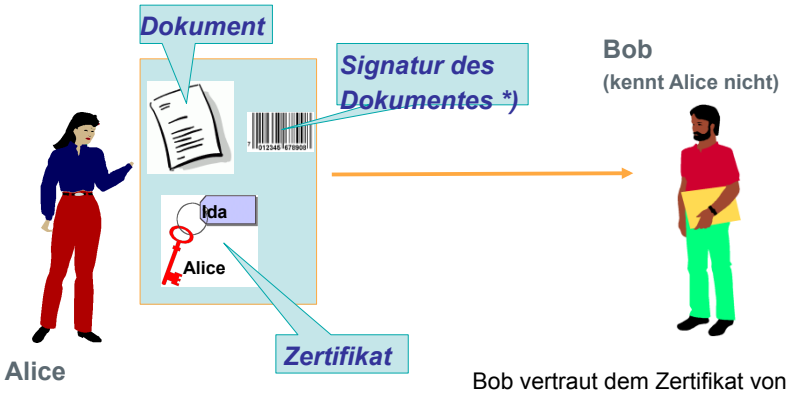
- z.B. für Secure Socket Verbindungen (https, SSL)

Identitätsnachweise für

- Server bzw. Clients für verschlüsselte Verbindungen
- RAS Token (Shared Key im Token)
- SIM-Karten, Kabelmodems (personalisierte Auslieferung)

Ursprungsnachweis für Dokumente

DHBW Stuttgart



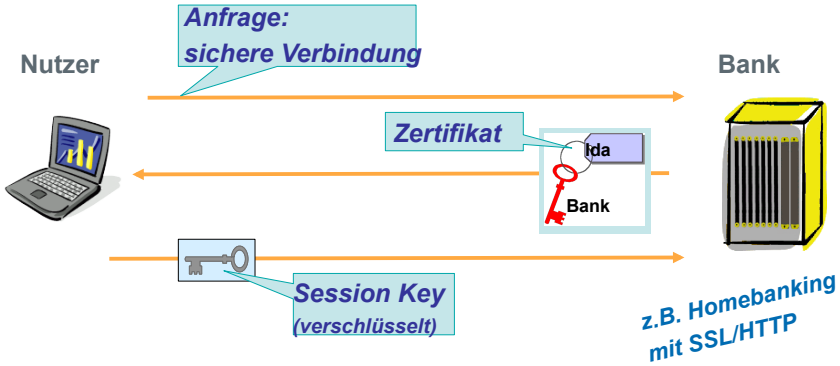
*) Signatur: mit dem privaten Schlüssel von Alice verschlüsselte Prüfsumme des Dokumentes

Bob vertraut dem Zertifikat von Ida und kann prüfen, dass:

- das Dokument von Alice stammt
- das Dokument nicht manipuliert wurde

Aufbau verschlüsselter Verbindungen

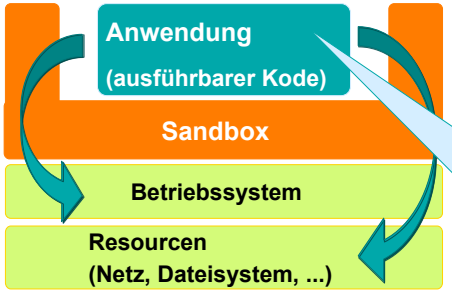
DHBW Stuttgart



Der Nutzer entnimmt dem Zertifikat den öffentlichen Schlüssel der Bank. Mit dem öffentlichen Schlüssel verschlüsselt er einen symetrischen Session Key, den er der Bank übermittelt. Der Session Key wird nun für den Austausch verschlüsselter Dokumente verwendet.

Kapselung von Software

DHBW Stuttgart



Nur vertrauenswürdige Anwendungen erhalten Zugriff auf das System und seine Resourcen.

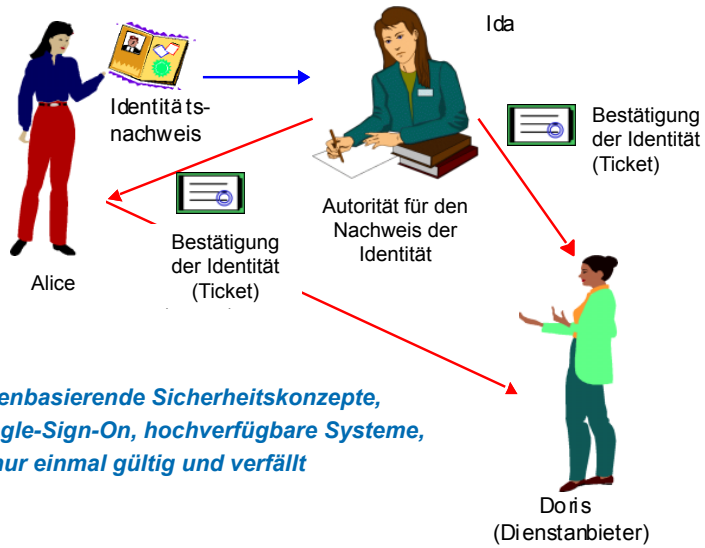
Vertrauensbeweis durch ein Zertifikat:

- Software stammt aus einer vertrauenswürdigen Quelle
- Software wurde nicht manipuliert.

? **Signierte Trojaner?**

Tickets bzw. Token als Eintrittskarte

DHBW Stuttgart



Für rollenbasierende Sicherheitskonzepte, z.B. Single-Sign-On, hochverfügbare Systeme, Ticket nur einmal gültig und verfällt

Inhalt

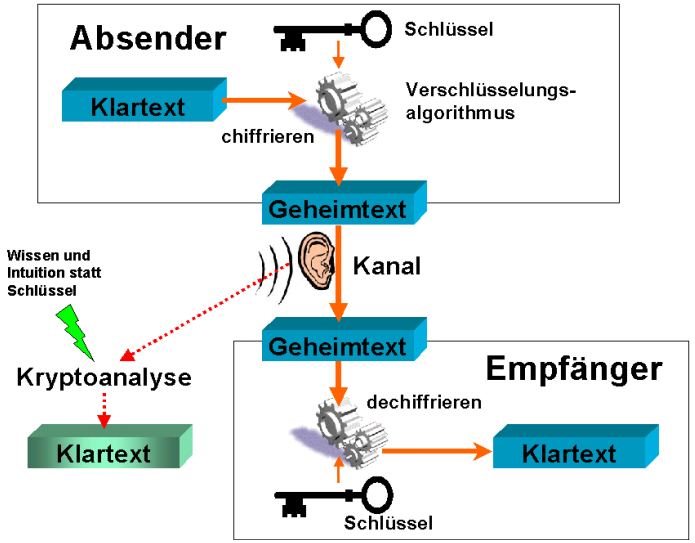
DHBW Stuttgart

Sicherheit

- Begriffe
- Bedrohungen
- Schutzmaßnahmen
- Identitätsnachweise
- Geheimniskrämerei: Verschlüsselung symmetrisch und asymmetrisch, Hashfunktionen
- Verfügbarkeit, Hochverfügbare Systeme

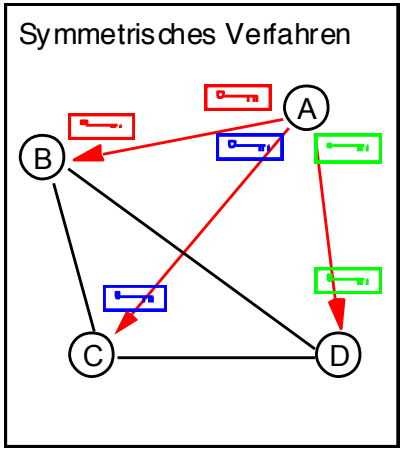
Verschlüsselung und Entschlüsselung

DHBW Stuttgart

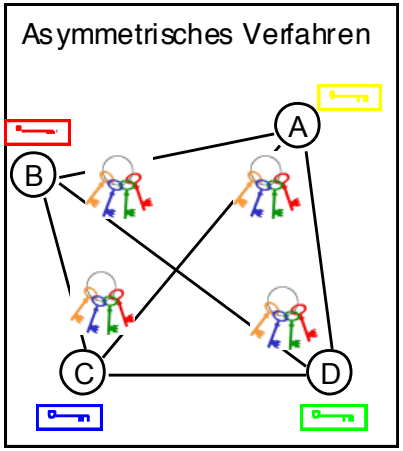


Schlüssel und Schlüsselpaare

DHBW Stuttgart



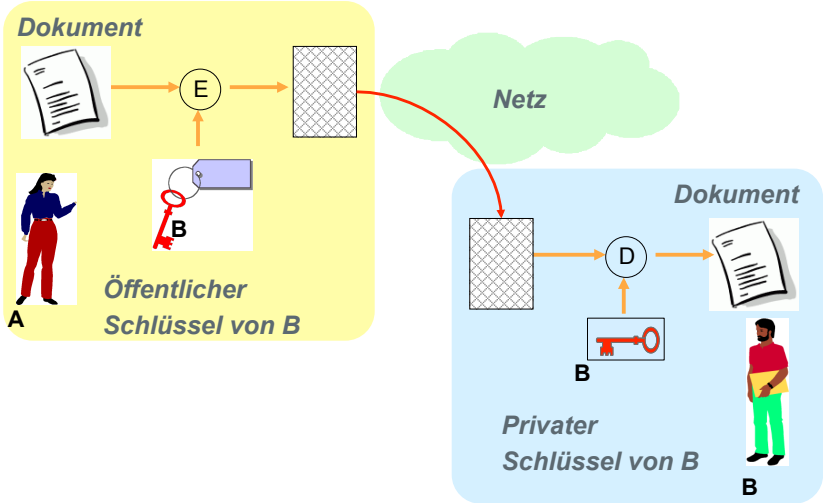
Schnelle Verfahren, aber Verteilung der Schlüssel problematisch



Langsam, aber Schlüsselverteilung gelöst

Asymetrische Verschlüsselung

DHBW Stuttgart



Hash-Funktion als Prüfsumme

DHBW Stuttgart

Nachricht
bzw. Dokument

↓

Hash
Funktion

↓

128 Bit/ 160 Bit
Ergebnis

Hashfunktion (auch *message digest*):

- generiert eine Prüfsumme fixer Länge,
- aus der das Eingangsdokument nicht rekonstruierbar ist und
- die sich bei kleinsten Änderungen im Eingangsdokument ändert.

Prüfsumme (*hash*) lässt sich als Integritätsnachweis für Nachrichten und Dokumente verwenden, sowie in Kombination mit einem privaten Schlüssel als Ursprungsnachweis (z.B. Signatur bzw. message authentication codes).

Strecken und Dehnen

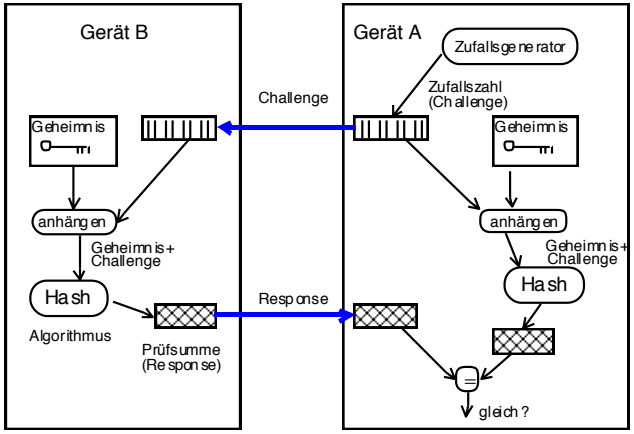
DHBW Stuttgart

Gymnastik

authentisieren, verschlüsseln
und signieren

Authentisieren mit Challenge-Response

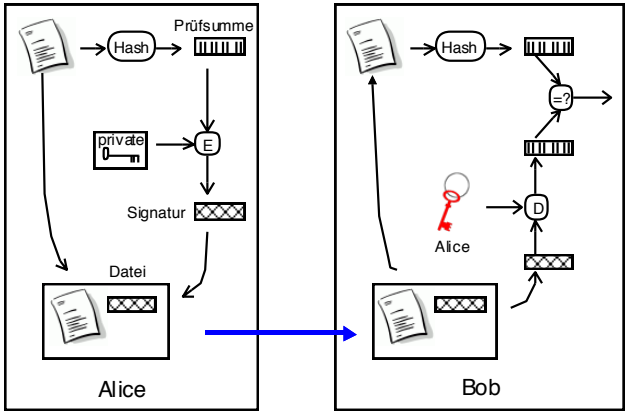
DHBW Stuttgart



- Worin liegt der Vorteil gegenüber einfachem Authentisieren mit User-ID und Passwort? (Hinweis: was wird im Klartext übermittelt? Was wird beim nächsten Mal im Klartext übermittelt?)

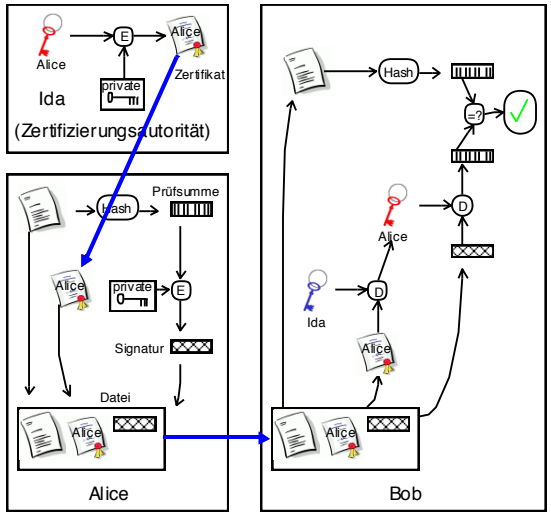
Ein Dokument signieren - einfacher Fall

DHBW Stuttgart



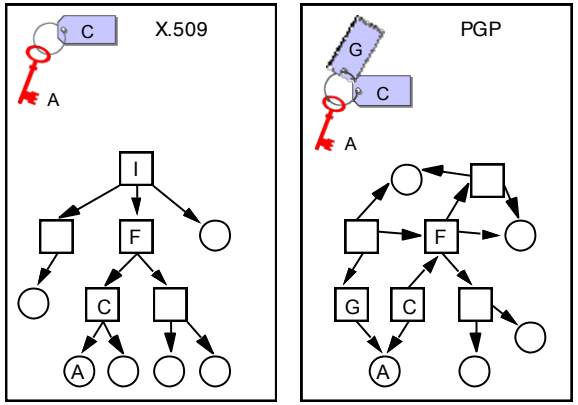
- Wie funktioniert das? (Hinweis: E=Encryption/Verschlüsselung, D= Decryption/Entschlüsselung)
- Woher bekommt Bob den öffentlichen Schlüssel von Alice und woher weiß er, das es der korrekte Schlüssel ist?

Ein Dokument signieren - Root Zertifikat



- Was ist der Unterschied zum Verfahren auf der letzten Seite? Vorteile?

Vertrauensbeziehungen bei Zertifikaten



- Zertifikate nach dem X.509 Standard benötigen streng hierarchische Vertrauensbeziehungen.
- Zertifikate nach PGP (bzw. GnuPG) sind da flexibler.
- Was wären die Vorteile bzw. Nachteile im Vergleich der Verfahren?

Inhalt

Sicherheit

- Begriffe
- Bedrohungen
- Schutzmaßnahmen
- Identitätsnachweise
- Geheimniskrämerei
- Verfügbarkeit: Redundanz + Kapselung
- Hochverfügbare Systeme

Was ist Redundanz?

Department of
Redundancy Department

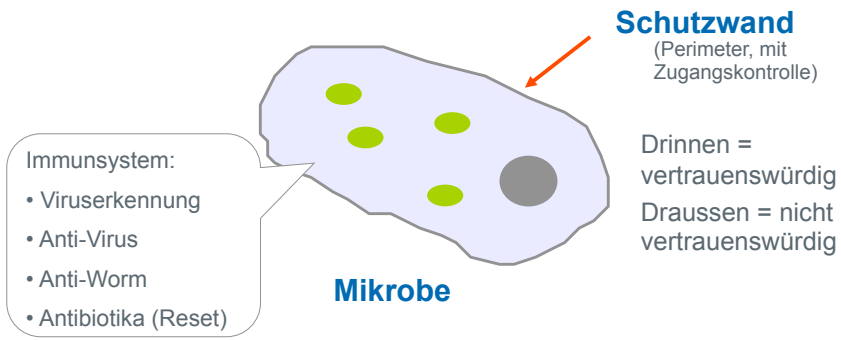
Office hours

Mo – Fr: 8am – 5pm, 9am – 6pm

Tu – Mo: 9am – 4pm

Was ist Kapselung?

DHBW Stuttgart



Drinnen = vertrauenswürdig

Draussen = nicht vertrauenswürdig

Kapselung = Perimeter-basierender Schutz

(ein fundamentales Konzept und ganz alter Hut)

Inhalt

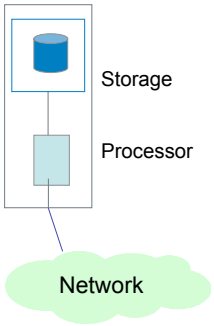
DHBW Stuttgart

Sicherheit

- Begriffe
- Bedrohungen
- Schutzmaßnahmen
- Identitätsnachweise
- Geheimniskrämerei
- Verfügbarkeit
- Hochverfügbare System: Lösungsansätze

Redundanz: Grundlagen

DHBW Stuttgart



Zu schützen:

- Zustände (States) im Prozessor
- Daten im Speicher

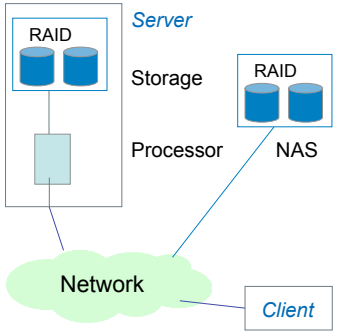
Lösungen:

- Zustände: Der Anwendungssoftware überlassen (z.B.Kapselung von Transaktionen, Jounal-Files) bzw. dem Anwender überlassen (zwischendurch Speichern)
- Daten im Speicher: Back-ups

- Reicht für Desktop-PCs (nicht wirklich hochverfügbar)

Redundante Speicher

DHBW Stuttgart



Zu schützen:

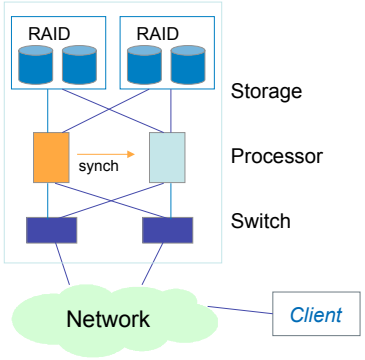
- Daten im Speicher

Lösung:

- Redundante Speichermedien (lokales RAID bzw. Network Attached Storage mit RAID)
- Back-ups

- Reicht für kleine Netze (nicht wirklich hochverfügbar)

Doppelt genäht hält besser

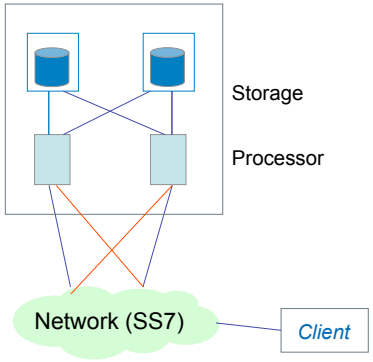


Systemarchitektur

- Redundante Switches (Ethernet)
- Redundante Prozessoren mit synchronisiertem Arbeitsspeicher
- Redundanter Speicher
- Gleicher Standort
- Erweiterbar mit mehr Prozessoren und Speicher

- Reicht für Systeme mittlerer Grösse ohne Disaster-Recovery
- Fail-Over bzw. Switch-Over für Wartung/Updates
- Schutz vor instabiler bzw. bösartiger Software (Anwendung, OS, Middleware)?

„Mated-Pairs“ in TK-Netzen

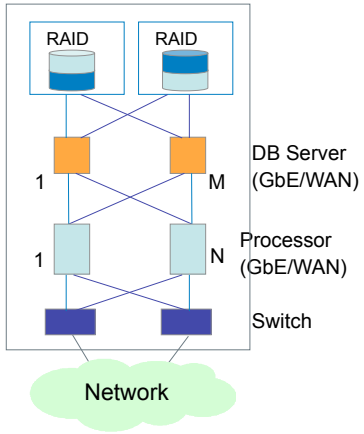


Systemarchitektur

- Redundante Prozessoren mit redundantem Speicher
- Netz unterstützt Fail-Over (Felhlerpfad wird vorkonfiguriert)
- Spezialfall der 2N Redundanz
- Wird teuer für viele Systeme (2N)

- Reicht für Systeme mittlerer Grösse ohne Disaster-Recovery
- Netz muss Fehlerpfade unterstützen
- Schutz vor instabiler bzw. bösartiger Software?

Einer Extra: N+1 Redundanz

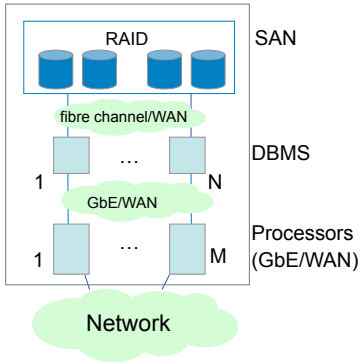


Systemarchitektur

- Redundanter Speicher (RAID, persistente Daten)
- M+1 redundante Datenbank-Server mit synchronisiertem Arbeitsspeicher
- N+1 redundante Prozessoren
- SW-Architektur auswärts skalierbar für grosse, verteilte Systeme

- Konzept: Trennung der Daten von der Anwendung (Data Base Servers), Ausfall eines Prozessors/DB Servers ohne Datenverlust
- Systeme mittlerer Grösse

N+k Redundanz mit Speichernetzen



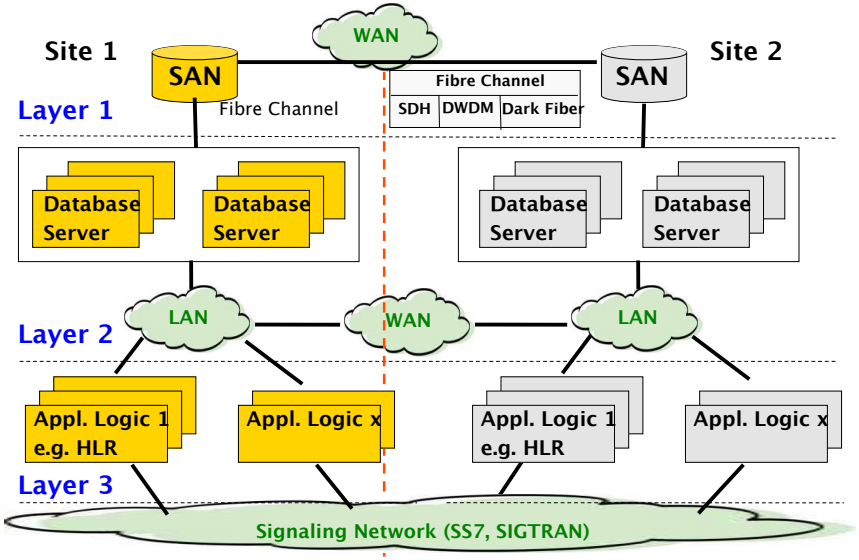
Systemarchitektur

- Redundante Speicher
- Redundantes Datenbank Management System (DBMS)
- Redundante Prozessoren
- Geographische Redundanz über Hochgeschwindigkeitsnetze
- Virtualisierung der Resourcen of (Speicher und Prozessor)
- Unterstützt N+k für Prozessor, DBMS und Speicher

- Reicht für grosse, verteilte Systeme mit höchster Verfügbarkeit
- Anwendung/Watchdog benötigt für Recovery
- Schutz vor instabiler bzw. bösartiger Software?

Beispiel: N+k Redundanz im Kernnetz

DHBW Stuttgart



Vergleich Redundanzkonzepte für TK

DHBW Stuttgart

Characteristic	Typical High Availability Systems	Redundancy by Distributed Storage Networks
Unit Cost	High (Proprietary HW and standby redundant policy)	Low (Commercial off-the-shelf HW and optimised redundancy policy)
Typical Architecture	Mated-pair	Load-sharing peers
Local Fault Tolerance	2 x N	N + k
Geographical Redundancy	4 x N	N + k
Disaster Recovery Time	Minutes -> Hours	Instant

Bedrohungen für verteilte Systeme

DHBW Stuttgart

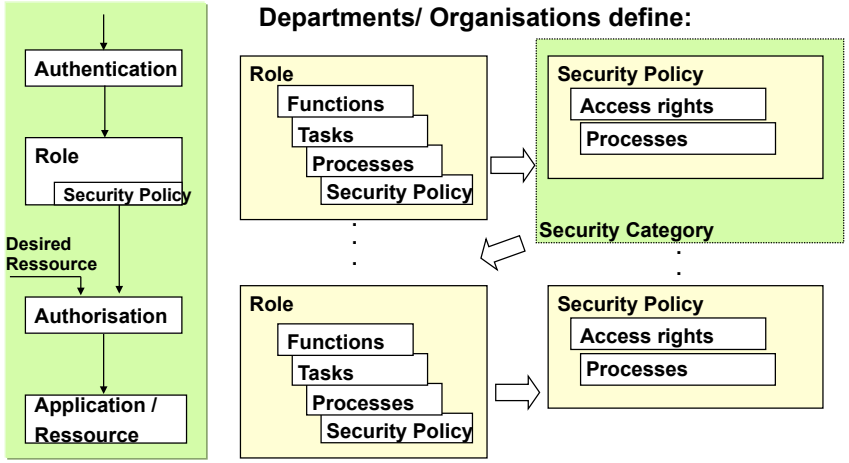
- Gleiche Gefahren wie für isolierte Systeme.
- Das Potential für Schaden ist wesentlich höher.

Jedoch:

- Kann für den Schutz viel mehr investiert werden als in isolierte Systeme.

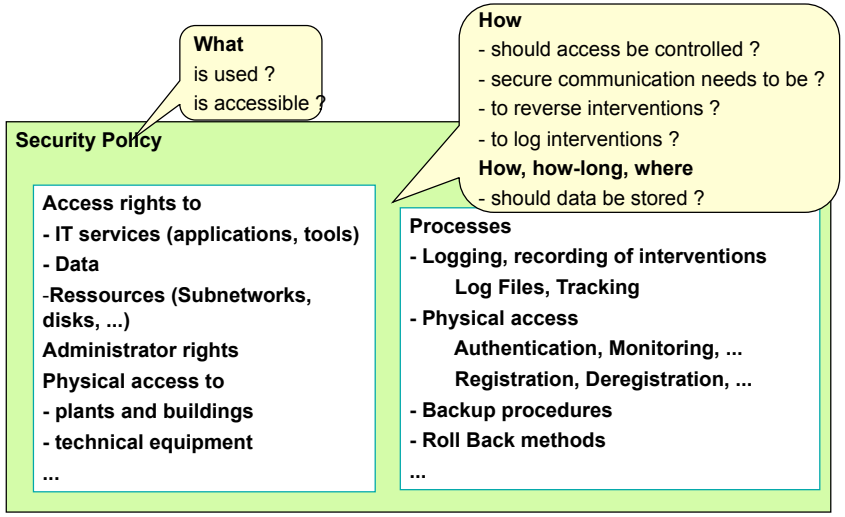
Sicherheitskonzept: Zugangskontrolle

DHBW Stuttgart



Richtlinien (Policies)

DHBW Stuttgart



Technik der digitalen Netze

DHBW Stuttgart

ENDE Teil 3 – Sicherheit

Literaturempfehlung: Bruce Schneyer, Secrets & Lies: IT-Sicherheit in einer vernetzten Welt, dpunkt.verlag/Wiley; Auflage: 1. Aufl. (2001), ISBN-13: 978-3898641135

Sicher ist nur, dass nichts wirklich sicher ist.
Nicht einmal das ist sicher.
Joachim Ringelnatz

DHBW Stuttgart

Technik der digitalen Netze
Teil 4 – Planung und Dimensionierung

Stephan Rupp
Nachrichtentechnik

www.dhbw-stuttgart.de

Inhalt

DHBW Stuttgart

Planung und Dimensionierung

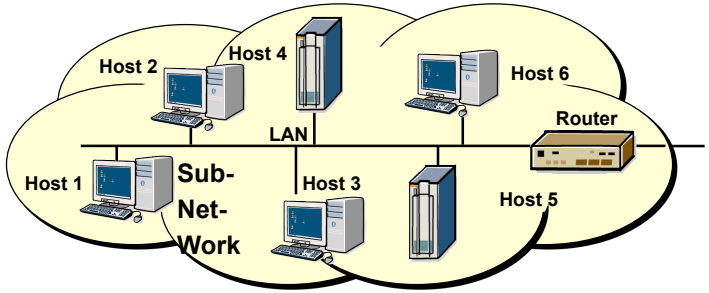
- IP-basierte Netze
- Voice over IP
- Verkehrsmodelle und Systemdimensionierung
- Daten und Redundanz

IP basierende Netze - Subnetworks

DHBW Stuttgart

Subnetworks (Teilnetze) sind die kleinsten Netzbereiche im Internet.

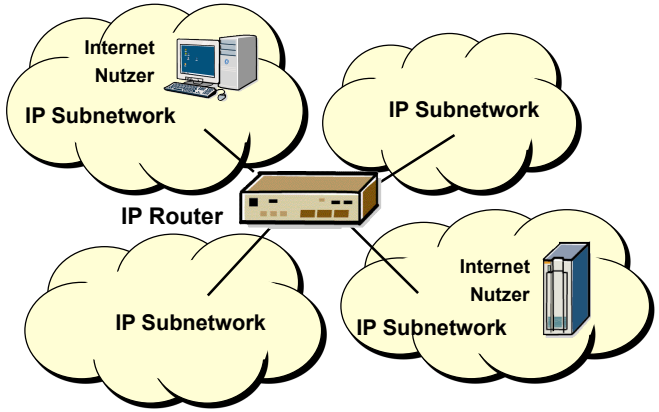
- Üblicherweise entsprechen sie einem LAN-Segment.
- Sie bestehen aus Workstations und Servern - „Internet Hosts“.
- Jeder „Internet Host“ hat (mindestens) eine IP-Adresse.
- Router bilden den Übergang zwischen den Subnetworks.



Quelle: Harald Orlamünder

Verbinden von Teilnetzen (1)

DHBW Stuttgart



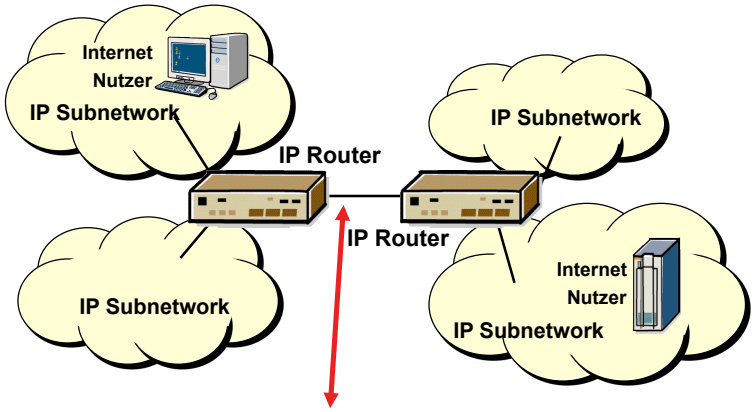
IP Subnetworks werden durch **IP Router** miteinander verbunden.

Der IP Router besitzt eine IP-Adresse per Port.

Quelle: Harald Orlamünder

Verbinden von Teilnetzen (2)

DHBW Stuttgart



Um eine größere Strecke zu überwinden wird ein Router-Paar eingesetzt.

Quelle: Harald Orlamünder

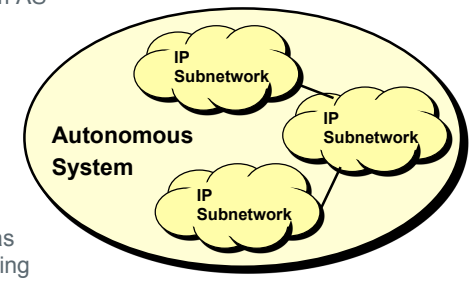
IP-Netze: Autonomes System

DHBW Stuttgart

Ein Autonomes System (AS) besteht aus einer Menge Router und Netze (Subnetworks), die einer gemeinsamen technischen Verwaltung unterstehen.

Das Autonomes System ist charakterisiert durch:

- ein gemeinsames Routing-Protokoll (üblicherweise)
- volle Erreichbarkeit im AS



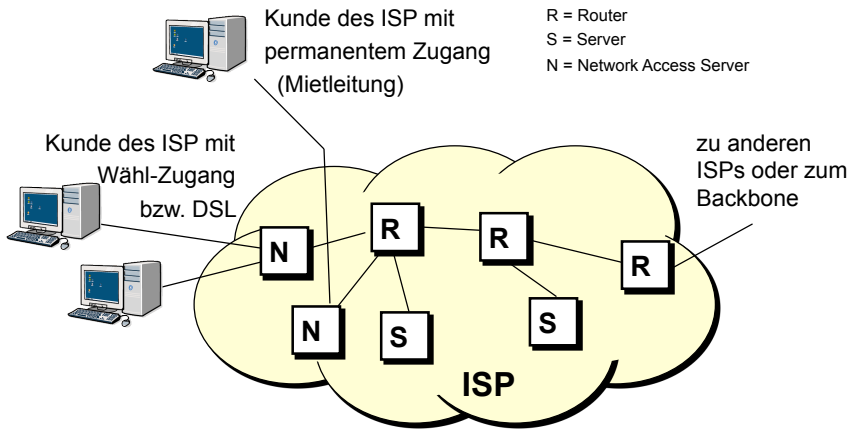
In der OSI-Welt wird das Autonome System “Routing Domain” genannt.

Quelle: Harald Orlamünder

Internet Service Provider (ISP)

DHBW Stuttgart

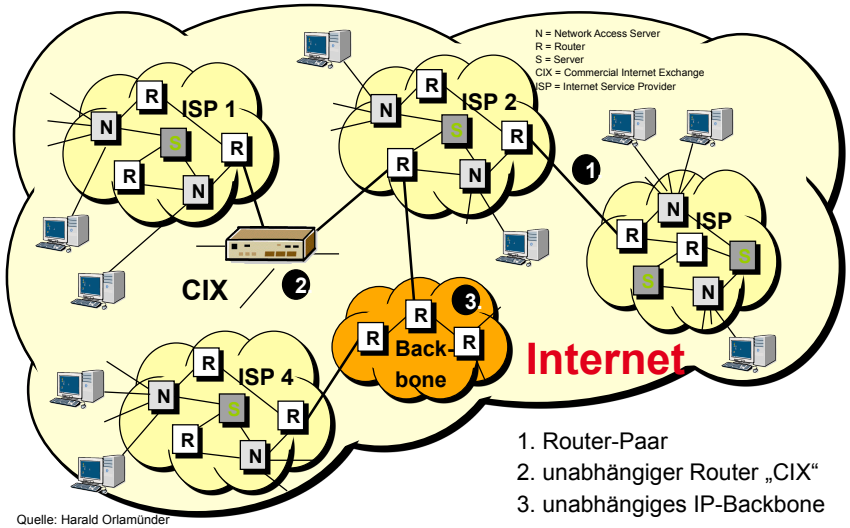
Logische Sicht des Netzes



Quelle: Harald Orlamünder

Das Internet als Netz

DHBW Stuttgart



1. Router-Paar
2. unabhängiger Router „CIX“
3. unabhängiges IP-Backbone

Quelle: Harald Orlamünder

Inhalt

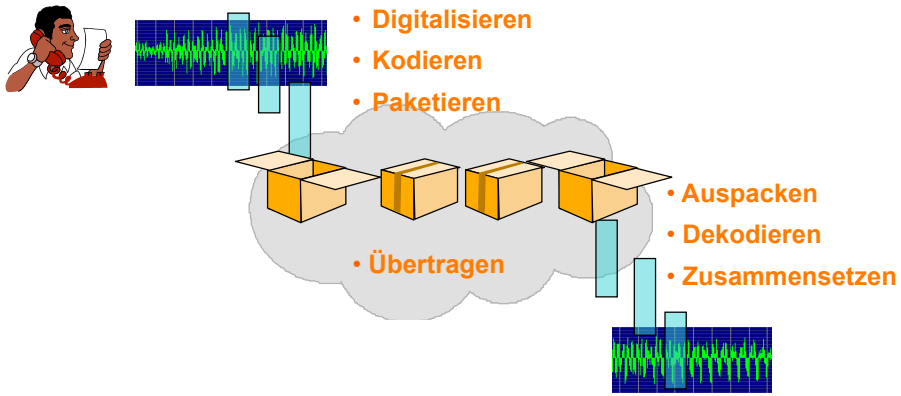
DHBW Stuttgart

Planung und Dimensionierung

- IP-basierte Netze
- Voice over IP
- Verkehrsmodelle und Systemdimensionierung
- Daten und Redundanz

Sprachpakete im Internet

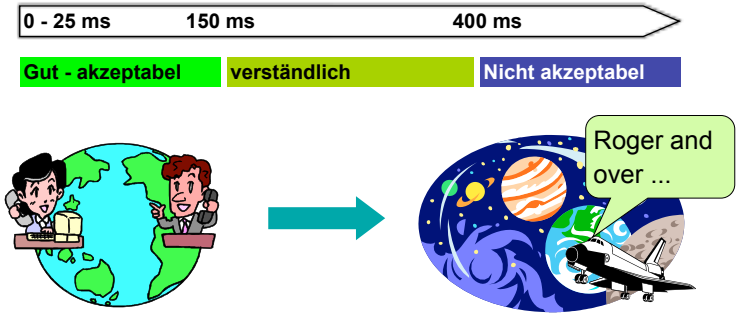
DHBW Stuttgart



Voice over IP

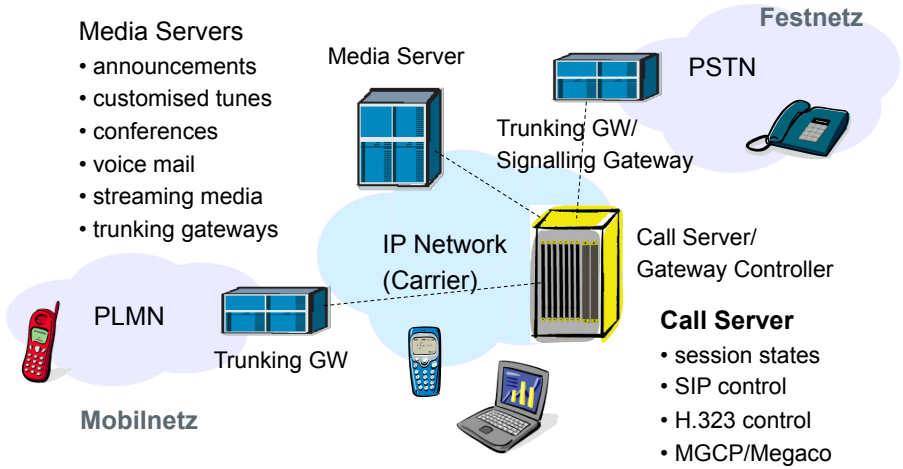
DHBW Stuttgart

Von Mund zu Ohr: Telefonieren verträgt wenig Verzögerungen



Öffentliche Netze

DHBW Stuttgart



SIP Happens

DHBW Stuttgart

SIP: Session Initiation Protocol (Signalisierungsprotokoll für Sessions)

- User Agent: Anwendungssoftware auf Terminals (SIP End Points)
- Terminals: PCs, Telefone, …
- Sind User Agents Clients oder Server?
  - Client: Ich rufe an.
  - Server: Ich nehme einen Anruf an.
- User Agent: Client + Server

Quelle: Gerd Siegmund

Inhalt

DHBW Stuttgart

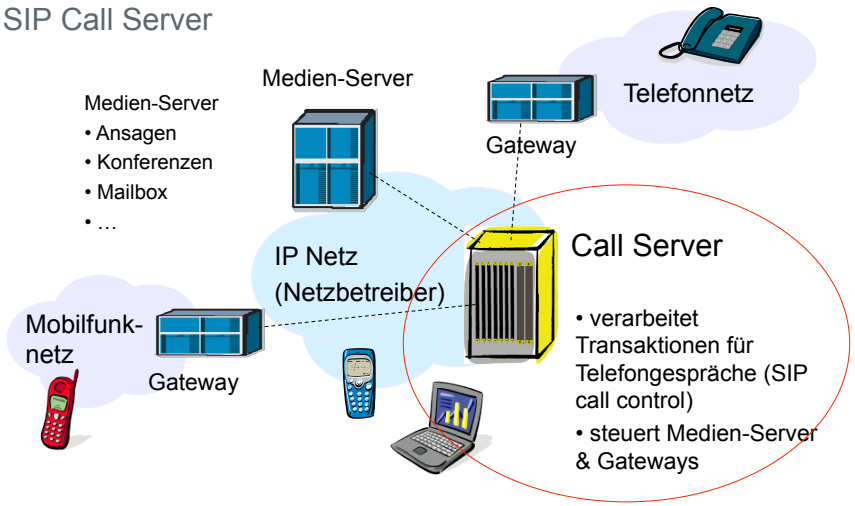
Planung und Dimensionierung

- IP-basierte Netze
- Voice over IP
- Verkehrsmodelle und Systemdimensionierung
- Daten und Redundanz

Beispiel: Öffentliche Netze

DHBW Stuttgart

SIP Call Server



Bemessungsgrößen für den Call Server

DHBW Stuttgart

Transaktionsrate:

- Transaktionen für Anrufe (SIP Transaktionen)
- Transaktion: Verbindung aufbauen, Verbindung auflösen, Ticket zur Abrechnung generieren, bzw. Ausnahmebehandlung

Verkehrsmodell (Beispiel):

- 1 Mio Teilnehmer (Subscribers)
- 500 Bytes Daten pro Teilnehmer (Teilnehmerprofil in der Datenbank)
- 4 Anrufe pro Teilnehmer in der Hauptverkehrsstunde
- Bemerkung: Hauptverkehrsstunde = Bemessungsgrösse; Messwert BHCA = Busy Hour Call Attempts (Transaktionen in der Hauptverkehrsstunde)

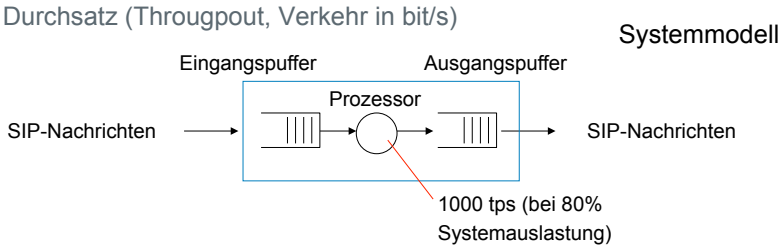
Transaktionsrate im Call Server:

- ca. 1000 tps (Transaktionen pro Sekunde)
- Bemerkung: Bei 1 Mio Teilnehmer: 4 Millionen BHCA, bei ca. 4000 Sekunden/Stunde ergeben sich ca. 1000 tps)

Bemessungsgrößen (2)

DHBW Stuttgart

Durchsatz (Througpout, Verkehr in bit/s)



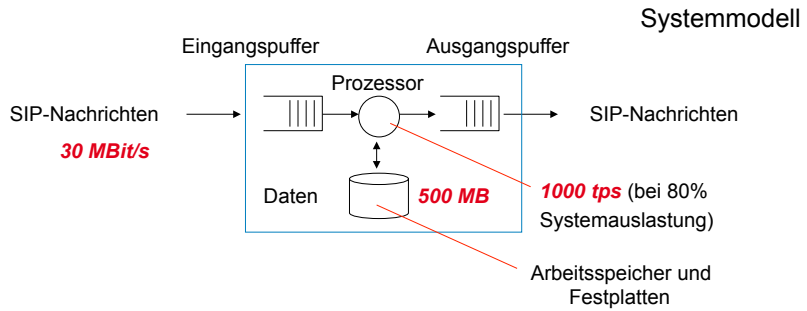
- Pro Transaktion: 3 Nachrichten mit 10 kBit Länge pro Nachricht
- 1000 Transaktionen pro Sekunde (Ergebnis siehe letzte Seite)
- 30 Mbit/s Durchsatz für Signalisierung (control traffic)

Datenbank:

- 500 Bytes pro Teilnehmer für Call States und Teilnehmerprofil (location, presence, service settings, …)
- 500 MByte Datenbank (Arbeitsspeicher & Disk)

Modell des Call Servers

DHBW Stuttgart



Nichtfunktionale Anforderungen:

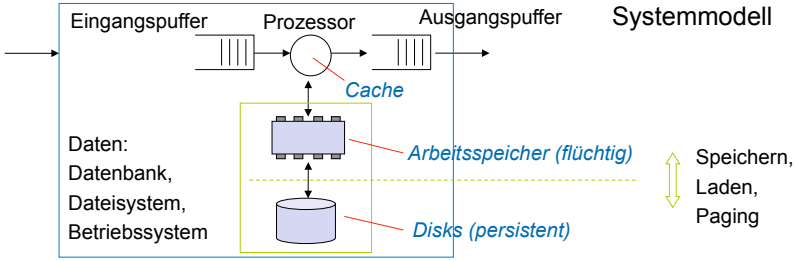
- Verfügbarkeit (Redundanz, Kapselung, …)
- Sicherheit (Schutz des Systems und der Daten)
- Konventionen bzgl. Bauweise (Umgebungsbedingungen: Temperatur, EMV, mechanische Beanspruchung, Schadstoffe, Brandverhalten, …)

EMV,: elektromagnetische Verträglichkeit (Einstrahlung, Abstrahlung, Spannungsspitzen, ...)

Verfeinerung des Modells

DHBW Stuttgart

Dauer der Transaktion



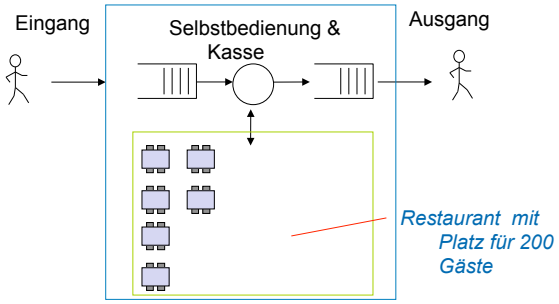
Wieviele gleichzeitig aktive Sessions gibt es?

- Aktive Sessions = Transaktionen pro Sekunde x Dauer der Transaktion
- Annahme: Telefonanruf dauert 100 Sekunden
- 1000 tps x 100 s = 100.000 aktive Sessions
- 500 Bytes per Session (Teilnehmerprofil) => 50 MB im Arbeitsspeicher

Zur Verweildauer der Transaktion

DHBW Stuttgart

Fast Food Restaurant



Mittlere Aufenthaltsdauer pro Gast: 15 Minuten

Frage: Wie viele Gäste pro Stunde (bzw. pro Minute) muss die Kasse bedienen können?

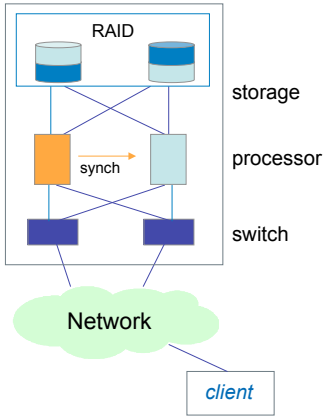
Nichtfunktionale Anforderungen

DHBW Stuttgart

Beispiel: 2x Redundanz als Designvorgabe

bzgl. Verfügbarkeit

- Speicher: Disks in RAID Konfiguration (z.B. RAID1)
- Prozessor:
  - Cluster-Konfiguration mit 2x Prozessoren
  - Datenbank im Arbeitsspeicher
  - Synchronisation der Arbeitsspeicher im Cluster
  - Switch-over und Fail-over mit gleichen IP-Adressen



Call Server - Zusammenfassung

DHBW Stuttgart

Funktionale Anforderungen

Verkehrsmodell (Erfahrungswerte):

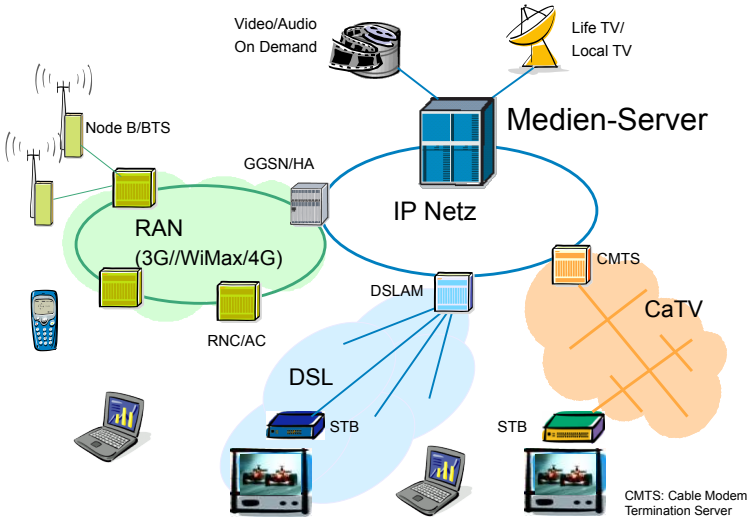
- 1 Mio Teilnehmer (subscribers)
- 500 kBytes Daten pro Teilnehmer (Teilnehmerprofil in der Datenbank)
- 4 Anrufe pro Teilnehmer in der Hauptverkehrsstunde
- 100 Sekunden Dauer pro Anruf
- 3 Nachrichten (in und out) pro SIP Transaktion
- 10 kBits pro Nachricht

Systemanforderungen (Ergebnis aus Vorgaben):

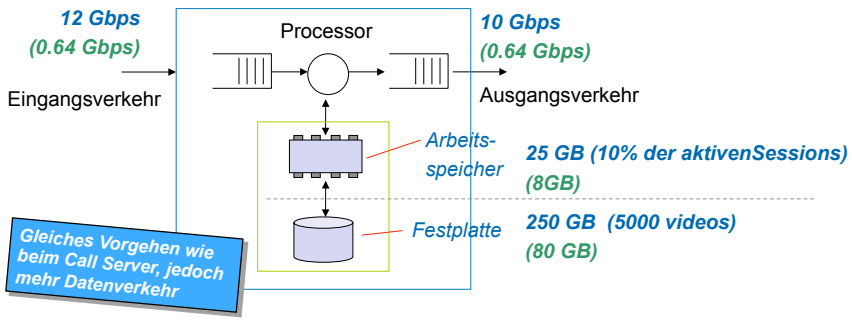
- 1000 tps (Transaktionen pro Sekunde)
- 30 Mbit/s Troughput für Call Control (SIP-Nachrichten)
- 500 MBytes Datenbank für Teilnehmerprofile
- 50 MBytes Arbeitsspeicher

Nichtfunktionale Anforderungen: Verfügbarkeit, Umgebungsbedingungen

Beispiel: Medien-Server



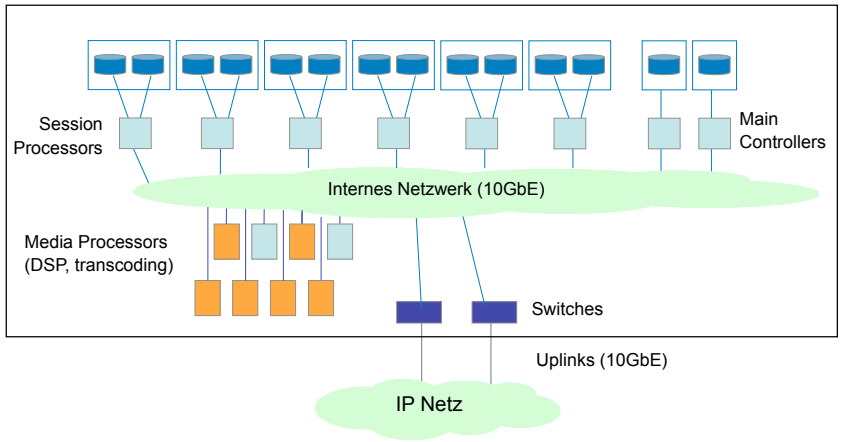
Modell des Medien-Servers



	Wireless Networks	Wireline Networks
200.000 Subscribers	128 kbps per session	2 Mbps per session
30 tps	640 Mbps total traffic	10 Gbps total traffic
180 s per transaction		
5000 parallel sessions		

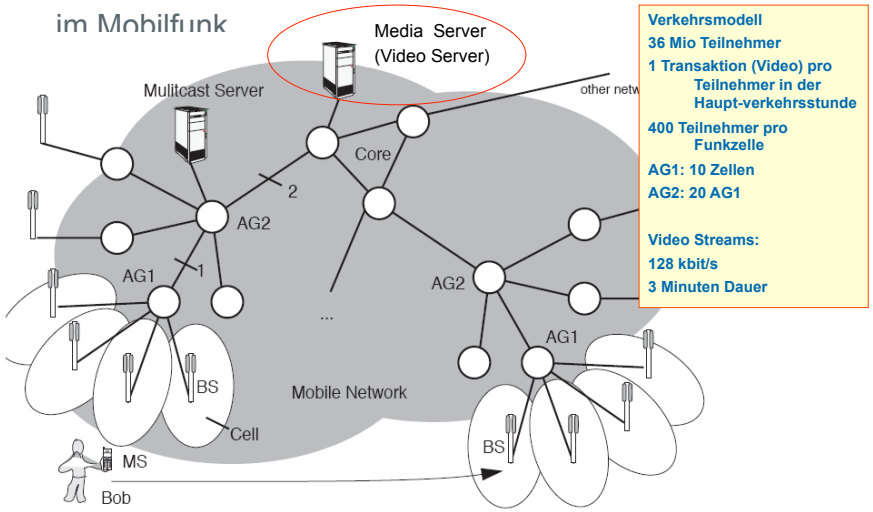
Verkehrsmodell

Systemarchitektur des Medien-Servers



DSP: Digitaler Signalprozessor (spezialisiert auf Bildverarbeitung bzw. Audioverarbeitung, beispielsweise zum umkodieren von Formaten)

Gymnastik - Medienserver …



Medienserver im Mobilfunk (2)

DHBW Stuttgart

Fragen

- Wie gross ist der Verkehr für Video-Streaming pro Funkzelle?
- Wieviele Transaktionen pro Sekunde (für Anfragen und Abspielen von Videos) muss der Media-Server bedienen?
- Welchen Verkehr (bit/s) muss der Media-Server bewältigen (gleichzeitig abgespielte Videos)?

Bonus-Stretch (Einschätzung):

- Funkzelle: Wie passt dieser Verkehr (Frage 1) zur Kapazität gängiger Mobilfunkstandards?
- Media-Server: Würde man diese Menge an Verkehr (Frage 3) mit einem einzigen System bedienen wollen?
- Media-Server: Kann man diese Art Server parallelisieren?

Inhalt

DHBW Stuttgart

Planung und Dimensionierung

- IP-basierte Netze
- Voice over IP
- Verkehrsmodelle und Systemdimensionierung
- Daten und Redundanz

Daten und Redundanz

DHBW Stuttgart

Anwendungsfall:

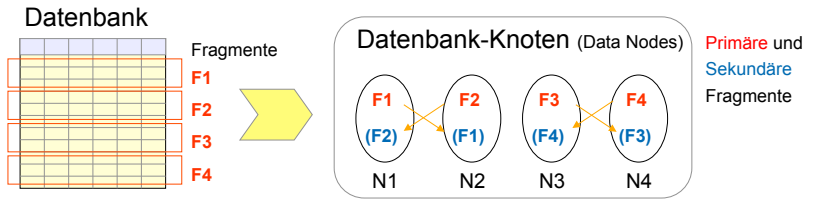
- Laufende Transaktionen werden im Arbeitsspeicher vorgehalten.
- Beispiele: Call Server, Home Location Register, Medien-Server
- Wegen der hohen Anzahl Teilnehmer fallen große Datenmengen an.

Aufgabe:

- Schutz dieser Daten gegen Ausfälle einzelner Server.
- Abspeichern auf Festplatte kommt wegen der diesbezüglichen Wartezeiten nicht in Frage.

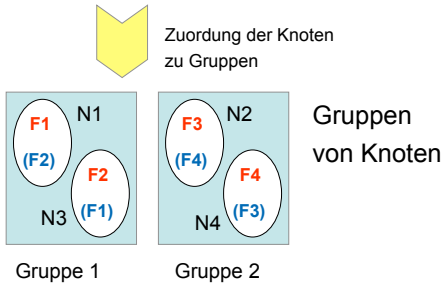
Lösung: Redundante Datenbank

DHBW Stuttgart



Verteilte Datenbank:

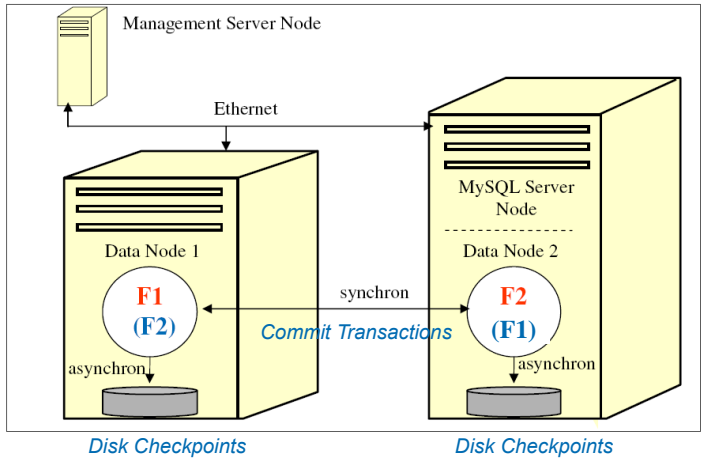
- Definiere Fragmente (F1, F2, …)
- Ordne Fragmente den Datenbank-Knoten inkl. Spiegel-Fragmenten zu (logische Organisation)
- Fragmente werden zwischen den Datenbank-Knoten auf pro Transaktion synchronisiert
- Ordne Datenbank-Knoten Gruppen von Knoten (Servern) zu (phys. Organisation)
- Datenbank verbleibt im Arbeitsspeicher mit Sicherung in definierten Zeitintervallen (Checkpoints) auf Festplatte



Beispiel: MySQL Cluster

DHBW Stuttgart

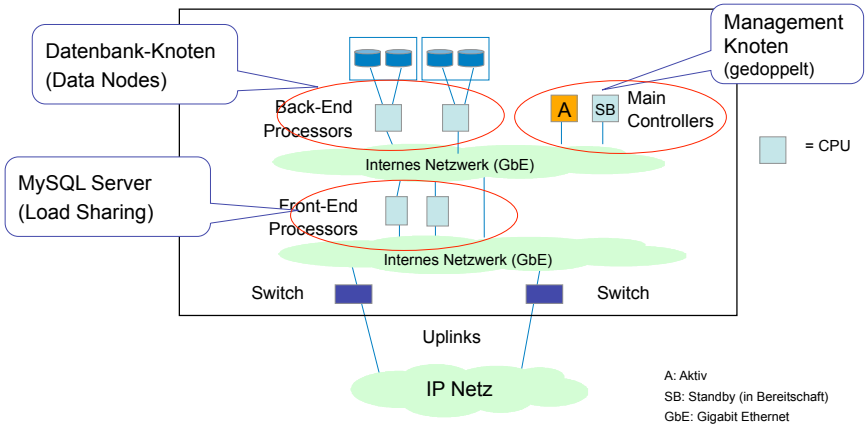
Minimale redundante Konfiguration



Systemarchitektur

DHBW Stuttgart

Server mit redundanter Datenbank



Aufgaben der Systemkomponenten

DHBW Stuttgart

Management Knoten:

- Starten alle Prozesse im Cluster
- Stellen Benutzerschnittstelle zur Verfügung

MySQL Server:

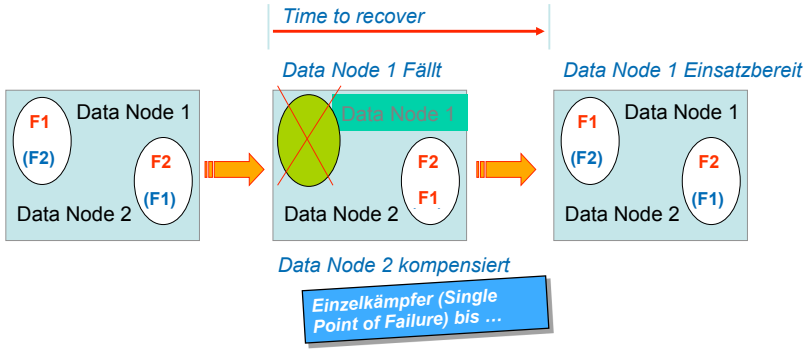
- Starten Leseanfragen und Schreibanfragen in den Datenbank-Knoten
- Arbeiten in Lastverteilung (load sharing)

Datenbank-Knoten:

- führen die redundante Datenbank,

Kritischer Pfad

DHBW Stuttgart



Verlust und Wiederherstellung (Recovery) eines Datenbank-Knoten:

- bei Verlust eines Knotens wird das Spiegel-Fragment im anderen Knoten aktiv
- jedoch ist das System jetzt nicht mehr redundant und daher gefährdet bis zur …
- … Wiederherstellung des verlorenen Datenbank-Knotens

Management Knoten:

- Konsequenz eines Verlustes: Keine Benutzerschnittstelle mehr, das Cluster arbeitet ohne Management weiter.
- Redundanz: Active/Standby

MySQL Server:

- Konsequenz eines Verlustes: Weniger Leistung, jedoch kein Datenverlust, da Anwendungen (= MySQL Server) und Daten (= Datenbank-Knoten) getrennt sind.
- Redundanz: N+1 mit Lastverteilung (Load Sharing)

Datenbank-Knoten:

- Konsequenz eines Verlustes: Kein Datenverlust, jedoch keine Absicherung mehr (Einzelkämpferposition des verbleibenden Spiegels), bis der Knoten wieder einsatzbereit ist.
- Redundanz: bis zu 3 Kopien der Daten (bis zu 3 Spiegel-Fragmente im Arbeitsspeicher)

ENDE Teil 4

Planung und Dimensionierung