DHBW Stuttgart

Kommunikationssysteme
Teil 1 - Ethernet

Stephan Rupp
Masterstudium Informations- und Kommunikationstechnik

www.dhbw-stuttgart.de

Inhalt

DHBW Stuttgart

Ethernet

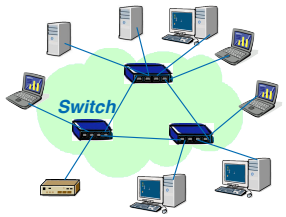
- Netzwerke: Beispiele, Adressierung
- Funktionsweise
- Operationen auf Layer 2 und Layer 3
- Ethernet Switches
- Systeme auf Layer 2 und Layer 3
- Protokolle

Netzwerke

DHBW Stuttgart

Lokale Netze (Local Area Networks)

- Arbeitsplatz
- Zuhause
- Telekommunikationsnetze
- Automatisierungstechnik
- Transport (Schiene, Luft, Wasser)
- Medizintechnik

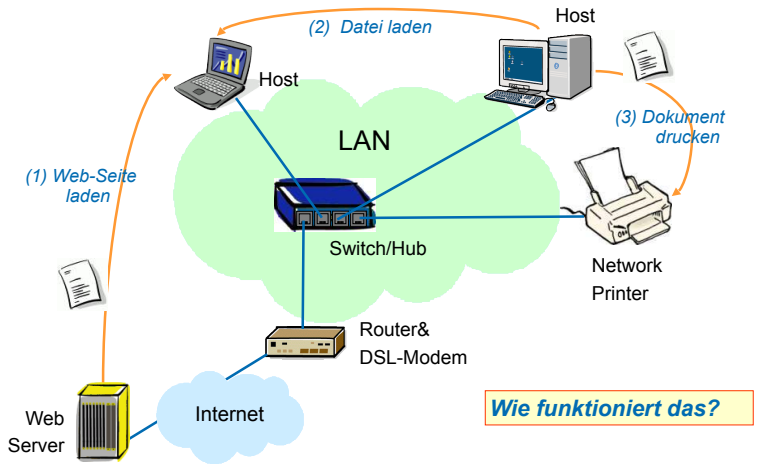


Lokales Netz = IP Subnetwork

- Teil des Internet bzw. privaten IP-Netzes
- Telekommunikationsnetze
  - Basis für IP basierte Dienste
  - Verkehrs-Aggregation über “Carrier Ethernet”

Beispiel: Heimnetz

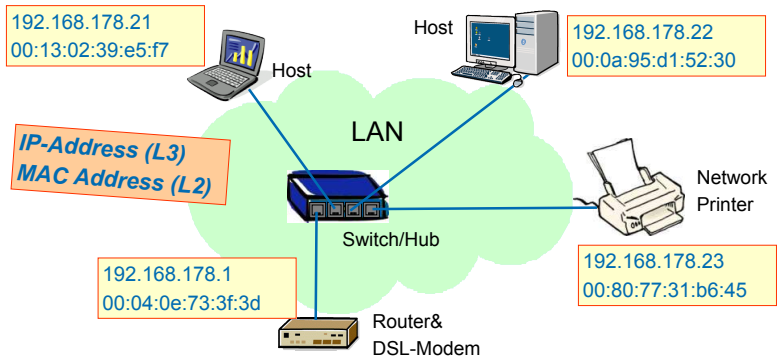
DHBW Stuttgart



Wie funktioniert das?

Adressen im Heimnetz

DHBW Stuttgart



- IP Adressen durch den Router dynamisch vergeben (DHCP)
- MAC Adressen vom Hertsller fest in die Netzwerkschnittstellen eingebaut

Inhalt

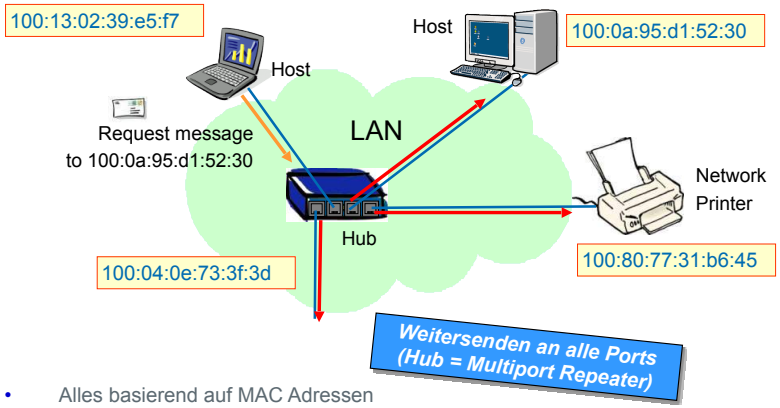
DHBW Stuttgart

Ethernet

- Netzwerke
- Funktionsweise: vom Hub zum Switch
- Operationen auf Layer 2 und Layer 3
- Ethernet Switches
- Systeme auf Layer 2 und Layer 3
- Protokolle

Funktionsweise Hub (1) – Anfrage

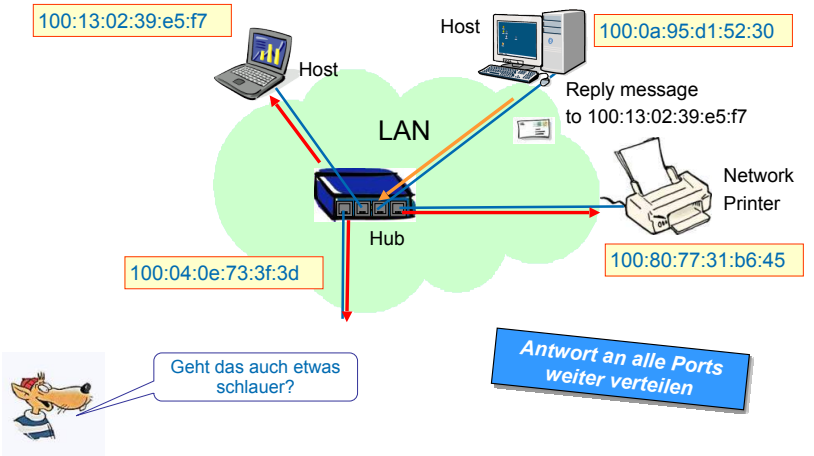
DHBW Stuttgart



- Alles basierend auf MAC Adressen
- Hub = Multiport Repeater

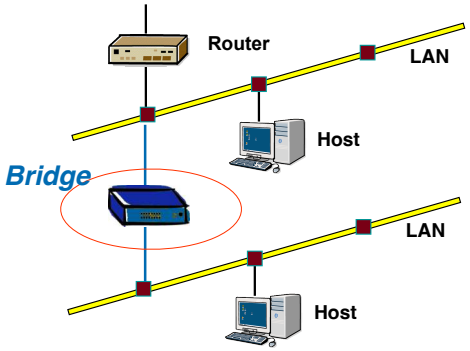
Funktionsweise Hub (2) – Antwort

DHBW Stuttgart



Vom Hub zur Bridge

DHBW Stuttgart



LAN Segment 1 (local traffic)

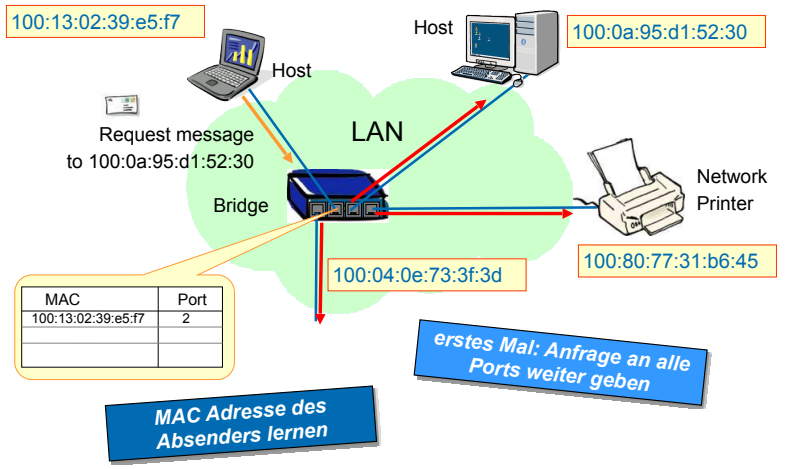
Traffic between segments

LAN Segment 2 (local traffic)

- Ein Hub "lötet" zwei LAN Segmente zusammen: jede Nachrícht wird an alle Ports weiter verteilt
- Eine Bridge "überspannt" zwei LAN Segmente: nur Nachrichten an Empfänger im jeweiligen Segment werden übermittelt

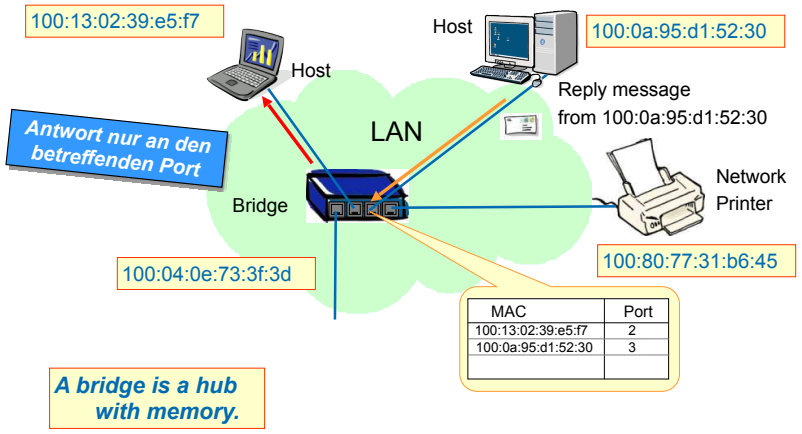
Funktionweise der Bridge – 1. Anfrage

DHBW Stuttgart



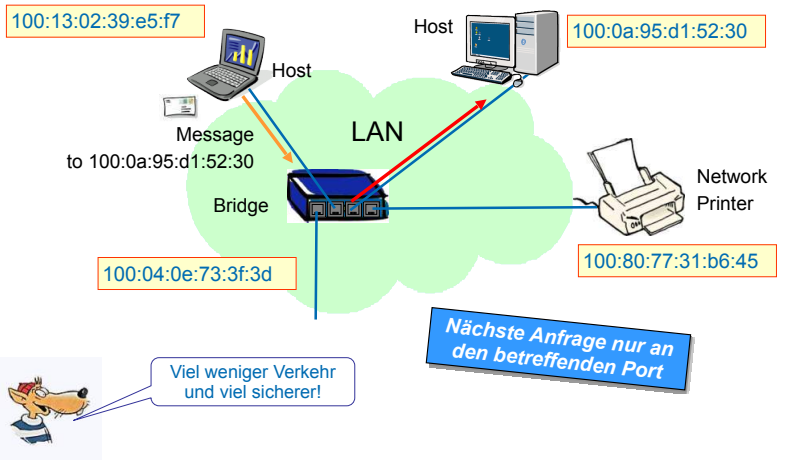
Funktionweise der Bridge – Antwort

DHBW Stuttgart



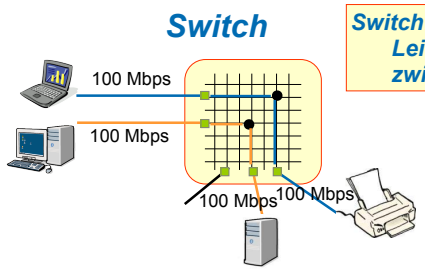
Funktionweise der Bridge – 2. Anfrage

DHBW Stuttgart



Hubs, Bridges und Switches

DHBW Stuttgart



Switch: Bridge mit voller Leitungs-Geschwindigkeit zwischen allen Ports

Inhalt

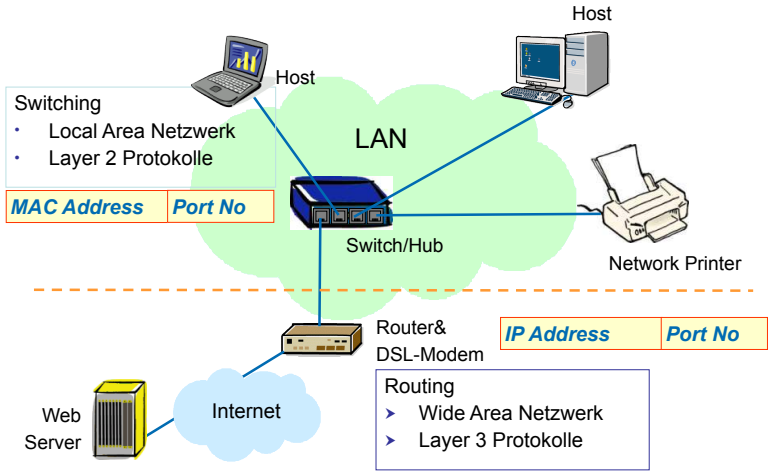
DHBW Stuttgart

Ethernet

- Netzwerke
- Funktionsweise
- Operationen auf Layer 2 und Layer 3
- Ethernet Switches
- Systeme auf Layer 2 und Layer 3
- Protokolle

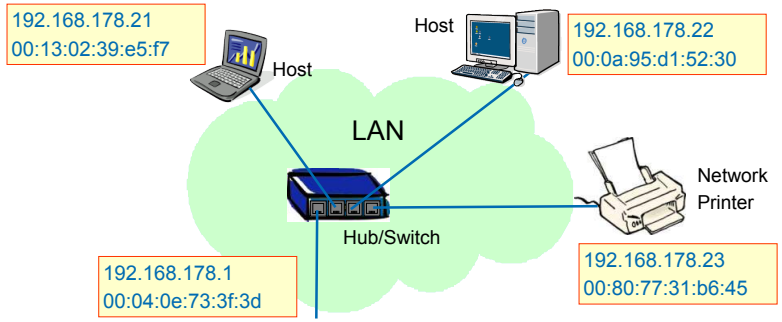
Switching (L2) und Routing (L3)

DHBW Stuttgart



IP Adressen als Host Identifier

DHBW Stuttgart

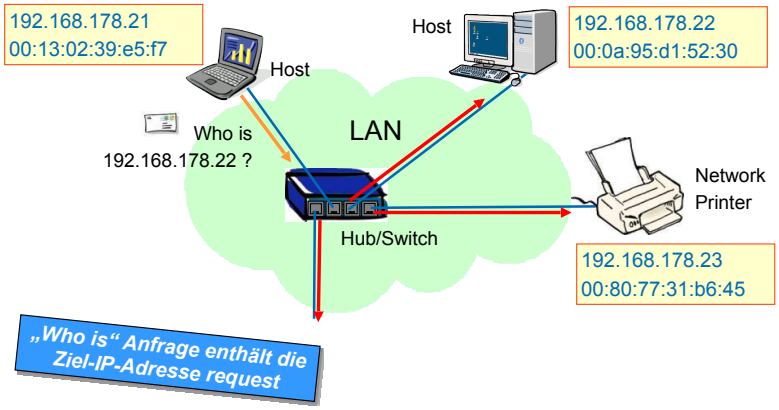


- IP Addresses: convenient host identifiers
- MAC addresses: used for message delivery

ARP (Address Resolution Protocol): Who is 192.168.178.22?

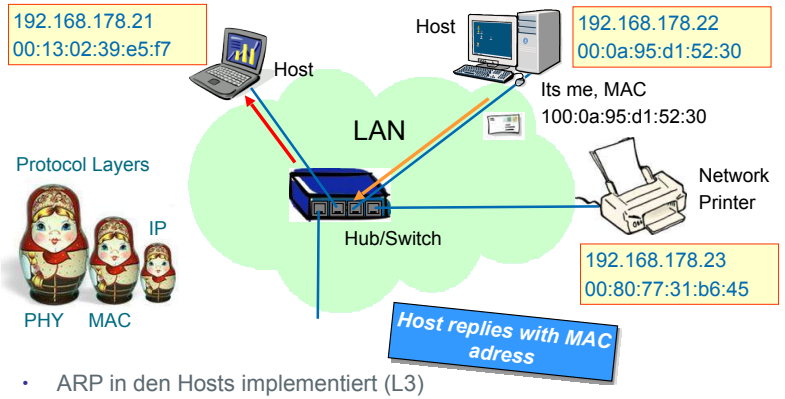
Address Resolution Protocol (1)

DHBW Stuttgart



Address Resolution Protocol (2)

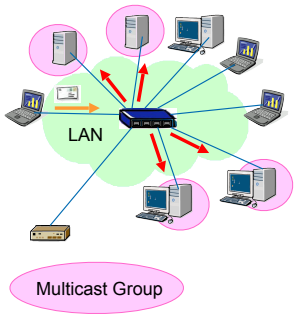
DHBW Stuttgart



- ARP in den Hosts implementiert (L3)
- löst IP-Adressen in MAC-Adressen auf
- Nur MAC-Adresses werden für die Zustellung verwendet (L2)

Mehr Tricks: Multicast

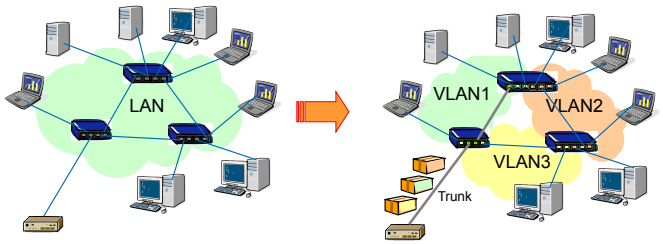
DHBW Stuttgart



- Nachricht an alle Mitglieder der Multicast-Gruppe weiterleiten
- Multicast = “Einer an Viele”
  - Broadcast = “Einer an Alle”
  - Unicast = “Einer an Einen”
- Multicast Adresse = Identifiziert eine Multicast Gruppe (Adress-Tabelle, Verteiler)

Noch mehr Tricks: Virtuelles LAN

DHBW Stuttgart



- Ports und Ethernet-Frames werden gruppiert (Tag = Markierung, Farbklecks)
- Segmentierung in einzelne, unabhängige Netze (LAN)
- Durch Aufteilung entsteht eine Umgebung mit reduzierter Komplexität.

Inhalt

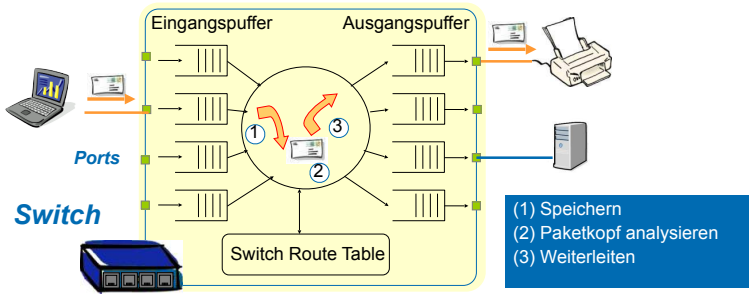
DHBW Stuttgart

Ethernet

- Netzwerke
- Funktionsweise
- Operationen auf Layer 2 und Layer 3
- Ethernet Switches
- Systeme auf Layer 2 und Layer 3
- Protokolle

Nachrichten Speichern und Weiterleiten

DHBW Stuttgart

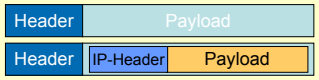


Nachrichtenverarbeitung im Switch

DHBW Stuttgart

Nachricht:

- Ethernet Rahmen (Frame)
- IP Paket (im Ehernet Rahmen)



Nachrichtenverarbeitung basiert auf Informationen im Paketkopf:

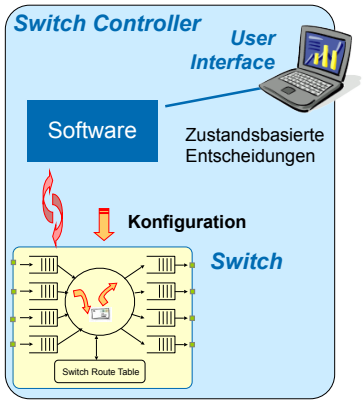
- MAC Adressen im Ethernet Paketkopf (Header)
- Option: Informationen im IP Peketkopf (Header)
- ebenso: VLAN tags, Quality of Service tags, …

Grenzen: Keine zustandsbasierten Entscheidungen möglich

- Sequenznummern für Rahmen oder Pakete
- Session IDs (Sitzungs-IDs) von Datenströmen
- Routen von IP-Paketen

Konfigurierbarer Switch

DHBW Stuttgart



Switch Controller:

- Konfigurationsparameter
- Benutzerschnittstelle (Command Line, GUI, MMI)
- Zustandsbasierte Entscheidungen

Implementierung:

- Software auf separatem Mikroprozessor
- setzt Register im Switch
- Kann für komplexe Routing – Aufgaben als Multi-Core CPU realisiert werden

Inhalt

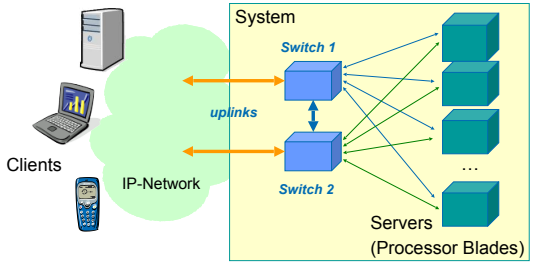
DHBW Stuttgart

Ethernet

- Netzwerke
- Funktionsweise
- Operationen auf Layer 2 und Layer 3
- Ethernet Switches
- Systeme auf Layer 2 und Layer 3
- Protokolle

Layer 2 Systemarchitektur

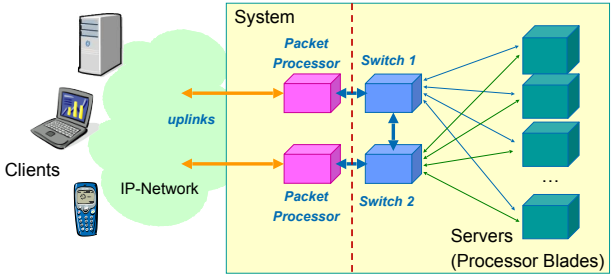
DHBW Stuttgart



- System: Server Farm (Pizza-Boxen plus Switch, bzw. Server Blades)
- Switches: in einfacher oder redundanter Konfiguration (Stern bzw. Doppel-Stern Topologie)
- Server direkt auf Layer 3 adressierbar (Switches = Layer 2, transparent)

Layer 3 Systemarchitektur

DHBW Stuttgart



- Vorgelagerte Paket-Prozessoren terminieren Layer 3
- Anwendungen: Load Balancing, SSL Entlastung, Verschlüsselung, Verarbeitung von TK-Sessions, Schutz (Fire Wall, Deep Packet Inspection, Anti-Virus), Routers, …
- Optionen: Redundanz zur Erhöhung der Verfügbarkeit im Fehlerfall

Inhalt

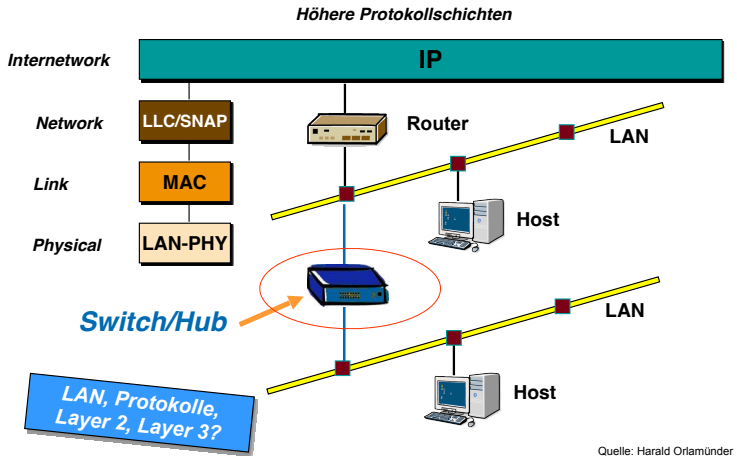
DHBW Stuttgart

Ethernet

- Netzwerke
- Funktionsweise
- Operationen auf Layer 2 und Layer 3
- Ethernet Switches
- Systeme auf Layer 2 und Layer 3
- Protokolle

Local Area Networks (LAN)

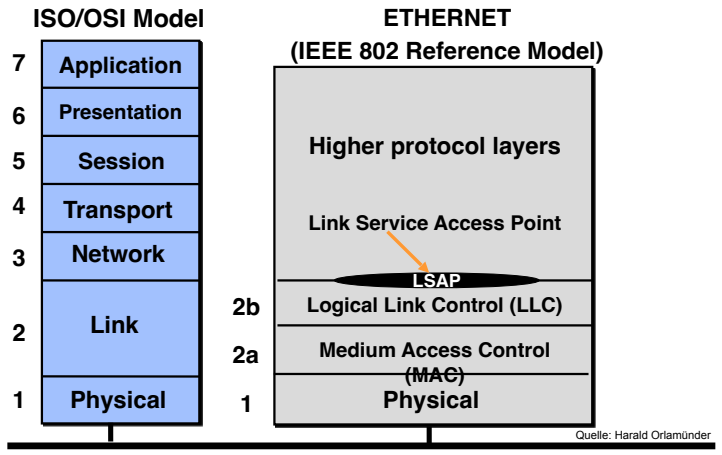
DHBW Stuttgart



Quelle: Harald Orlamünder

LAN - Protokolle

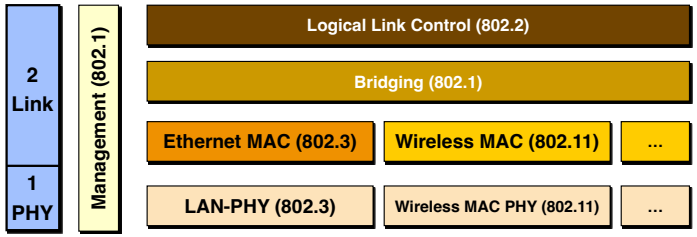
DHBW Stuttgart



Quelle: Harald Orlamünder

Local Area Network – IEEE Standards

DHBW Stuttgart

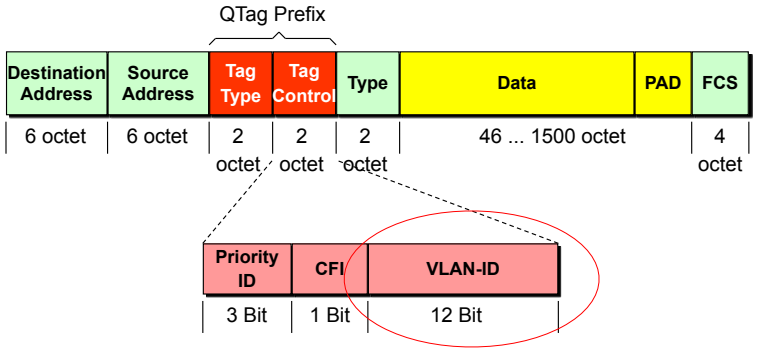


- Ebenfalls verfügbar zur Implementierung von Switches:
  - IEEE Referenzmodell
  - Verschiedene physikalische Layer (Coax, Copper Pairs, optical fibre), Übertraguns-Modi (half duplex, full duplex) und Geschwindigkeiten
  - Klassifikation zB. 10 BASE-5, 100 BASE-FX, …

Quelle: Harald Orlamünder

VLAN – Rahmenformat

DHBW Stuttgart



CFI Canonical Format Identifier
FCS Frame Check Sequence
PAD Padding

Konfigurierbarer Switch (L3 Switch)

DHBW Stuttgart

Konfigurierbarer Switch:

- hat eigene IP Adresse zum Anschluss eines Terminals zur Konfiguration
- Konfiguration über CLI (Command Line Interface), SNMP, TELNET

Ethernet/Bridging Protokolle (Layer 2)

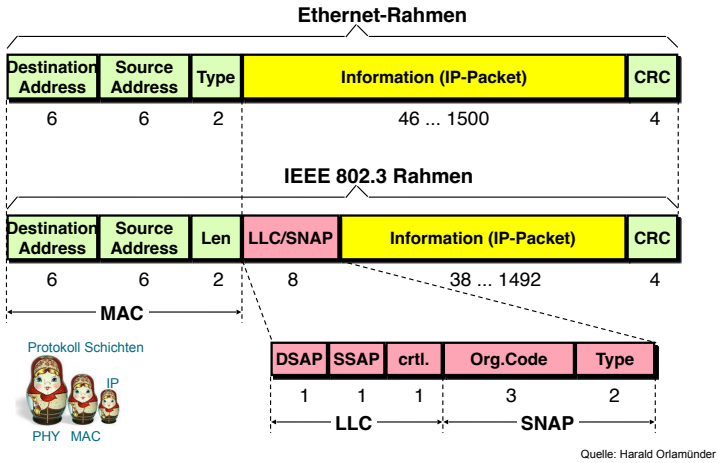
- Link aggregation (802.3ad), VLANs (802.1Q), Spanning Tree (802.1D, 802.1w), QoS (802.1p), Flow control (802.3x), GVRP, GMRP

IP Routing Protokolle (Layer 3)

- OSPFv2, RIPv2, VRRP, IGMP snooping, IPv4 forwarding, DiffServ, ARP, ICMP
- DCHP Client/Server: Empfang/Verteilung lokaler IP Adressen

Ethernet- und IEEE 802.3-Rahmen

DHBW Stuttgart



Quelle: Harald Orlamünder

Zuletzt: ARP-Demo

DHBW Stuttgart

Eine Demonstration der Funktionsweise des Address Resolution Protokolls (ARP) gibt es unter: https://www.youtube.com/watch?v=A7nih6SANYs

Bemerkungen:

- ARP ist ein sogenanntes “zustandsloses” Protokoll, d.h. das Protokoll kümmert sich nicht darum, ob eine Anfrage oder eine Antwort zur gleichen Transaktion gehören oder nicht
- Diese Eigenschaft macht ARP sehr leicht verwundbar gegen Lauschangriffe (Mithören bzw. Mitverfolgen aller Sessions, wie FTTP, VoIP, etc, sowie verwundbar gegen aktive Angriffe (Manipulierte Daten, Man in the Middle)
- Die Verwundbarkeit ist begrenzt auf das LAN bzw. IP-Subnetz
- Es gibt jedoch Angriffsmöglichkeiten auf allen Ebenen.

Quelle: Harald Orlamünder

Kommunikationssysteme

DHBW Stuttgart

ENDE Teil 1

Ethernet

DHBW Stuttgart

Kommunikationssysteme
Teil 2 – Ethernet basierte Feldbusse

Stephan Rupp
Masterstudium Informations- und Kommunikationstechnik

www.dhbw-stuttgart.de

Inhalt

DHBW Stuttgart

Ethernet basierte Feldbusse

- Vom Multiport-Repeater zum Ethernet-Switch
- Ethernet-Switches: Funktionsweise und Leistungsmerkmale
- Anforderungen im industriellen Einsatz
- Lösungsansätze für den industriellen Betrieb
- Realisierungsbeispiele

Inhalt

DHBW Stuttgart

Ethernet basierte Feldbusse

- Vom Multiport-Repeater zum Ethernet-Switch
- Ethernet-Switches: Funktionsweise und Leistungsmerkmale
- Anforderungen im industriellen Einsatz
- Lösungsansätze für den industriellen Betrieb
- Realisierungsbeispiele

Ethernet – Projekt 802 der IEEE

DHBW Stuttgart

Evolutionärer Ansatz seit den 80-er Jahren

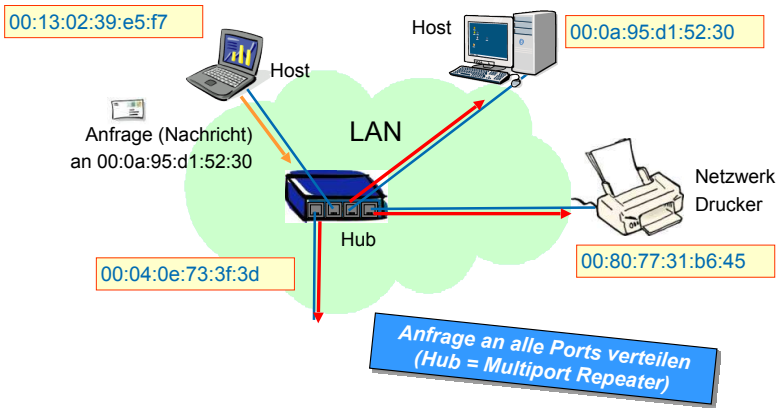
- Basisdefinition der beiden Layer 2-Protokollschichten MAC (Medium Access Control, IEEE 802.3) und LLC (Logical Link Control, IEEE 802.2),
- bei Bedarf ergänzt um höhere Steuerungsprotokolle (IEEE 802.1 unter anderem mit den Spanning Tree Protokollen, VLAN oder portbasierender Zugangskontrolle),
- ergänzt um anwendungsorientierte Erweiterung (IEEE 802.4 und höher).

Zwanglose Handhabung von Erweiterungen

- IEEE 802.11 definiert z.B. Wireless LAN MAC (als Ergänzung zu 802.3 LAN MAC), inklusive passender schnurloser Layer 1 Protokollschichten
- Link Aggregation (802.3ad), VLANs (802.1Q), Spanning Tree (802.1D, 802.1w), QoS (802.1p), Flusskontrolle (802.3x), sowie GVRP (Dynamic VLAN Registration) und GMRP (Dynamic L2 Multicast Registration)

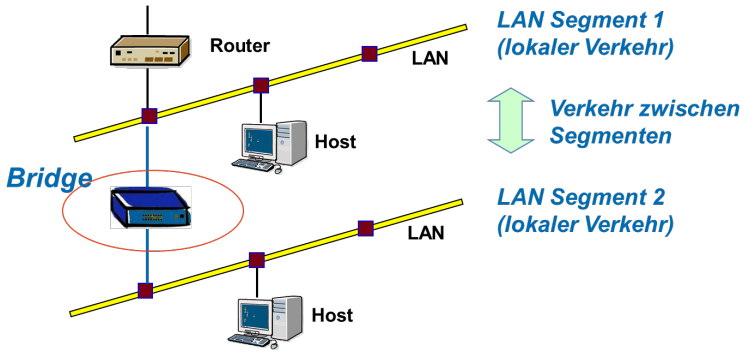
Netzwerk mit MAC Adressen

DHBW Stuttgart



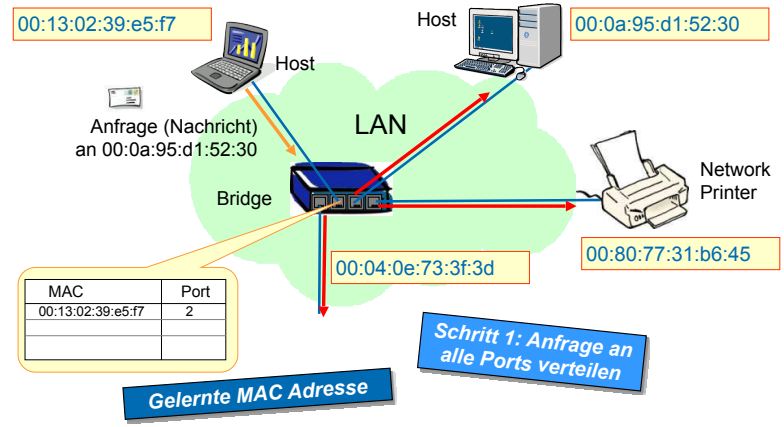
Verkehrsfluss in LAN-Segmenten

DHBW Stuttgart



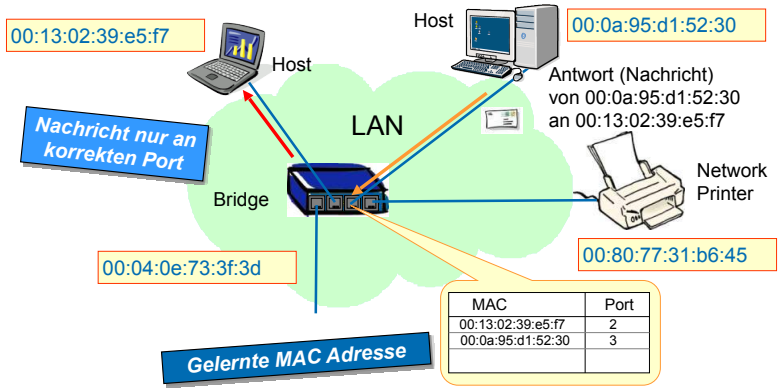
Lernen von MAC-Adressen (1)

DHBW Stuttgart



Lernen von MAC-Adressen (2)

DHBW Stuttgart



Inhalt

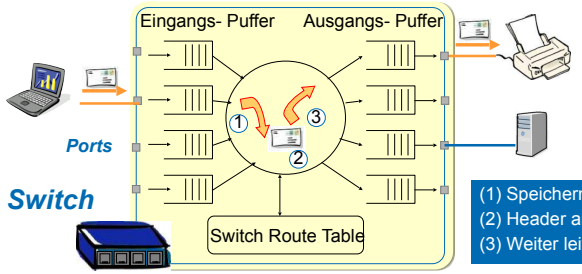
DHBW Stuttgart

Ethernet basierte Feldbusse

- Vom Multiport-Repeater zum Ethernet-Switch
- Ethernet-Switches: Funktionsweise und Leistungsmerkmale
- Anforderungen im industriellen Einsatz
- Lösungsansätze für den industriellen Betrieb
- Realisierungsbeispiele

Nachrichten speichern und weiterleiten

DHBW Stuttgart



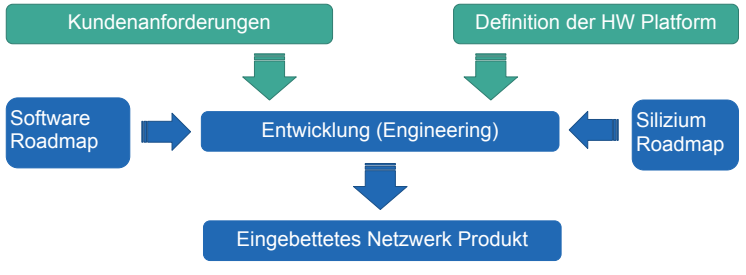
Nachricht:

- Ethernet Rahmen (Frame)
- IP Packet (im Ethernet Rahmen)

Header	Nutzdaten
Header	IP-Header Nutzdaten

Switches für den industriellen Einsatz

DHBW Stuttgart



Quelle: Kontron

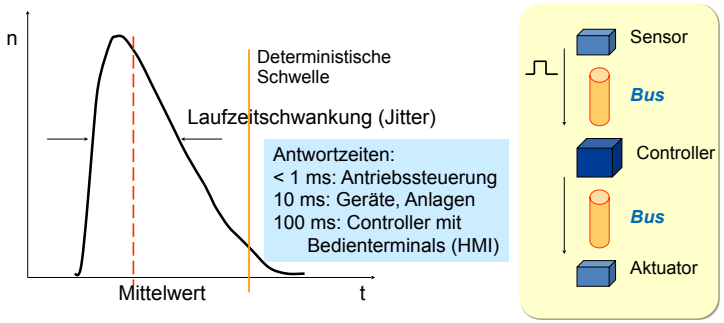
Inhalt

DHBW Stuttgart

Ethernet basierte Feldbusse

- Vom Multiport-Repeater zum Ethernet-Switch
- Ethernet-Switches: Funktionsweise und Leistungsmerkmale
- Anforderungen im industriellen Einsatz
- Lösungsansätze für den industriellen Betrieb
- Realisierungsbeispiele

Anforderungen im industriellen Einsatz



- Echtzeit = definierte Antwortzeiten
- Hohe Systemverfügbarkeit mit hinreichend kurzen Umschaltzeiten

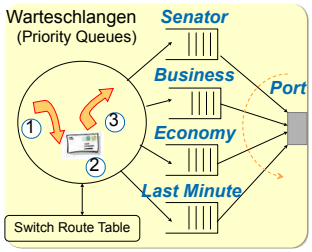
Inhalt

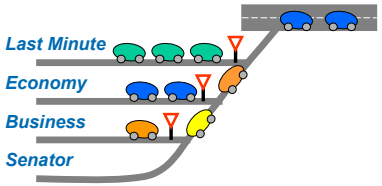
Ethernet basierte Feldbusse

- Vom Multiport-Repeater zum Ethernet-Switch
- Ethernet-Switches: Funktionsweise und Leistungsmerkmale
- Anforderungen im industriellen Einsatz
- Lösungsansätze für den industriellen Betrieb
- Realisierungsbeispiele

Vorfahrt für Prozessdaten

- Verkehrsklassen mit Priorisierung (Quality of Service)

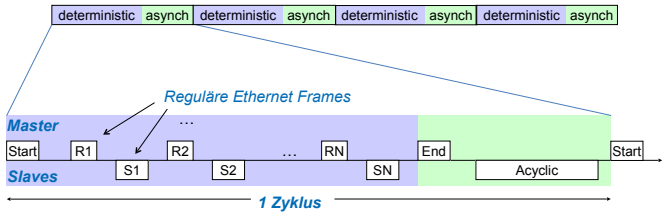




- Überschaubarer Verkehr bei Prozessdaten (Menge, Zyklus)
- Interferenz mit Verkehr niedriger Klassen ist unvermeidlich, jedoch planbar (abhängig von maximaler Paketlänge, Übertragungsrate und Netztopologie)

Orchestrierung – deterministischer Bus

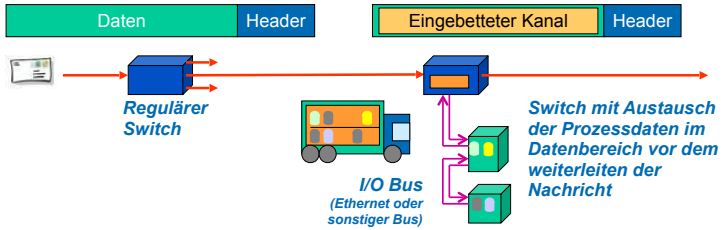
- Zeitmultiplex zwischen Prozessdaten und allen anderen Daten
- Bus-Master organisiert die Kommunikation der Prozessdaten zwischen Sendern und Empfängern.



Eingebetteter Kanal

DHBW Stuttgart

Prozessdaten als gemeinsames Telegramm im Datenbereich



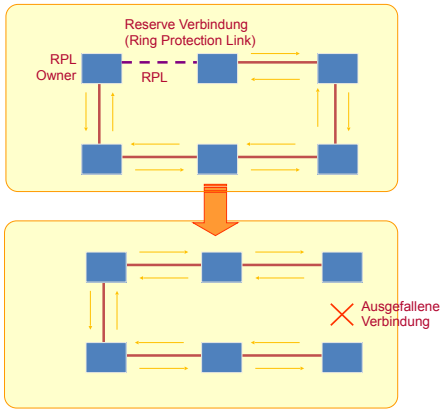
DEMO

- Standard Ethernet Rahmen
- Topologie: Verkettung aller Teilnehmer in einem Busabschnitt, ein Telegramm für alle anstelle einzelner Nachrichten
- Austausch der Prozessdaten beim weiterleiten des Ethernet Rahmens (erfordert spezielle Hardware für alle Teilnehmer)

Ringredundanz

DHBW Stuttgart

- Sternförmige Verkabelung ist nicht praktikabel, lineare Topologie
- Ring mit Reserve-verbindung (Ring Protection Link), die bei Verlust einer Verbindung aktiviert wird
- Überwachung des Betriebs durch Redundanz-Manager (RPL-Owner)
- Umschaltung auf die neue Topologie im Fehlerfall unter 500 ms



Inhalt

DHBW Stuttgart

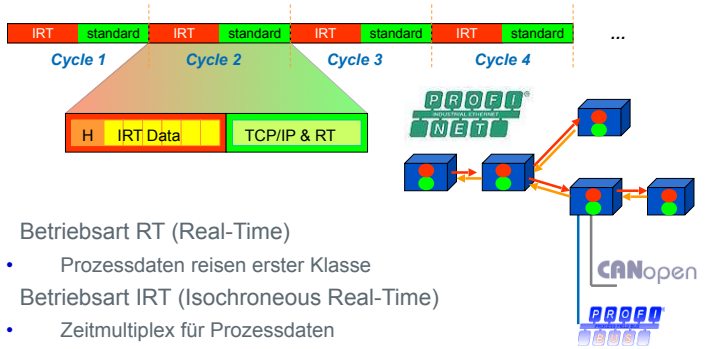
Ethernet basierte Feldbusse

- Vom Multiport-Repeater zum Ethernet-Switch
- Ethernet-Switches: Funktionsweise und Leistungsmerkmale
- Anforderungen im industriellen Einsatz
- Lösungsansätze für den industriellen Betrieb
- Realisierungsbeispiele

Profinet – Klassen und Zeitmultiplex

DHBW Stuttgart

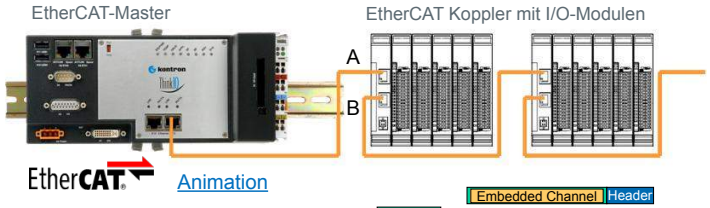
- Bestandteil von IEC 61158 und IEC 61784-2

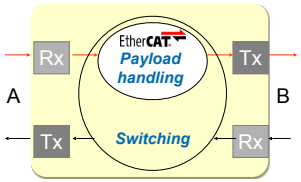


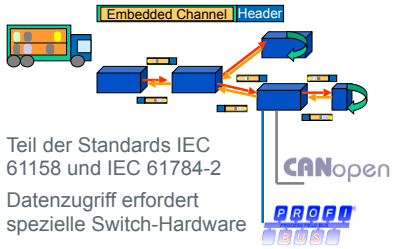
- Betriebsart RT (Real-Time)
  - Prozessdaten reisen erster Klasse
- Betriebsart IRT (Isochroneous Real-Time)
  - Zeitmultiplex für Prozessdaten
  - Zeitmultiplex erfordert spezielle Switch-Hardware

Ethercat – Eingebetteter Kanal

DHBW Stuttgart







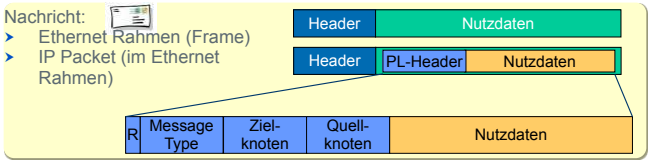
- Teil der Standards IEC 61158 und IEC 61784-2
- Datenzugriff erfordert spezielle Switch-Hardware

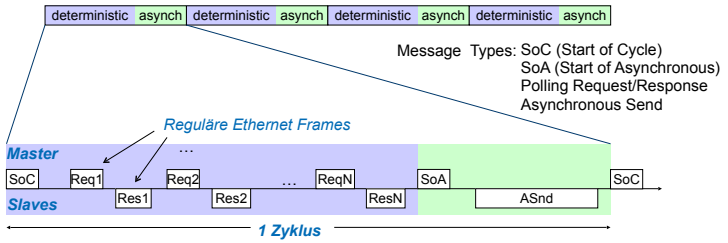
Ethernet POWERLINK

DHBW Stuttgart

Orchestrierung in Layer 3

Nachricht:
- Ethernet Rahmen (Frame)
- IP Packet (im Ethernet Rahmen)



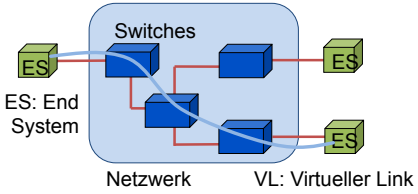


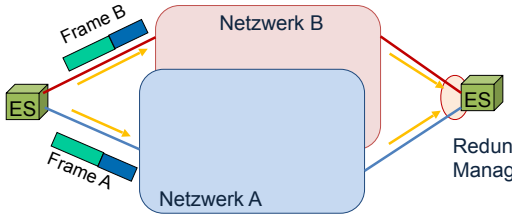
AFDX

DHBW Stuttgart

Avionics Full-Duplex Switched Ethernet

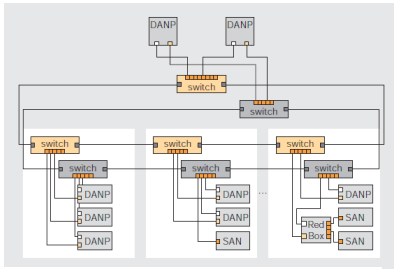
- ARINC 664 Standard
- Evolutionär
- Statische Konfiguration der Netzwerke (VL)
- Redundanter Betrieb zweier Netzwerke (full-duplex) ohne Umschaltzeiten





Elektrische Schaltanlagen

DHBW Stuttgart

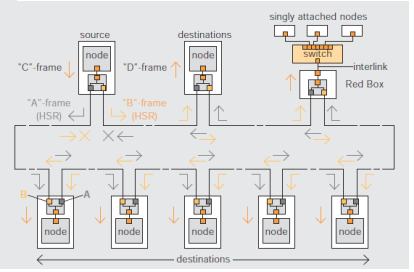


Doppelring mit Doppelstern
Parallel Redundancy Protocol (PRP)

HSR: High-Availbility Seamless Redundancy
MRP: Media Redundancy Protocol

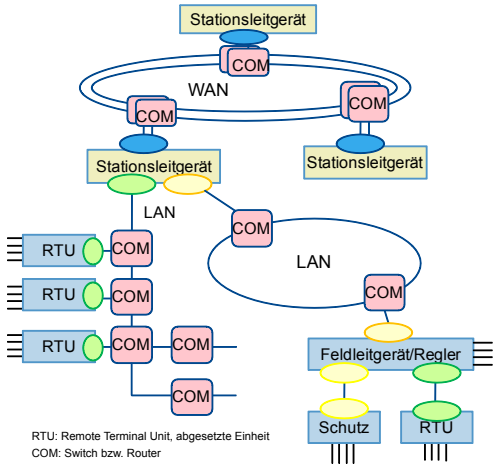
Quelle: ABB

Ringredundanz
Protokolle: HSR, MRP



Netztopologien

DHBW Stuttgart



Fernwirken (Wide Area Network, IP/ Ethernet):

redundante Verbindungen

- Doppelstern
- Doppelring

Lokales Netz (Local Area Network, Ethernet):

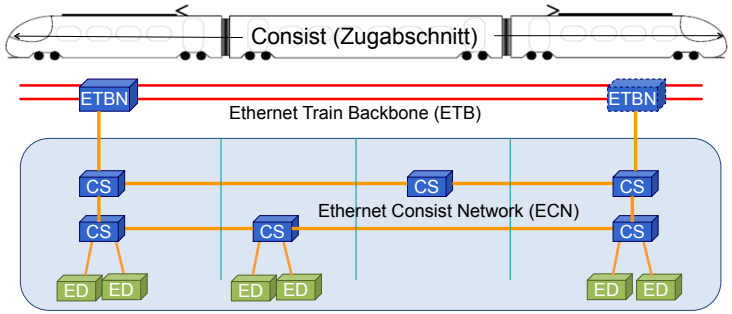
einfache und redundante Verbindungen

- Baumstruktur
- Ringstrruktur

TCN – Train Communication Network

DHBW Stuttgart

- IEC Norm 61375-1, Erweiterung auf 61375-4 (Ethernet Consist Network) und 61375-2-5 (Ethernet Train Backbone) in Arbeit, evolutionär



Besonderheit: dynamische Netzkonfiguration auf L3 basierend auf URIs

ETBN: Ethernet Train Backbone Node (Router) CS: Car Switch, Consist Switch (Ethernet Switch) ED: End Device

Zusammenfassung

DHBW Stuttgart

- Ethernet hat eine beispiellose Erfolgsgeschichte, nicht zuletzt wegen seines evolutionären Ansatzes.
- Ethernet ist als Feldbus zunehmen im Einsatz
  - Profinet, Ethercat, Ethernet Powerlink, Ethernet/IP, Sercos III, …
  - AFDX (Avionik), TCN (Bahnfahrzeuge), elektrische Schaltanlagen (IEC61850, MRP, HRS, PRP), …
- Anforderungen im industriellen Einsatz
  - Echtzeit = definierte Antwortzeiten
  - Verfügbarkeit (Redundanz für den Fehlerfall)
  - Die Anforderungen sind auf evolutionäre oder proprietäre Weise erfüllbar.
- Anforderungen auf Systemebene
  - Funktionale Sicherheit (Protokolle auf Anwendungsebene)
  - Schutz der Vertraulichkeit, Integrität und Authentizität.

Kommunikationsysteme

DHBW Stuttgart

ENDE Teil 2

Ethernet basierte Feldbusse

DHBW Stuttgart

Kommunikationssysteme
Teil 3 - Weitverkehrsnetze

Stephan Rupp
Masterstudium Informations- und Kommunikationstechnik

www.dhbw-stuttgart.de

Inhalt

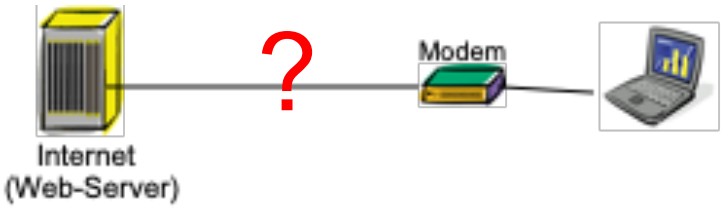
DHBW Stuttgart

Kommunikationssysteme - Einführung

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

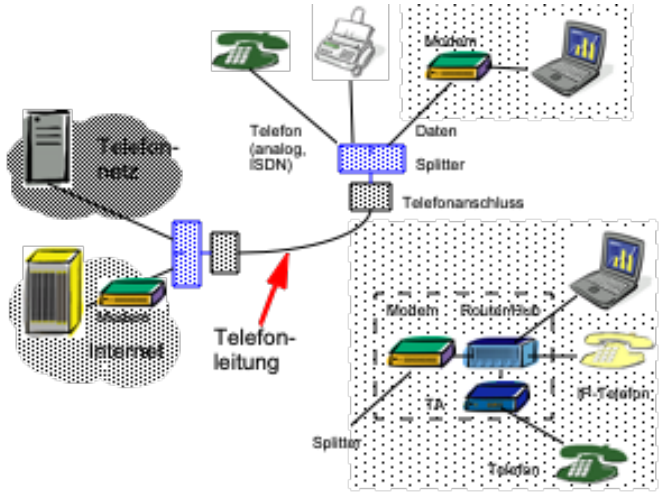
Was wissen wir über Netze?

DHBW Stuttgart



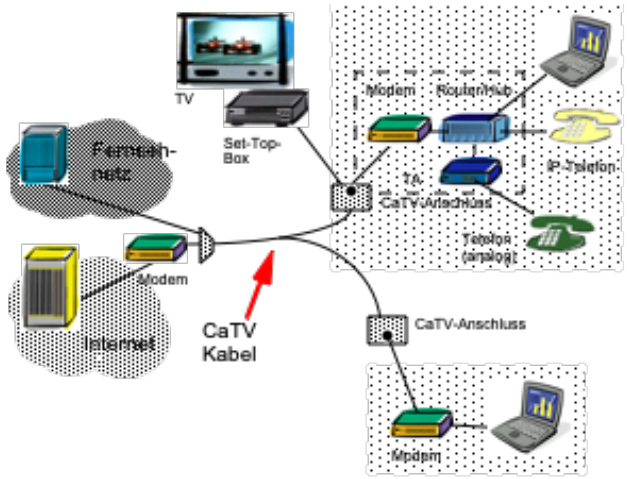
DSL - Was steckt dahinter?

DHBW Stuttgart



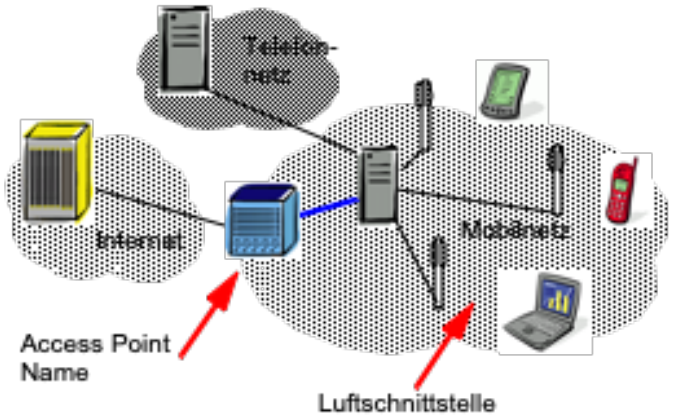
CaTV - Was steckt dahinter?

DHBW Stuttgart



Händi - Was steckt dahinter?

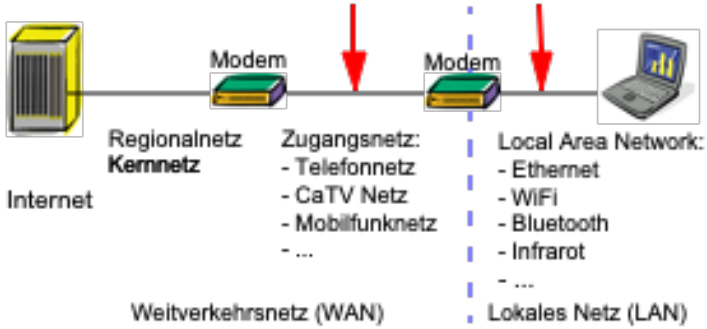
DHBW Stuttgart



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

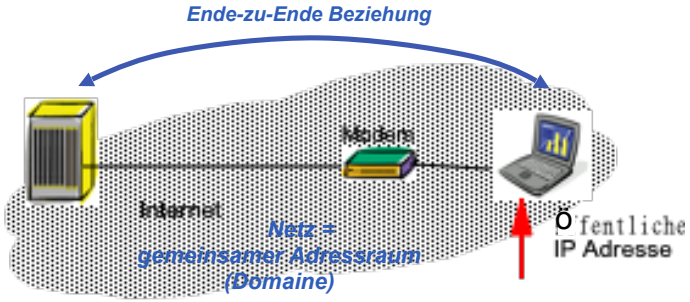
Funktionen, z.B. Mobilitätsverwaltung

- gleiche Funktionen
- viele unterschiedliche Implementierungen

Geografische Netzausprägung

Netze als Wölkchen

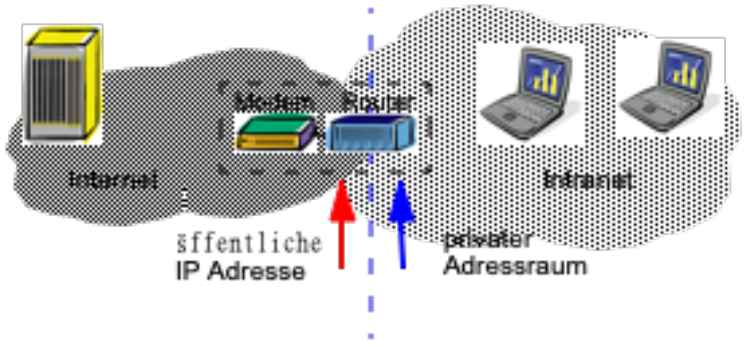
DHBW Stuttgart



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

Adressräume spannen Netze auf

DHBW Stuttgart



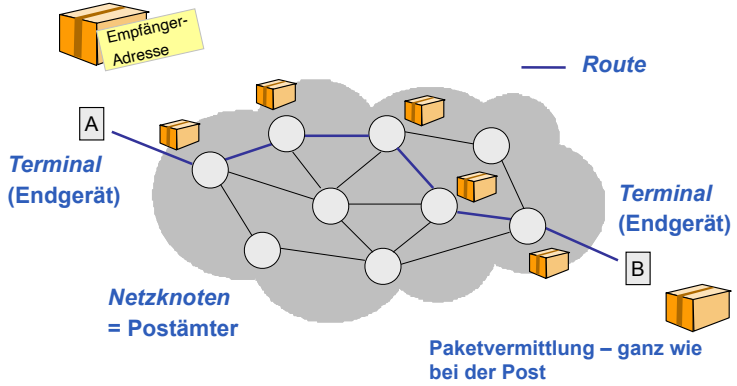
Das Händi als Modem

DHBW Stuttgart

In welchem Netz befindet sich das Gerät?

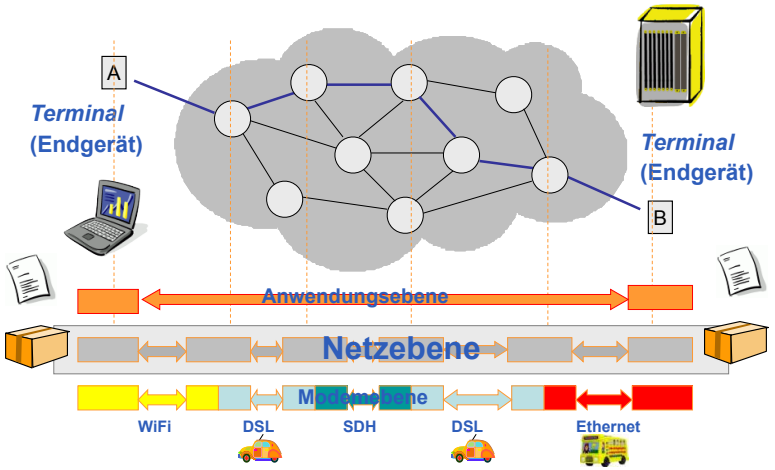
Schichtenmodell – Netzebene

DHBW Stuttgart



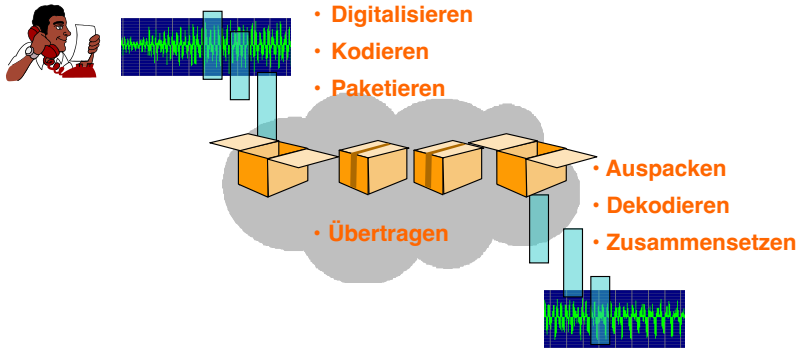
Schichtenmodell

DHBW Stuttgart



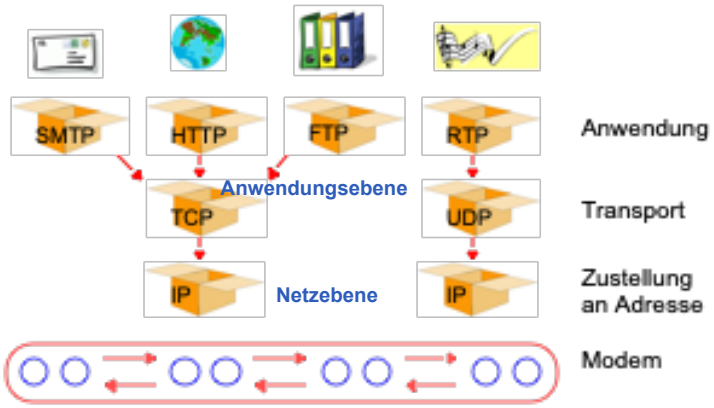
Anwendungsebene - Sprachpakete

DHBW Stuttgart



Schichtenmodell - Internet

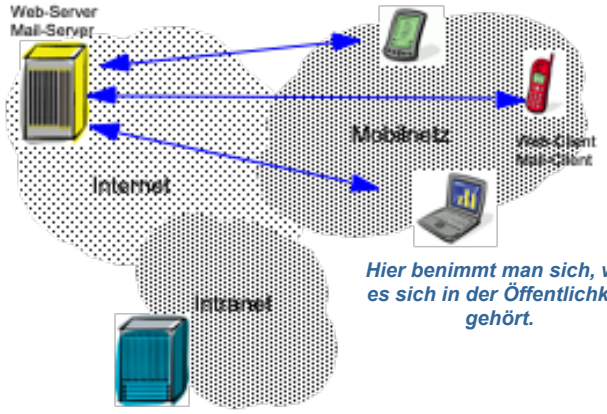
DHBW Stuttgart



Ganz unten durch: Leitungen und Luft

Öffentlicher Verkehr

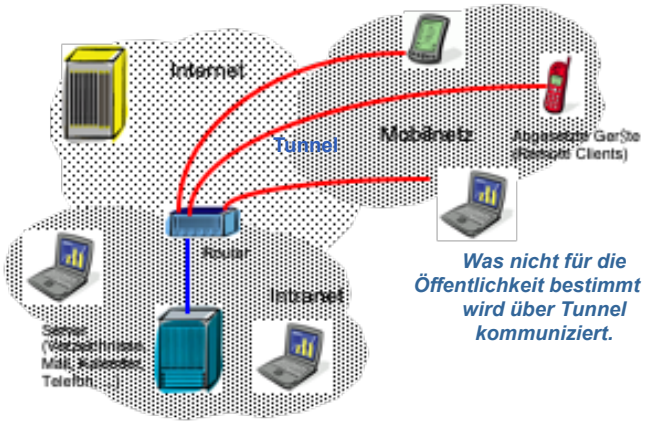
DHBW Stuttgart



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.

Inhalt

DHBW Stuttgart

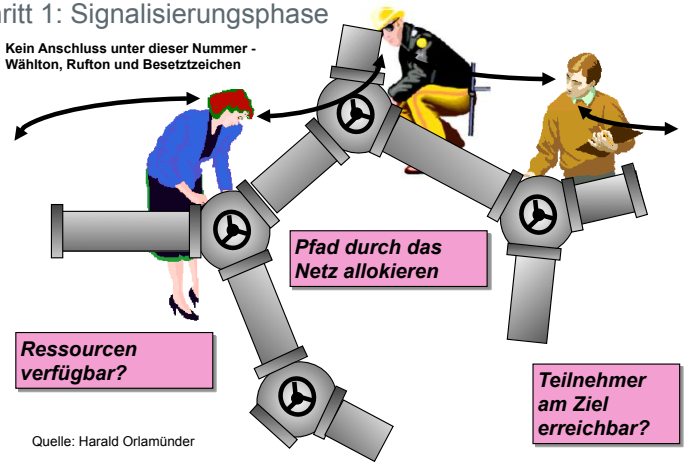
Technik der Netze - Einführung

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

Leitungsvermittlung

DHBW Stuttgart

Schritt 1: Signalisierungsphase

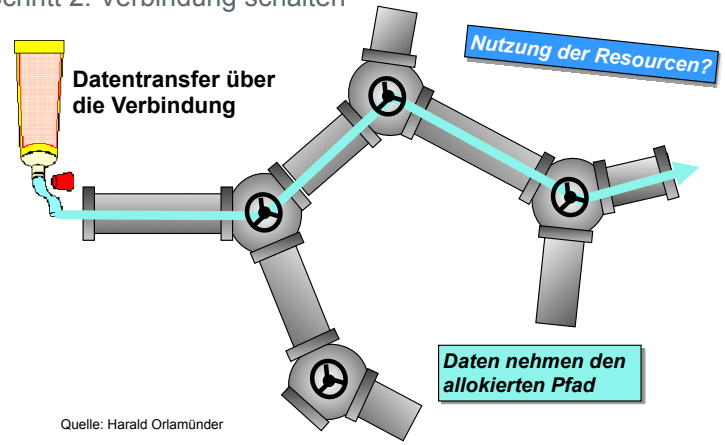


Quelle: Harald Orlamünder

Leitungsvermittlung

DHBW Stuttgart

Schritt 2: Verbindung schalten

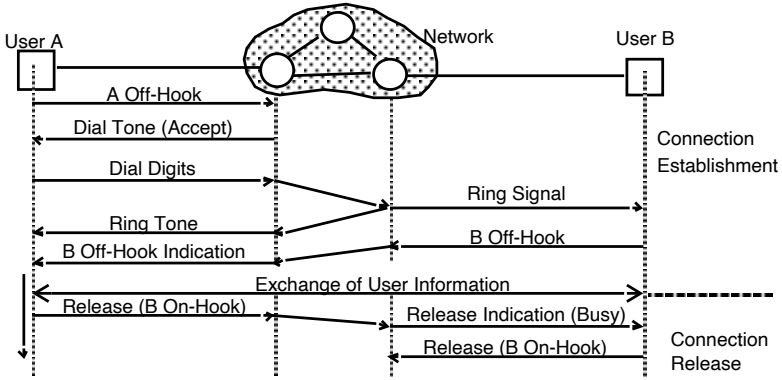


Quelle: Harald Orlamünder

Leitungsvermittlung

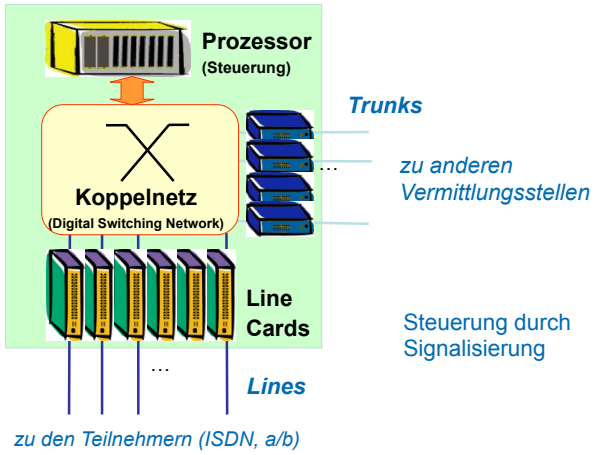
DHBW Stuttgart

Noch einmal: Schritt 1 und Schritt 2



Aufbau eines Vermittlungssystems

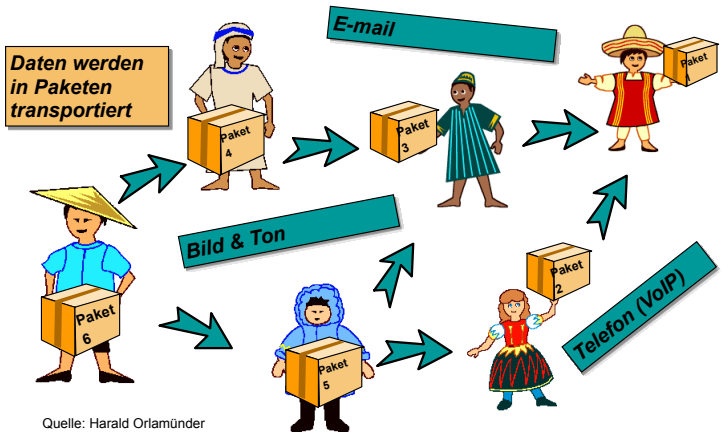
DHBW Stuttgart



Paketvermittlung

DHBW Stuttgart

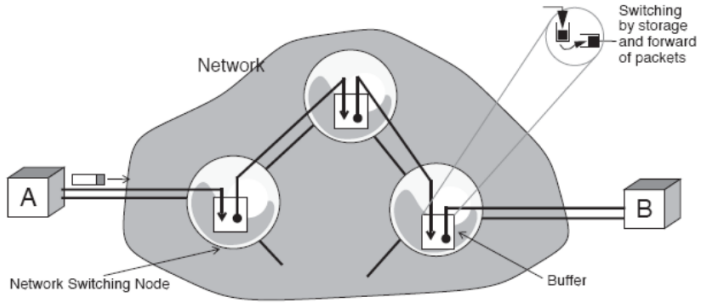
„Fein geschnitten und in Stücken“



Quelle: Harald Orlamünder

Postamt: Storage & Forward Routing

DHBW Stuttgart



Quelle: Gerd Siegmund

Inhalt

DHBW Stuttgart

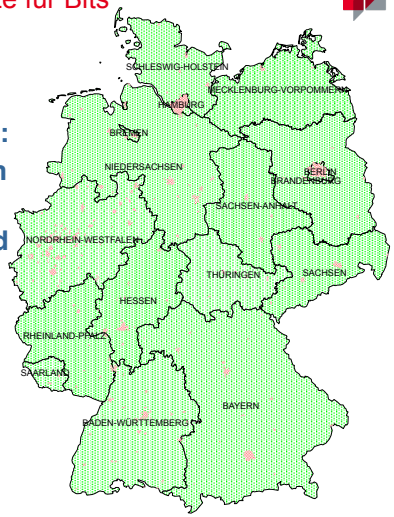
Technik der Netze - Einführung

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

Verkehrsnetze für Bits

DHBW Stuttgart

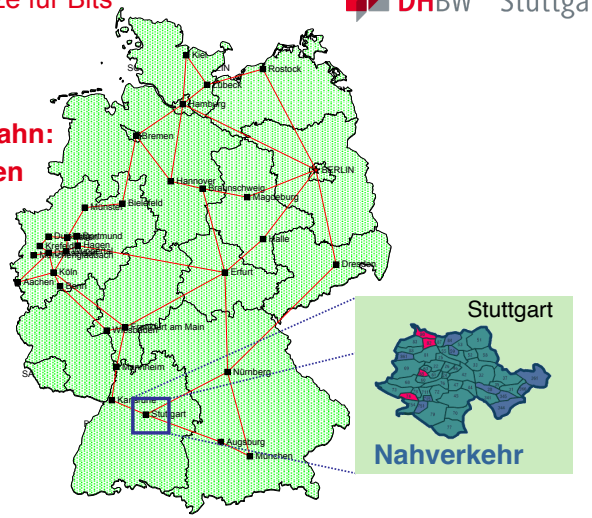
Ein Beispiel: die grössten Städte in Deutschland



Verkehrsnetze für Bits

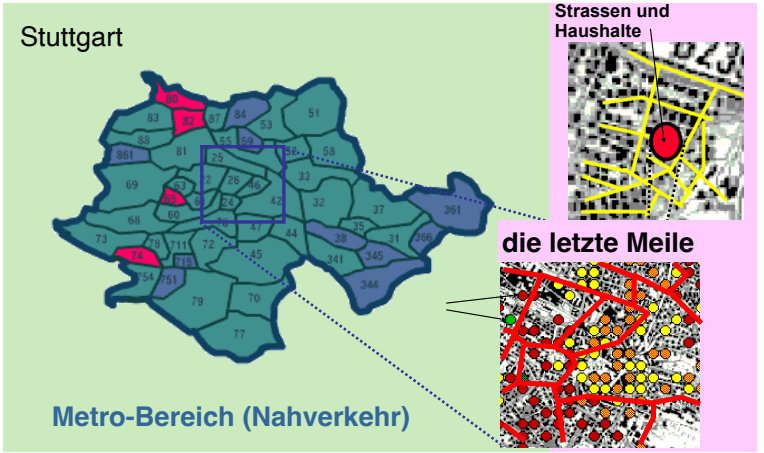
DHBW Stuttgart

Datenautobahn: zwischen den grössten Städten



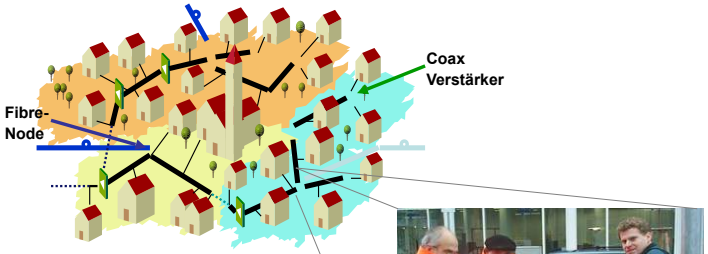
Nahverkehr und letzte Meile

DHBW Stuttgart



Zum Beispiel Kabel-TV Netze

DHBW Stuttgart



Ein zellulares Netz.

Braucht man das für Verteildienste (Broadcast)?

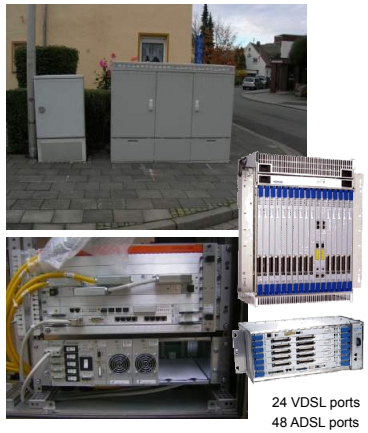
Quelle: Alcatel

Zum Beispiel DSL-Netze

DHBW Stuttgart

vorher

nachher



Source: Wikipedia, Web

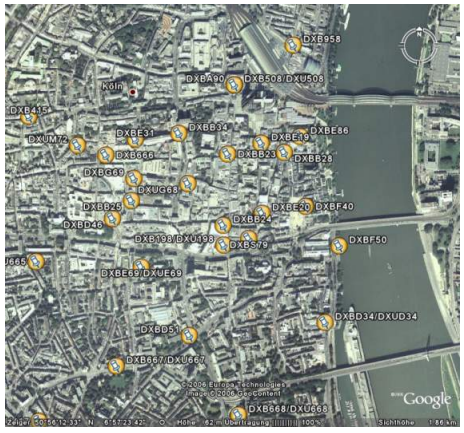
24 VDSL ports
48 ADSL ports
per line card

Zum Beispiel Mobilfunk

DHBW Stuttgart

BTS

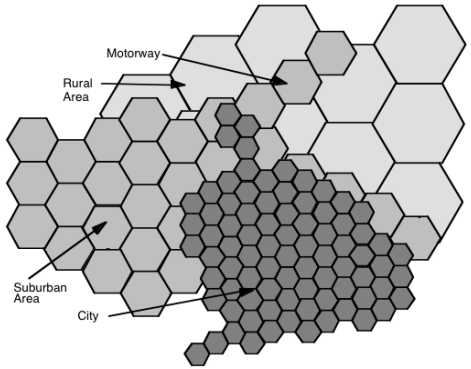
Node B
(BTS)



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

Zellulare Netzstruktur

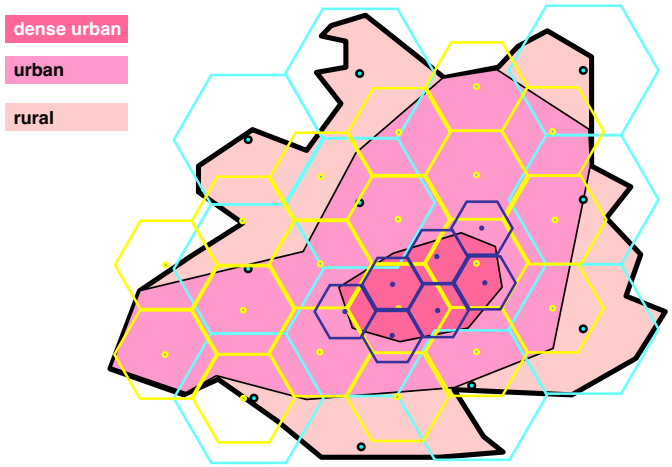
DHBW Stuttgart



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

Beispiel: Verkehrsdichte im Metronetz

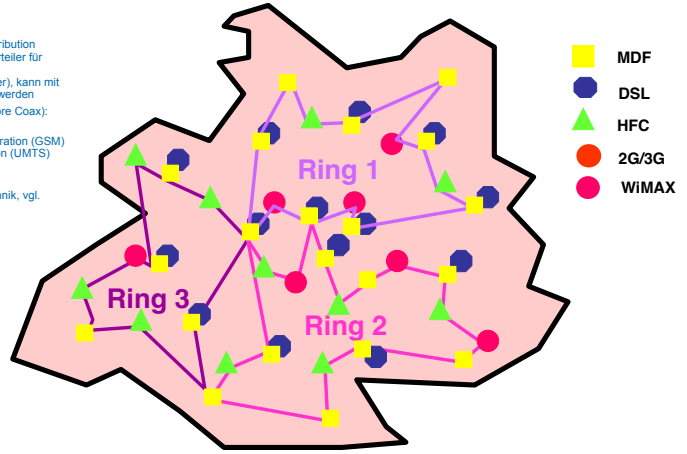
DHBW Stuttgart



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

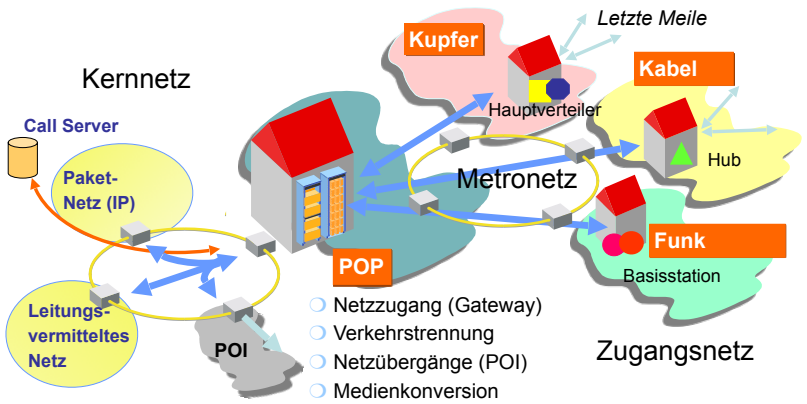
DHBW Stuttgart

Technik der Netze - Einführung

- Netze
- Leitungsvermittlung, 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)
  - CaTV-Netze (Kabelmodem, Kabeltelefon)
  - Mobilfunk der 2., 3. und 4. Generation (GSM/GPRS, UMTS, LTE): weiteres Wachstum durch Telematik, Maschinen, Internet der Dinge.
  - Hot-Spots (WiFi) für massives Datenaufkommen bzw. hohe lokale Verkehrsdichten

Strecken und Dehnen

DHBW Stuttgart

Gymnastik

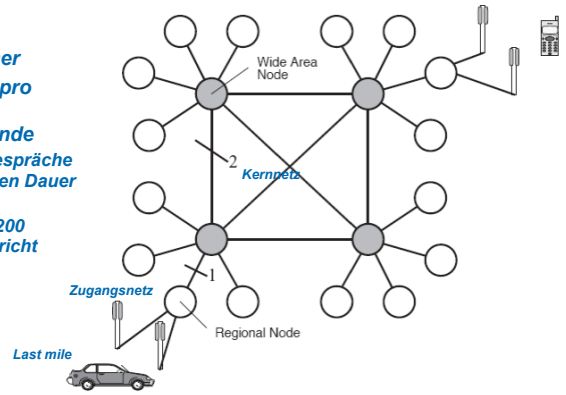
Netzdesign

Weitverkehrsnetz – Röhren für Bits

DHBW Stuttgart

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***



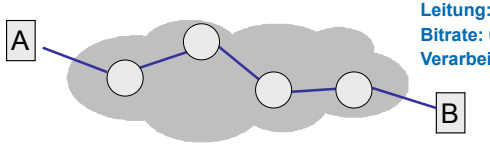
Struktur:

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

Weitverkehrsnetz - Fragen

DHBW Stuttgart

- 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

Strecken und Dehnen

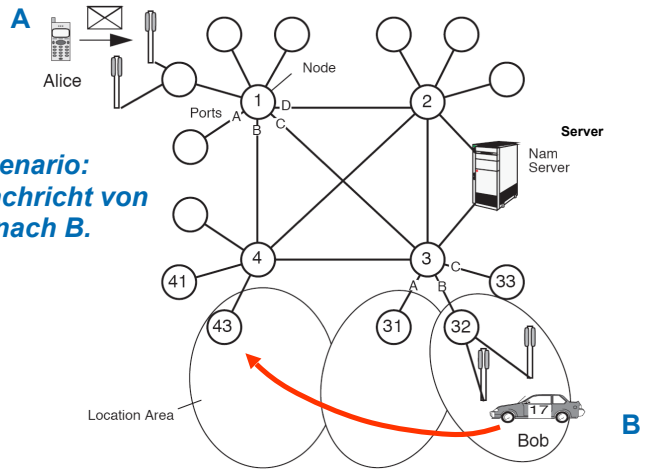
DHBW Stuttgart

Gymnastik

Mobilität

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?

DHBW Stuttgart

ENDE Teil 3

Weitverkehrsnetze

DHBW Stuttgart

Kommunikationssysteme
Teil 4 - Internet

Stephan Rupp
Masterstudium Informations- und Kommunikationstechnik

www.dhbw-stuttgart.de

Inhalt

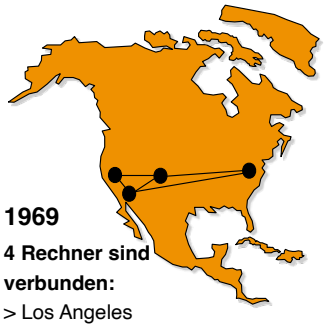
DHBW Stuttgart

Internet - Das Netz der Netze

- Historie
- Protokolle
- Adressierung im Internet
- IP-Netze
- Standardisierung

Internet Historie - ARPANET

DHBW Stuttgart



1969
4 Rechner sind verbunden:
> Los Angeles
> Stanford
> Santa Barbara
> Salt Lake City

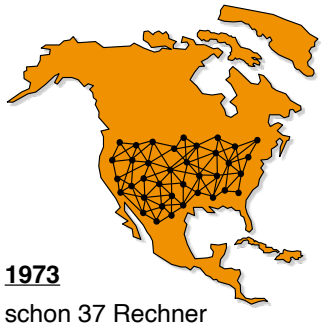
Mitte der 1960er Jahre:
ein militärisches Experiment mit dem Ziel einer zuverlässigen Kommunikation.
Aus dieser Forderung resultiert der verbindungslose Betrieb.
Gefördert durch die DARPA (Defence Advanced Research Projects Agency
das:
ARPANET

(Advanced Research Project Agency Network)

Quelle: Harald Orlamünder

Internet - Forschungsnetz & TCP/IP

DHBW Stuttgart



1973
schon 37 Rechner sind verbunden

1972/73
Das Netz wird für Universitäten und Forschungszentren geöffnet.

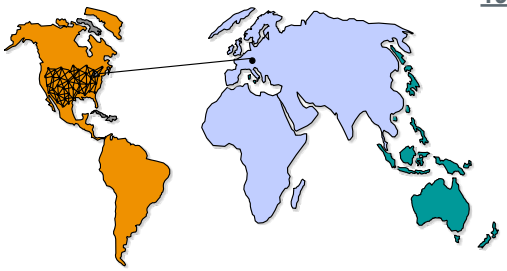
1982
Eine neue Protokoll-Generation wird eingeführt:
TCP/IP

(Transmission Control Protocol/ Internet Protocol)

Quelle: Harald Orlamünder

Internet - NSFNET

DHBW Stuttgart



1986

Das ARPANET wird an die NSF (National Science Foundation) übergeben und wird zum

NSFNET

1989 **Die Universität in Dortmund wird als erster Rechner in Deutschland an das Netz angeschlossen.**

1989

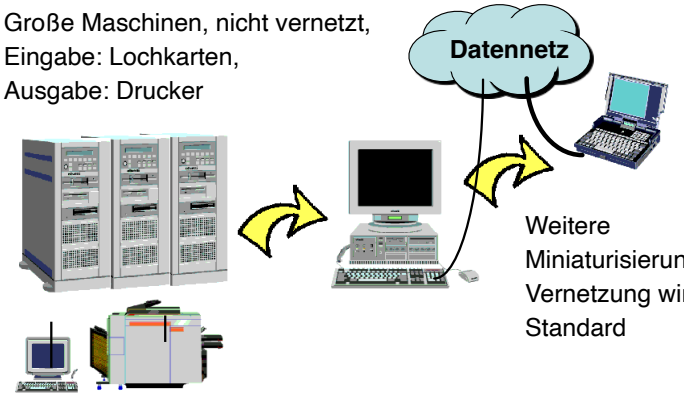
Das ARPANET stellt seinen Betrieb ein

Quelle: Harald Orlamünder

Die Geschichte der Rechner-Technik

DHBW Stuttgart

Große Maschinen, nicht vernetzt,
Eingabe: Lochkarten,
Ausgabe: Drucker



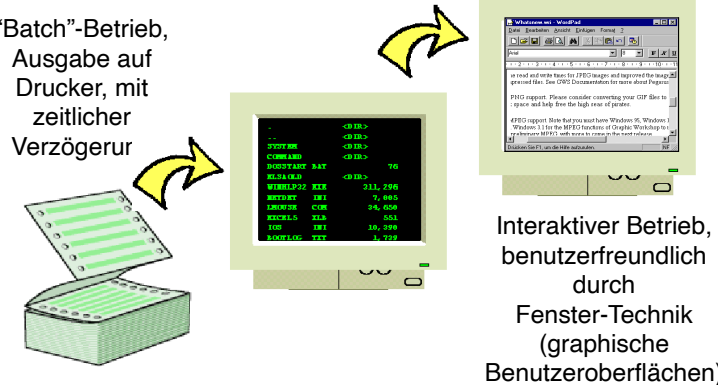
Weitere Miniaturisierung, Vernetzung wird Standard

Quelle: Harald Orlamünder

Die Geschichte der Rechner-Bedienung

DHBW Stuttgart

"Batch"-Betrieb, Ausgabe auf Drucker, mit zeitlicher Verzögerur



Interaktiver Betrieb, benutzerfreundlich durch Fenster-Technik (graphische Benutzeroberflächen)

Quelle: Harald Orlamünder

Die Rolle der Beteiligten

DHBW Stuttgart

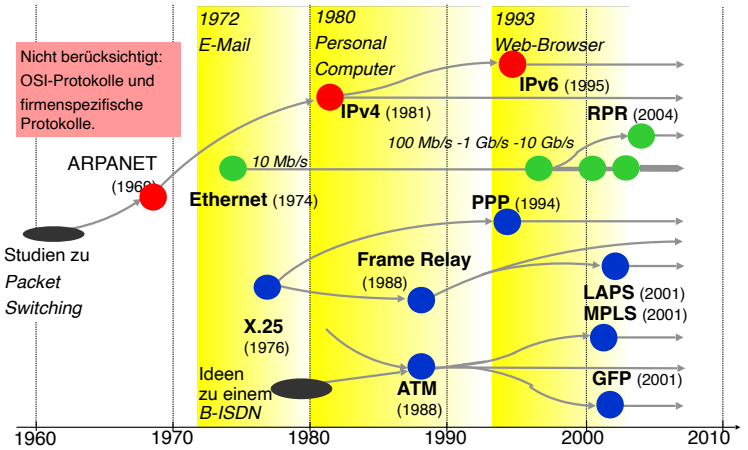
Die ehemaligen Studenten der Forschungsprojekte
gehen in die Industrie und zu Netzbetreibern und werden Entscheidungsträger .....

.... sie bringen ihr Know-how bezüglich Datennetzen und dem Internet ein und beeinflussen die weitere Entwicklung der Telekommunikation.

Quelle: Harald Orlamünder

Die Entwicklung der Paket-Protokolle

DHBW Stuttgart



Quelle: Harald Orlamünder

Inhalt

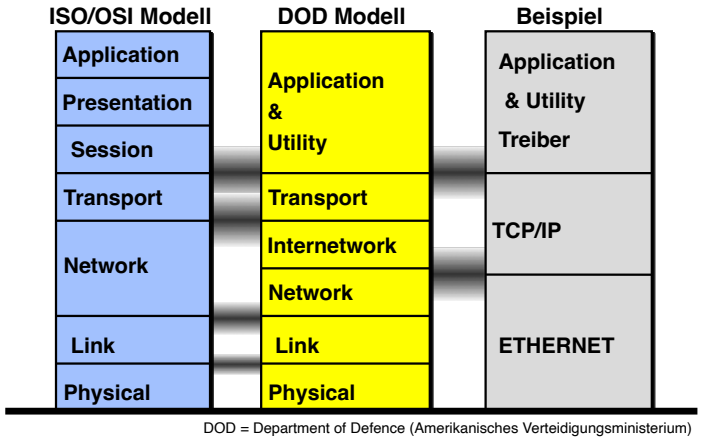
DHBW Stuttgart

Internet - Das Netz der Netze

- Historie
- Protokolle: IPv4, IPv6, TCP, UDP, Schicht 2 Protokolle
- Adressierung im Internet
- IP-Netze
- Standardisierung

Vergleich der Protocol-Stacks

DHBW Stuttgart

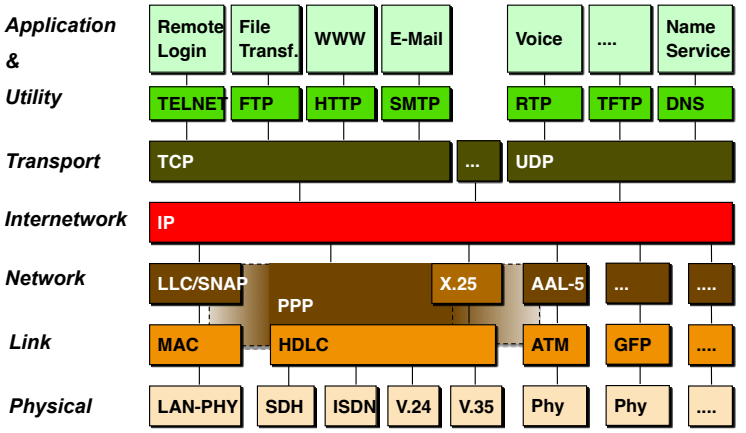


DOD = Department of Defence (Amerikanisches Verteidigungsministerium)

Quelle: Harald Orlamünder

TCP-IP Protocol Stack

DHBW Stuttgart



Quelle: Harald Orlamünder

Internet Protocol

DHBW Stuttgart

Das wichtigste Protokoll ist das

Internet Protocol (IP)

RFC 791 ***Internet Protocol, DARPA Internet Program Protocol Specification***
J.Postel, September 1981

als gemeinsame Schicht mit den Zusatzprotokollen:

Internet Control Message Protocol (ICMP),

RFC 792 ***Internet Control Message Protocol*** *(J.Postel, September 1981)*

Address Resolution Protocol (ARP),

RFC 826 ***Ethernet Address Resolution Protocol: Or converting network protocol addresses to 48.bit Ethernet address for transmission on Ethernet hardware*** *(D.C.Plummer, November 1982)*

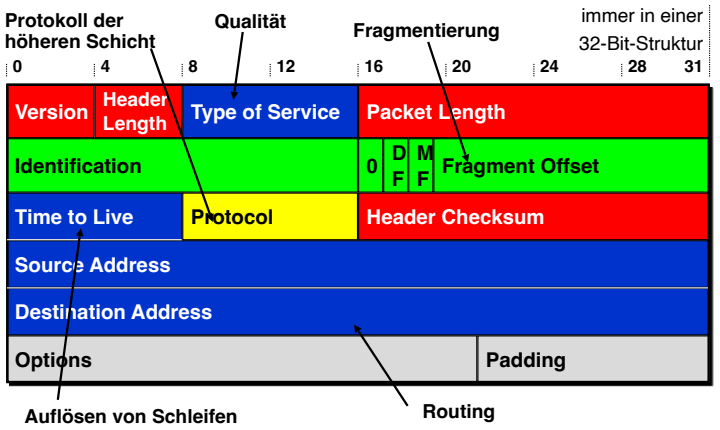
Reverse Address Resolution Protocol (RARP)

RFC 903 ***Reverse Address Resolution Protocol***
(*R. Finlayson, T. Mann, J.C. Mogul, M. Theimer, Juni 1984)*

Quelle: Harald Orlamünder

Protokollkopf des Internet Protocols

DHBW Stuttgart



Quelle: Harald Orlamünder

IPv6 - Die Ideen für ein neues Protokoll

DHBW Stuttgart

- Das gegenwärtige Internet Protokoll - Version 4 - wurde 1981 entwickelt. Seit dieser Zeit läuft es gut im Internet, war aber nie für ein so großes Netz wie es das heutige Internet darstellt, gedacht.
- Es gibt einige Defizite im Protokoll die z.B. Sicherheit, Mobilität und Qualität betreffen. Sie werden heute über Zusatzprotokolle abgewickelt (Mobile-IP, IPsec,...).
- 1991 wurde mit den Arbeiten zu einer neuen Version - Version 6 - begonnen, die alle neuen Ideen beinhalten und die Version 4 ersetzen sollte.

(IP Version 5 war für das „Stream Protocol" (ST) reserviert, das keine Bedeutung erlangte.)

Quelle: Harald Orlamünder

IPv6 - Zeitlicher Ablauf

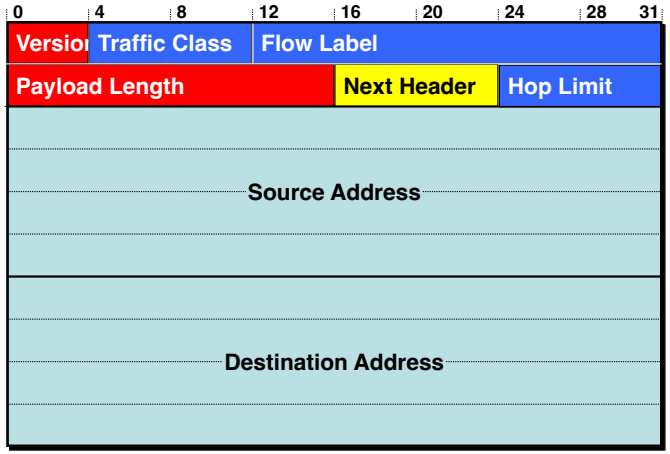
DHBW Stuttgart

- **1991:** Das IAB (Internet Activities Board, heute: Internet Architecture Board) beginnt mit Studien zum Wachstum des Internet.
- **1994:** Eine Arbeitsgruppe in der IETF veröffentlicht den RFC 1752: The Recommendation for the IP Next Generation Protocol
- **1996:** In 5 RFCs werden die Details von IPv6 nieder gelegt. (RFC 1883, 1884, 1885, 1886, 1933)
- **1998:** Ein neuer Satz von RFCs wurde veröffentlicht, 4 der Ursprungs-RFCs wurden ersetzt und die Struktur des Paketkopfes sowie die Adressierung geändert. (Am wichtigsten ist RFC 2460: IPv6 Specification

Quelle: Harald Orlamünder

IPv6 Grundlagen - Paketkopf - Struktur

DHBW Stuttgart

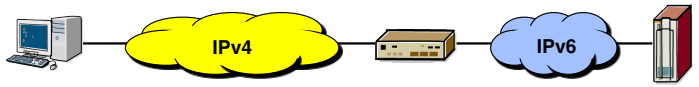


Quelle: Harald Orlamünder

IPv6 – Migration - Interworking-Fälle

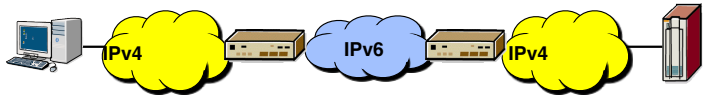
DHBW Stuttgart

1. Kommunikation zwischen Hosts in verschiedenen Protokoll-Welten.



2. Kommunikation zwischen IPv6-Hosts über ein IPv4-Zwischennetz

3. Kommunikation zwischen IPv4-Hosts über ein IPv6-Zwischennetz



Quelle: Harald Orlamünder

IPv6 - Zusammenfassung

DHBW Stuttgart

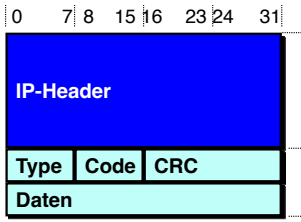
- IPv6 ist nicht die beste Lösung für ein neues Protokoll.
- IPv6 alleine reicht nicht aus, es werden zusätzliche Protokolle in „Version 6“ benötigt.
- Es gibt Übergangszeit der „Migrations-Szenarien“ mit all ihren Nachteilen.
- Trotzdem: wegen der erwarteten Adressknappheit wird IPv6 eingeführt werden, Start 2012.
- Treiber für die Einführung sind:
  - Mobilfunk (3G) wegen der „Always-On-Eigenschaft“.
  - Der Asiatisch-Pazifische-Raum wegen der wenigen IPv4-Adressen, die dort registriert sind
  - Europa, politisch motiviert für eine neue Generation Internet.

Quelle: Harald Orlamünder

Internet Control Message Protocol

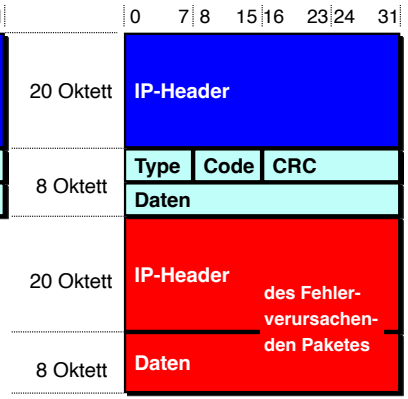
DHBW Stuttgart

ICMP-Anfrage und -Antwort



Protokoll zur Überwachung und Fehlerbehandlung des IP selbst.

ICMP-Fehlermeldung



Quelle: Harald Orlamünder

Internet Control Message Protocol

DHBW Stuttgart

Typ	Code		Bedeutung
00	00	Echo request	Anfragen und
08	00	Echo reply	Antworten
09	00	Router advertisement	
0A	00	Router solicitation	
0D	00	Timestamp request	
0E	00	Timestamp reply	
F2	00	Address Mask request	
F3	00	Address Mask reply	
03	00	Network unreachable	Fehlermeldungen :
	.....		*Ziel unerreichbar*
03	0F	Precedence cutoff in effect	
04	00	Source Quench	
05	00	Redirect for Network	Fehlermeldungen :
05	01	Redirect for Host	*Umleitungen*
05	02	Redirect for Type of Service and Network	
05	03	Redirect for Type of Service and Host	
0B	00	Time to live equals zero during transit	Fehlermeldungen :
0B	01	Time to live equals zero during reassembly	*Zeitgeber*
0C	00	IP Header bad	Fehlermeldungen :
0C	01	required option missing	*Parameter*

z.B. für „PING“ benutzt

Quelle: Harald Orlamünder

Transportprotokolle - TCP und UDP

DHBW Stuttgart

Die beiden wichtigsten Protokolle der Transportschicht sind das verbindungsorientierte

Transmission Control Protocol (TCP)

RFC 793 Transmission Control Protocol, DARPA Internet Program Protocol Specification (J.Postel, August 1980)

RFC 2581 TCP Congestion Control (M.Allman, V.Paxson,W.Stevens; April 1999)

und das verbindungslose

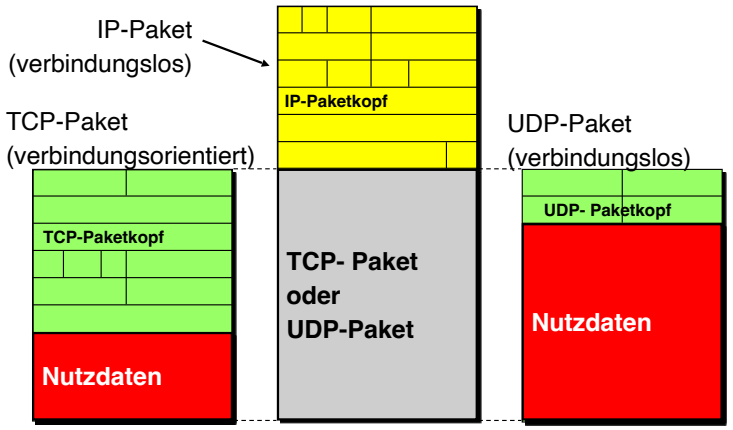
User Datagram Protocol (UDP)

RFC 768 User Datagram Protocol (J.Postel, September 1981)

Quelle: Harald Orlamünder

IP transportiert TCP oder UDP

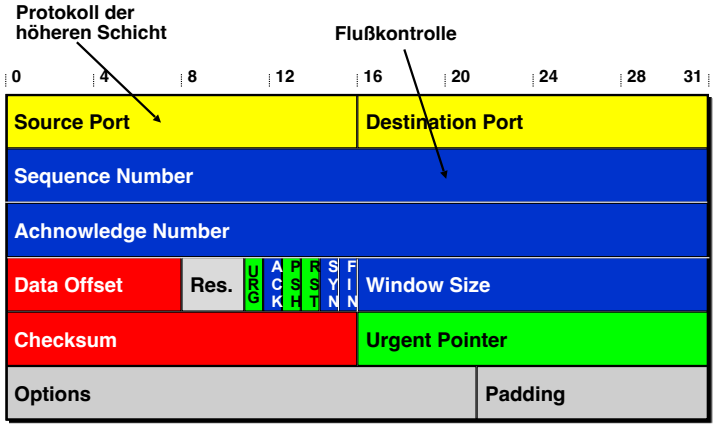
DHBW Stuttgart



Quelle: Harald Orlamünder

TCP Protokollkopf

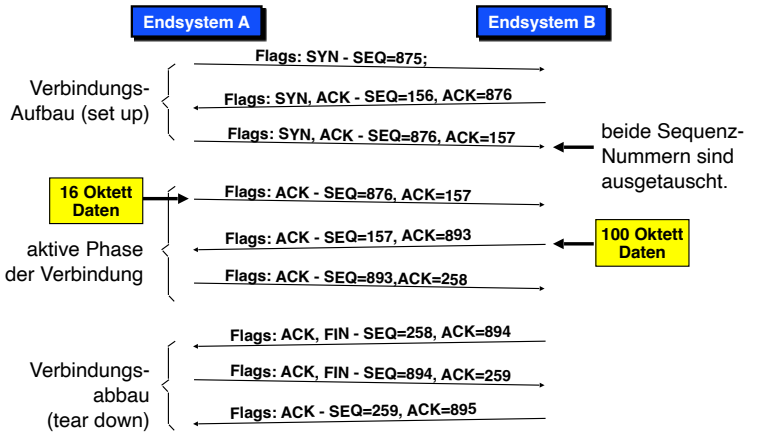
DHBW Stuttgart



Quelle: Harald Orlamünder

Verbindungen mit TCP

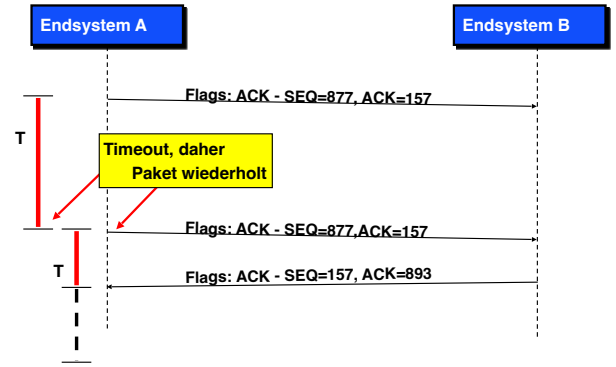
DHBW Stuttgart



Quelle: Harald Orlamünder

TCP - Timeout

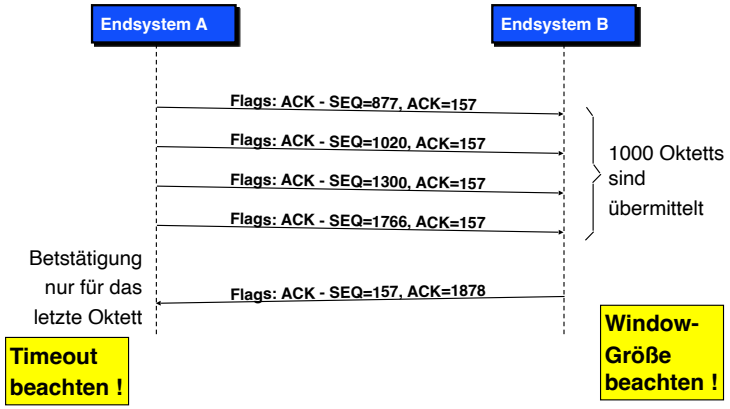
DHBW Stuttgart



Quelle: Harald Orlamünder

TCP - Bestätigung für mehrere Pakete

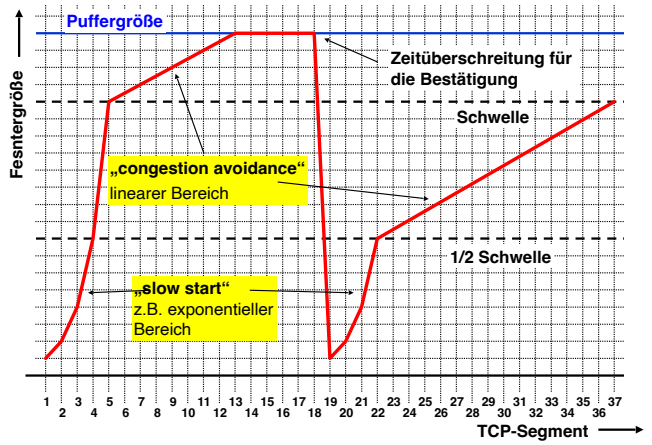
DHBW Stuttgart



Quelle: Harald Orlamünder

TCP Ablauf der Flußkontrolle

DHBW Stuttgart



Quelle: Harald Orlamünder

TCP - Kritische Punkte der Flußkontrolle

DHBW Stuttgart

Aufgrund der Flusskontrolle nicht geeignet für Echtzeit-Anwendungen (Beschränkung der Bandbreite im Fall von Engpässen im Netz).

- Echtzeit-Anwendungen nutzen UDP.

Die Bandbreite wird nicht „fair“ zwischen den Benutzern aufgeteilt.

- Verbindungen mit kurzen Paketverzögerungszeiten erhalten mehr Bandbreite.

„Pump-Effekt“ bei der Bandbreite aufgrund des Flusskontroll-mechanismus.

- Das System nähert sich langsam der bereitgestellten Kapazität im Netz an und startet im Fehlerfall (Überschreiten der spezifizierten Quittungszeit) von vorne (Startlevel).

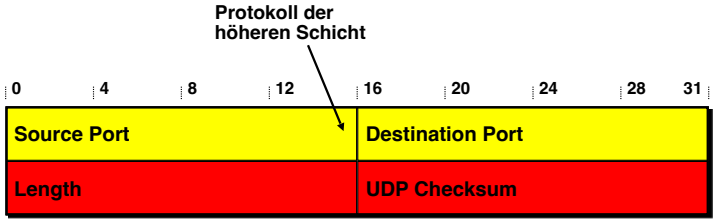
Quelle: Harald Orlamünder

UDP - Protokollkopf

DHBW Stuttgart

Nur eine kleine Erweiterung des IP Protokolls:

- Schutz des UDP-Protokollkopfes durch eine Prüfsumme (CRC).
- Auswahl des richtigen Dienstes (=höhere Schichten)

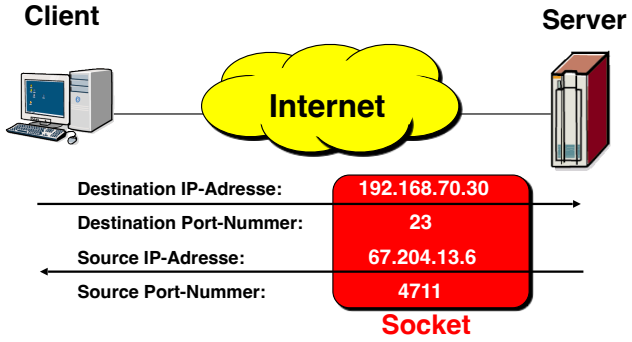


Quelle: Harald Orlamünder

Socket Definition

DHBW Stuttgart

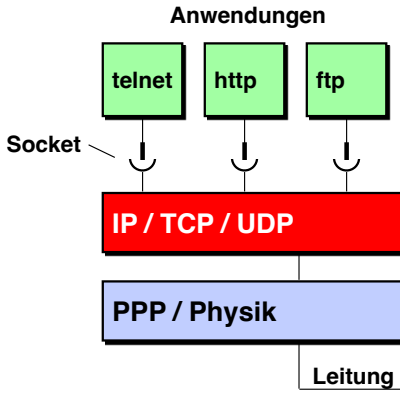
Das Tupel aus **IP-Adresse** und **Port-Nummer** wird „Socket“ genannt (Steckverbinder für Anwendungen).



Quelle: Harald Orlamünder

Socket Anwendung

DHBW Stuttgart



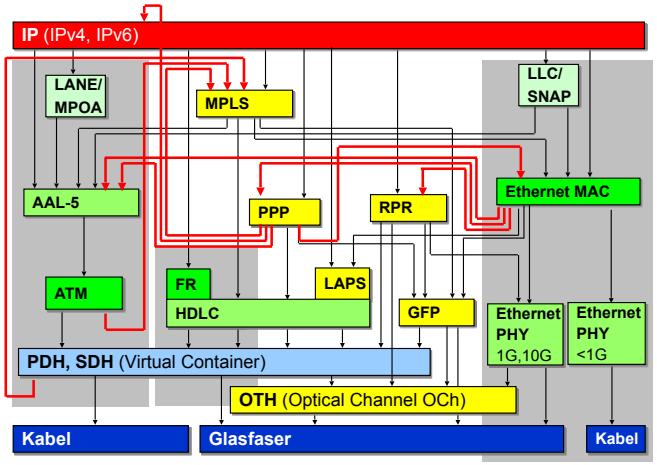
Diese Darstellung veranschaulicht den Begriff eines „Socket“ - deutsche Übersetzung: Fassung, Muffe, Hülse,...

Die Anwendung wird „eingesteckt“

Quelle: Harald Orlamünder

Die heutige Protokollvielfalt

DHBW Stuttgart



Quelle: Harald Orlamünder

Schicht-2-Protokolle

DHBW Stuttgart

IP-Pakete können über viele Übertragungsmedien übertragen werden.

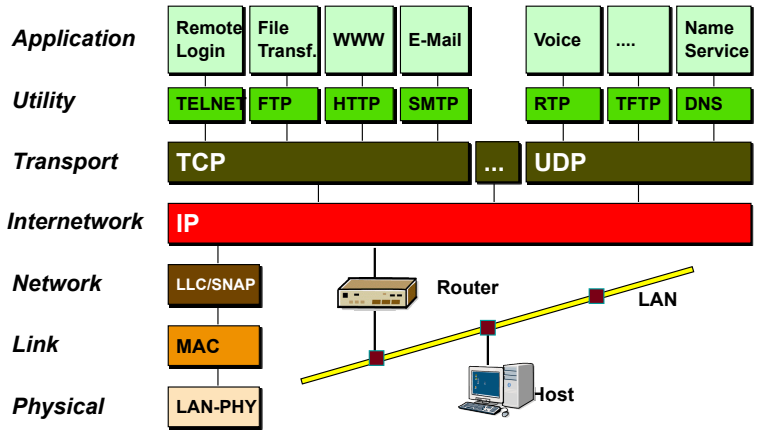
Dazu werden jeweils verschiedenen Schicht-1- und Schicht-2-Protokolle eingesetzt:

- **Local Area Networks** - mit Medium Access Control (Ethernet, Token Ring, ...)
- **Point-to-Point-Protokoll** über verschiedene Medien (RFC 1661 The Point-to-Point Protocol, W.Simpson, Juli 1994)
- **Nutzung von ATM, MPLS** (Classical IP over ATM, MPLS, MPOA, ...)

Quelle: Harald Orlamünder

Local Area Network als Transport von IP

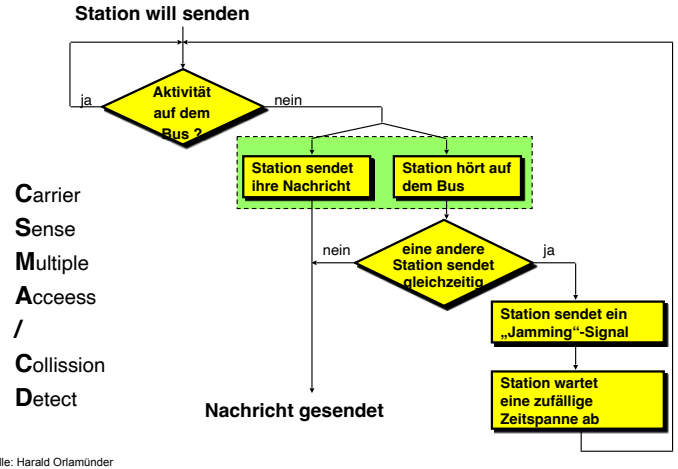
DHBW Stuttgart



Quelle: Harald Orlamünder

Local Area Network CSMA/CD Ablauf

DHBW Stuttgart

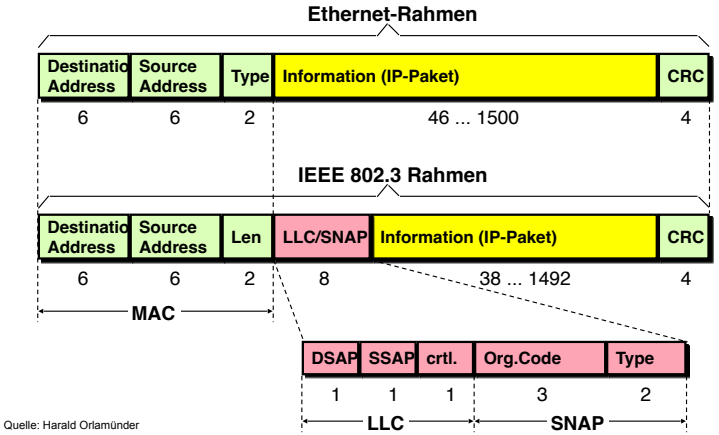


Quelle: Harald Orlamünder

LAN (Local Area Network)

DHBW Stuttgart

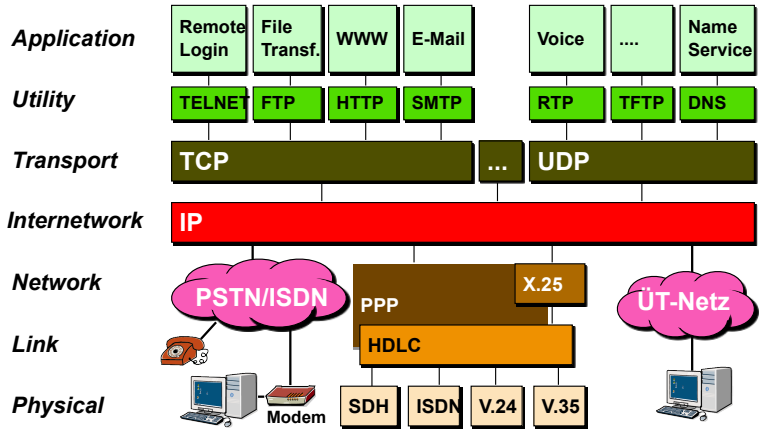
Ethernet- und IEEE 802.3-Rahmenstruktur



Quelle: Harald Orlamünder

IP über Telekommunikationsnetze

DHBW Stuttgart



Quelle: Harald Orlamünder

Point-to-Point Protocol (PPP) - Prinzip

DHBW Stuttgart

Das PPP besteht aus drei Komponenten:

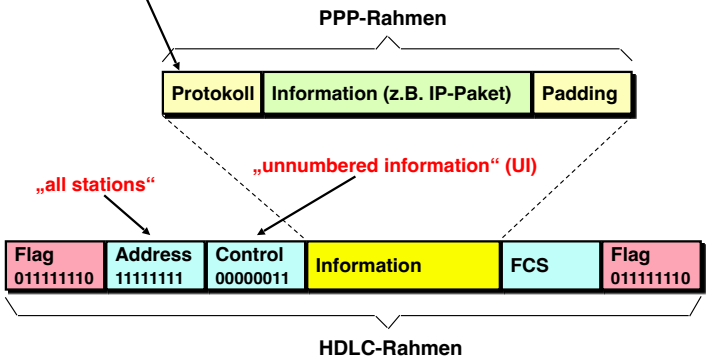
- Eine Methode um Paket-Daten entsprechend verpackt zu übertragen - **PPP Encapsulation**.
  Dabei wird von einer bidirektionalen Vollduplex-Übertragung ausgegangen.
- Ein Protokoll um die Übertragungsstrecke auf- und abzubauen, zu konfigurieren und zu testen,
  das **Link Control Protocol (LCP).**
- Ein entsprechendes Steuerprotokoll, um verschiedene Schicht-3-Protokolle auf- und abzubauen und zu konfigurieren,
  das **Network Control Protocol (NCP).**

Quelle: Harald Orlamünder

PPP - Rahmenstruktur

DHBW Stuttgart

Kennzeichnet das entsprechende, transportierte Protokoll
(Network Layer Protocol, Link Control Protocol, Network Control Protocol, ...)



Quelle: Harald Orlamünder

Inhalt

DHBW Stuttgart

Internet - Das Netz der Netze

- Historie
- Protokolle
- Adressierung im Internet: IP-Adressen, Domains, URLs
- IP-Netze
- Standardisierung

Namen und Adressen im Internet

DHBW Stuttgart

Die Internet-Architektur kann bezüglich Namen und Adressen als dreistufige Struktur angesehen werden:

- die **IP-Adressebene** erlaubt es, Geräte im Internet (Hosts und Router) anzusprechen und einen Weg zwischen solchen Geräten ausfindig zu machen.
  z.B.: `192.168.70.30`
- die **DNS-Namensebene** erlaubt es, ein System im Internet anzusprechen, das eine Anwendung bietet (Host-System).
  z.B.: `www.dhbw-stuttgart.de`
- die **Ressourcen-Ebene** erlaubt es, verschiedenste Internet Ressourcen anzusprechen (Uniform Resource Locator (URL)/ Uniform Resource Name (URN)/Uniform Resource Indicator (URI).
  z.B.: `http://dhbw-stuttgart/news/983010.htm`

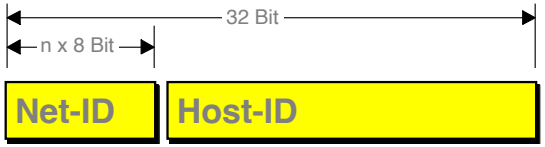
Quelle: Harald Orlamünder

IP-Adressen für IPv4 - Allgemein

DHBW Stuttgart

Die IPv4 Adresse:

- ist 32 Bit lang (> 4x10E9 Adressen);
- ist strukturiert in einen "**Network Identifier**" (Net-ID) und einen "**Host Identifier**" (Host-ID);

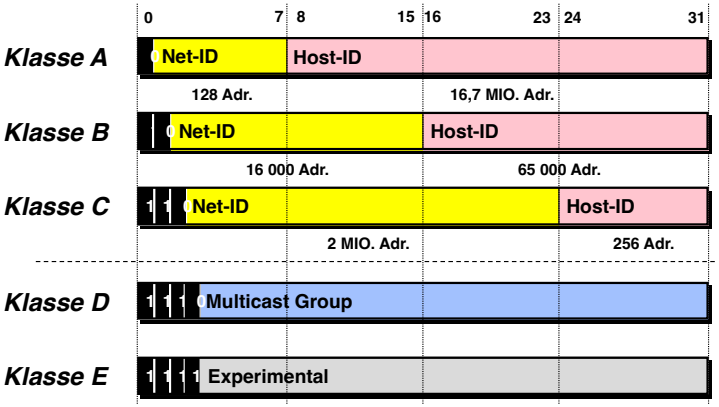


- wird im „dotted-decimal" Format geschrieben, z.B.:
  `192.168.70.30`
- wird von verschiedenen Organisationen verwaltet

Quelle: Harald Orlamünder

Adress-Klassen für IPv4

DHBW Stuttgart



Strukturierung verursacht Adress-Knappheit!

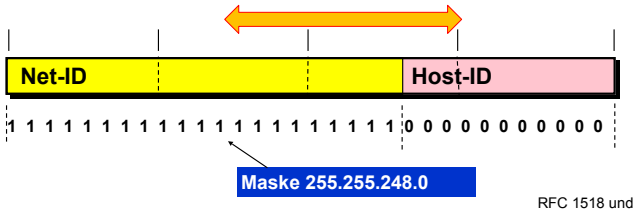
RFC 1020

Quelle: Harald Orlamünder

DHBW Stuttgart

Classless Inter Domain Routing (CIDR)

- Jedes Netz erhält eine Serie von aufeinanderfolgenden Class C Adressen und eine „**Maske**“.
- Die Maske zeigt an, welcher Teil der Adresse die „Net-ID“ bildet.
- Beispiel: ein Netz, das 2048 Adressen benötigt, erhält 8 Class C Adressen und eine Maske „**255.255.248.0**“.



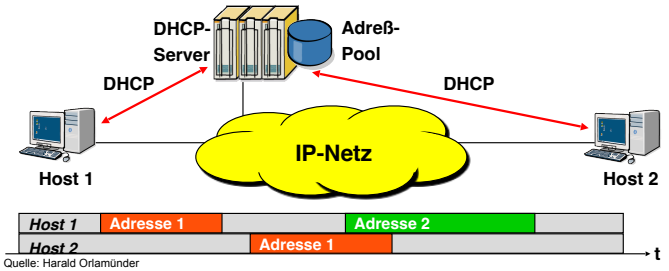
RFC 1518 und RFC 1519

Quelle: Harald Orlamünder

DHBW Stuttgart

Dynamic Host Configuration Protocol (DHCP)

- Der einzelne Host hat keine feste IP-Adresse, sondern beim Einloggen erhält er dynamisch eine aus einem Pool.
- Erweiterung des alten BOOT-Protokolls (BOOTP).



RFC 2131

Quelle: Harald Orlamünder

DHBW Stuttgart

Network Address Translator (NAT) für Intranets

- Der NAT ist eine Einheit, die interne (lokale) IP-Adressen (z.B. von innerhalb eines Intranets) in externe (globale) IP- Adressen übersetzt.
- Lokale IP-Adressen sind nicht eindeutig und können in anderen Intranets wiederverwendet werden.
- Der Mechanismus ist natürlich nur dann brauchbar, wenn mehr lokale als globale Adressen benötigt werden. (Problem wenn Extern-Verkehr überwiegt !)
- Einige Adressblöcke sind für Intranets reserviert:

10.0.0.0 – 10.255.255.255	1x Class A
172.16.0.0 – 172.31.255.255	16x Class B
192.168.0.0 – 192.168.255.255	256x Class C

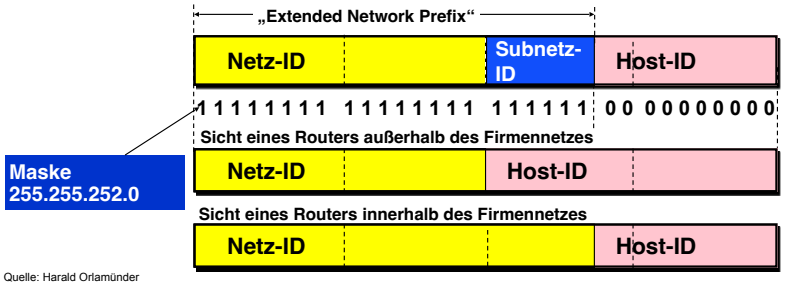
RFC 1631 und RFC 1918

Quelle: Harald Orlamünder

DHBW Stuttgart

Große Intranets wollen ihren internen Bereich ebenfalls strukturieren. Die IP-Adresse wird dazu in drei Teile zerlegt:

- Net-ID - vom Internet benutzt,
- Subnet-ID - vom Intranet für Netzstruktur benutzt,
- Host-ID - vom Intranet für Hosts benutzt.



Quelle: Harald Orlamünder

IPv6 – Addressing - Allgemein

DHBW Stuttgart

Die IPv6-Adresse ist: **128 Bit** lang (>3x10^{38} Adressen) oder genau:
340 282 366 920 938 463 463 374 607 431 768 211 456

Der Adressraum ist so gross, dass selbst mit einer strukturierten Adresse mehr als 1500 Adressen pro m² Erdoberfläche zur Verfügung stehen.

strukturiert (nur die „Aggregable Global Unicast Address“ ist im Detail spezifiziert);

die letzten 64 Bit werden „**Identity**“ genannt
(sie bleiben auch bei Wechsel des Providers erhalten);

wird im hexadezimalen **„colon“-Format**, geschrieben,
(8 Anteile je 16 Bits) z.B.:

`108F:0:0:0:8:800:200C:417A`

Quelle: Harald Orlamünder

Domain Name System - Allgemeines

DHBW Stuttgart

Für eine bessere „Lesbarkeit“ wurde das „Domain Name System“ erfunden. Es besteht aus hierarchischen Strukturen für Nutzer und Hosts. Die „Top Level Domain“ (TLD) kennzeichnet Kategorien oder Länder

Host

`www.dhbw-stuttgart.de`

Top Level Domain

generic TLDs (gTLD)
.com = Commercial
.net = Administrative Organisations
.org = other Organisations
.int = international Organisations
.edu = Education (de facto nur USA)
.gov = Government (nur USA)
.mil = Military (nur USA)
➨ **76% aller Domains**

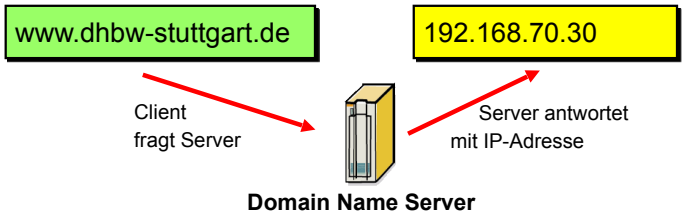
country code TLDs (ccTLD)
.de = Germany
.fr = France
.uk = United Kingdom
.at = Austria
.au = Australia
.....
Code gemäß ISO 3166
➨ **24% aller Domains**

Quelle: Harald Orlamünder

Prinzip des Domain Name Server

DHBW Stuttgart

Zum Routen der Pakete muss eine Übersetzung zwischen dem Namen nach dem Domain Name System und der 32-Bit-IP-Adresse durchgeführt werden.

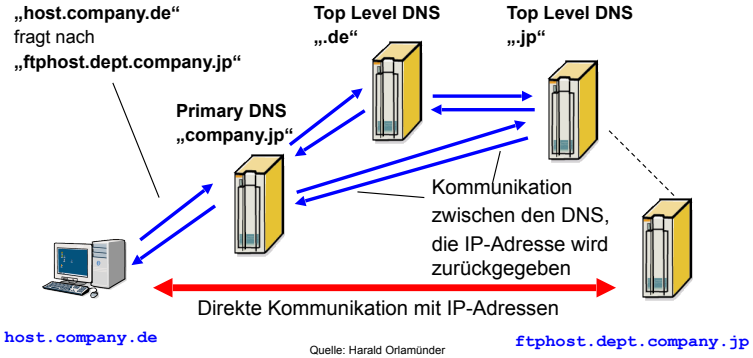


Quelle: Harald Orlamünder

DNS-Anfrage über mehrere Server

DHBW Stuttgart

Falls der „Primary Domain Name Server“ die Adresse nicht über-setzen kann, werden weitere Domain Name Server hinzugezogen:

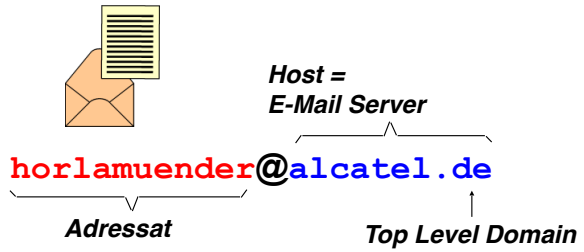


Quelle: Harald Orlamünder

E-Mail Adressen sind Namen

DHBW Stuttgart

- Eine E-Mail-Adresse (die in Wirklichkeit ein Name ist) korrespondiert mit dem Domain Name System.
- Nur der angesprochene Host (also der E-Mail-Server) kennt die einzelnen Adressaten.



Quelle: Harald Orlamünder

URI / URL / URN - Definitionen

DHBW Stuttgart

- Der **Universal Resource Identifier** (URI) ist ein Konzept: „to encapsulate a name in any registered name space, label it with the name space and producing a member of the universal set“.
- Der **Uniform Resource Locator** (URL) ist ein URI „which refers to objects accessed with existing protocols“.
- Sein Aufbau entspricht folgendem Schema :

  `<scheme>:<scheme specific part>`

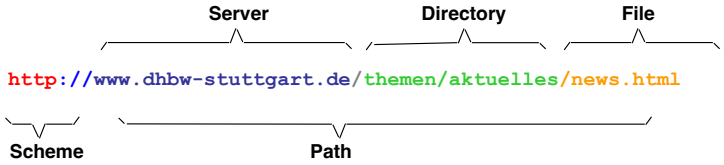
- Der **Uniform Resource Name** (URN) ist ein Versuch „to define more persistent names than any URL“

Quelle: Harald Orlamünder

Uniform Resource Locator - Format

DHBW Stuttgart

Ein URL gibt Objekten im Internet einen Namen, z.B.:



ftp	File Transfer protocol
http	Hypertext Transfer Protocol
gopher	The Gopher protocol
mailto	Electronic mail address
news	USENET news
nntp	USENET news using NNTP access
telnet	Reference to interactive sessions
wais	Wide Area Information Servers
file	Host-specific file names
prospero	Prospero Directory Service

RFC 1630 und RFC 1738

Quelle: Harald Orlamünder

Inhalt

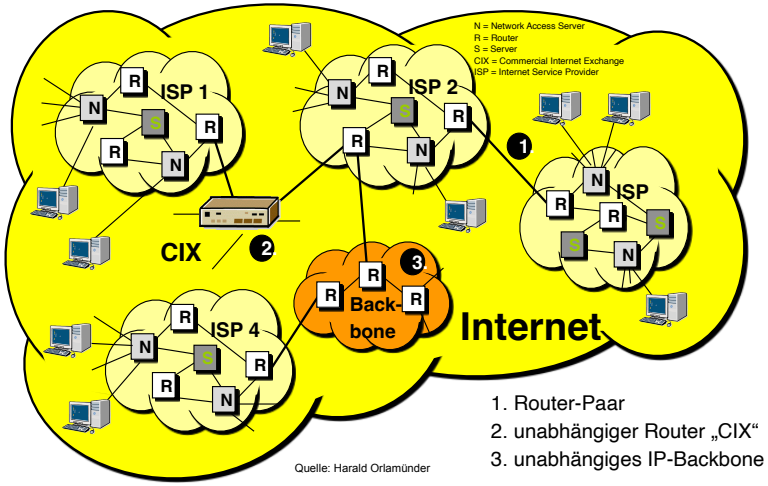
DHBW Stuttgart

Internet - Das Netz der Netze

- Historie
- Protokolle
- Adressierung im Internet: IP-Adressen, Domains, URLs
- IP-Netze: Netzstrukturen, Routing, Netzelemente
- Standardisierung

Das „Internet“ als Netz

DHBW Stuttgart



Quelle: Harald Orlamünder

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

Inhalt

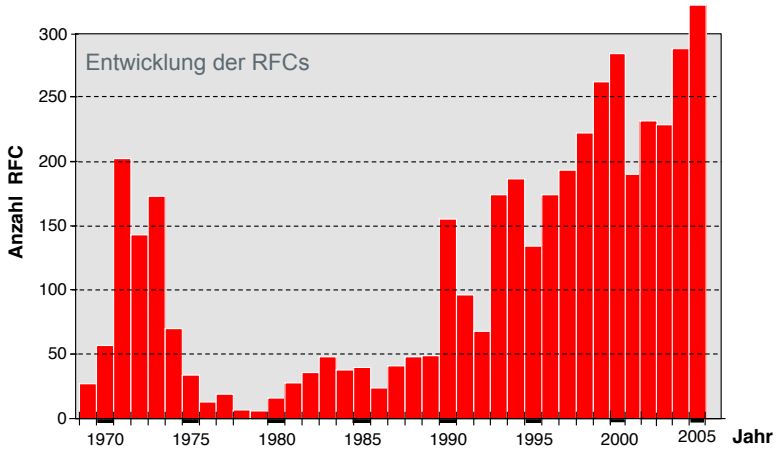
DHBW Stuttgart

Internet - Das Netz der Netze

- Historie
- Protokolle
- Adressierung im Internet
- IP-Netze
- Standardisierung

Standardisierung im Internet

DHBW Stuttgart



Kommunikationssysteme

DHBW Stuttgart

ENDE Teil 4

Internet

Literaturempfehlung: Harald Orlamünder, Paket-basierte Kommunikations-Protokolle: Hüthig Telekommunikation; Auflage: 1 (2005) ISBN-13: 978-3826650468

DHBW Stuttgart

Kommunikationssysteme
Teil 5 – Sichere Kommunikation

Stephan Rupp
Masterstudium Informations- und Kommunikationstechnik

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):

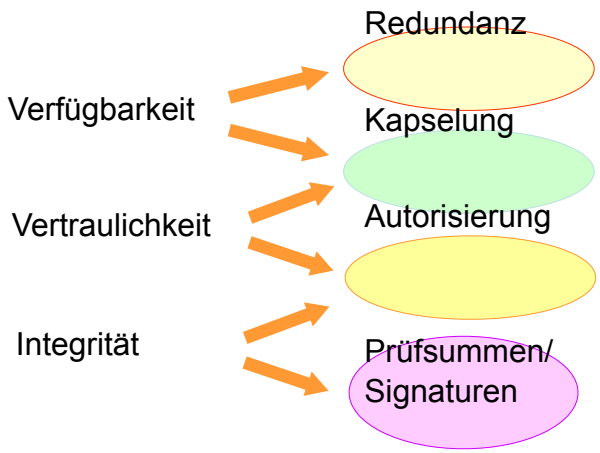
- Anwendungen bzw. Dienste sollten für autorisierte Nutzer jederzeit verfügbar sein
- Angriffe auf die Systemverfügbarkeit müssen verhindert oder abgewehrt können (Lastabwehr, Denial of Service, schädliche Software)
- Nicht jede Software ist vertrauenswürdig!
- Lösungen: Redundanz, Kapselung und Sicherheitsmodell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

CIA
(für die Fans von Eselsbrücken)

Englisch - Deutsch
Security = Sicherheit
Safety = funktionale Sicherheit

Sicherheitskonzepte

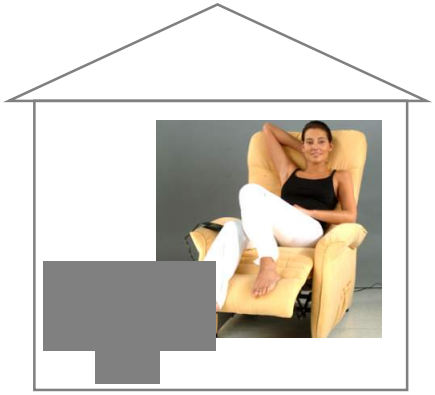
DHBW Stuttgart



Was ist Kapselung (Encapsulation)?

DHBW Stuttgart

Bob in einer unsicheren Umgebung



Alice in einer sicheren Umgebung

Inhalt

DHBW Stuttgart

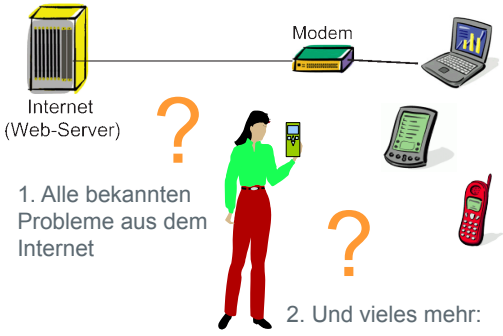
Sicherheit

- 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

Schreibtisch
(zuhause oder im Geschäft)

Mobile Dienste: unterwegs und überall dabei

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

DHBW Stuttgart

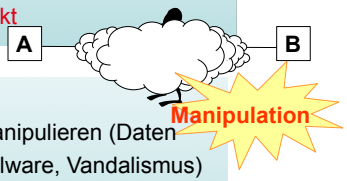
Passive Angriffe

- 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

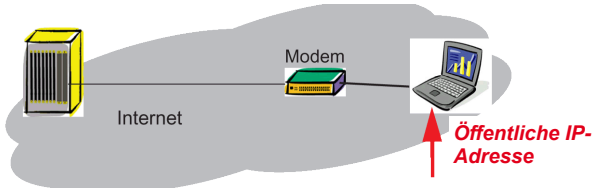
Sicherheit

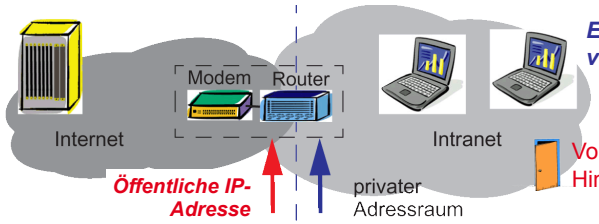
- Begriffe
- Bedrohungen
- Schutzmaßnahmen: Verhaltensregeln, die eigenen 4 Wände, der Vorraum
- Identitätsnachweise
- Geheimniskrämerei
- Verfügbarkeit, Hochverfügbare Systeme

Verhaltensregeln

DHBW Stuttgart

Öffentliches oder fremdes Netz = nicht vertrauens-würdig





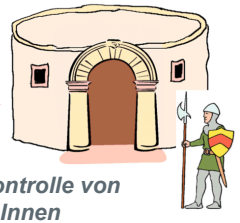
Eigenes Netz = vertrauenswürdig

Vorsicht vor Hintertüren!

Die eigenen 4 Wände

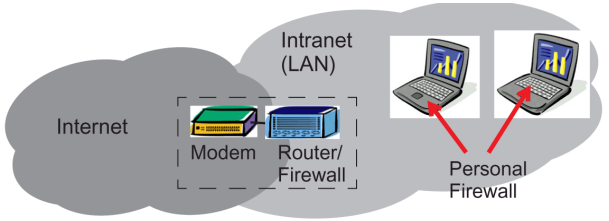
DHBW Stuttgart

Stadttor



= Zugangskontrolle von Aussen und Innen

Firewall



Mehrstufige Kapselung

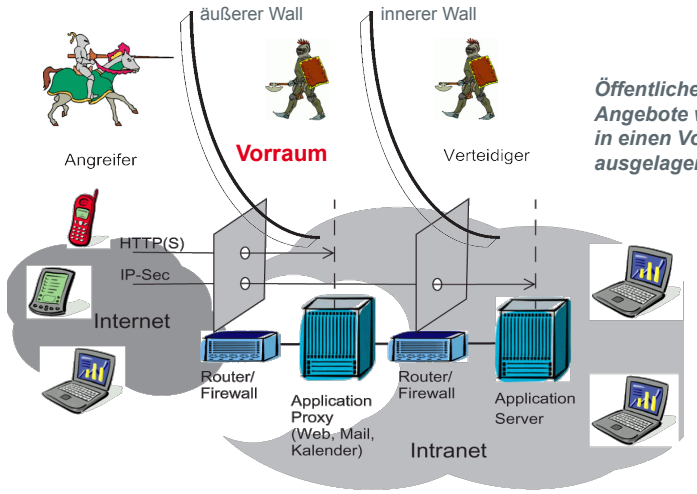
DHBW Stuttgart

Vorraum: Marktplatz und Lobby

Burg Falkenstein, Luftbild von Westen

Vorraum

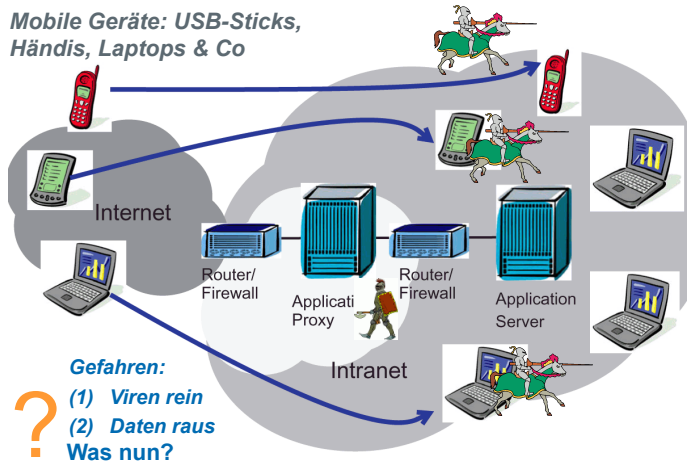
DHBW Stuttgart



Öffentliche Angebote werden in einen Vorraum ausgelagert

An der Firewall vorbei ins Intranet

DHBW Stuttgart



Inhalt

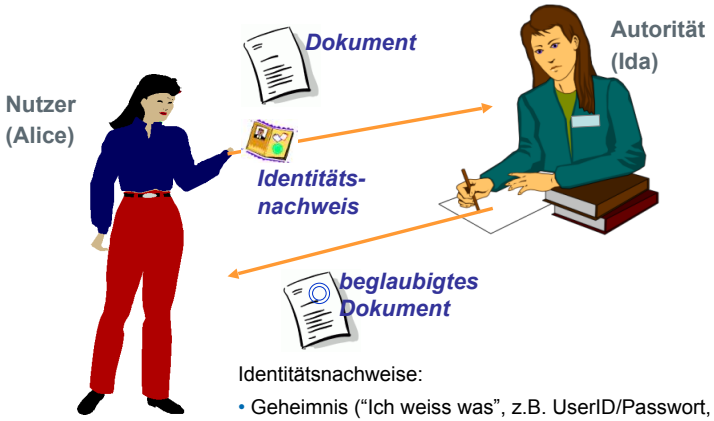
DHBW Stuttgart

Sicherheit

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

Identitätsnachweis, Ursprungsnachweis

DHBW Stuttgart

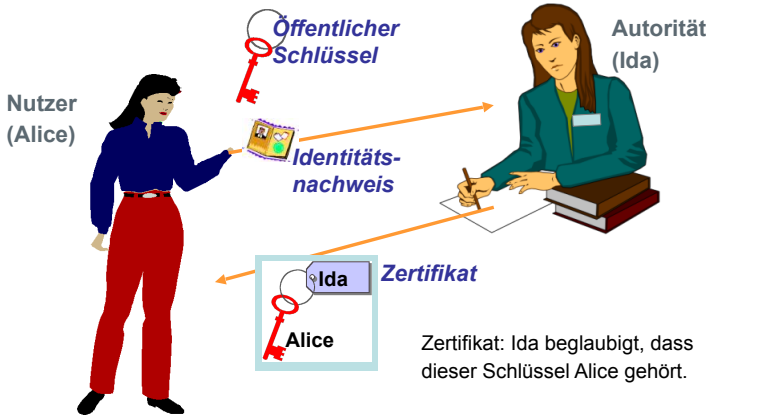


Identitätsnachweise:

- 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

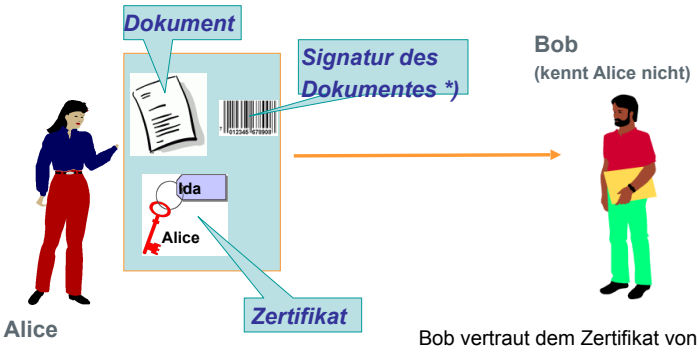
- z.B. für Secure Socket Verbindungen (https, SSL)

Identitätsnachweise für

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

Ursprungsnachweis für Dokumente

DHBW Stuttgart



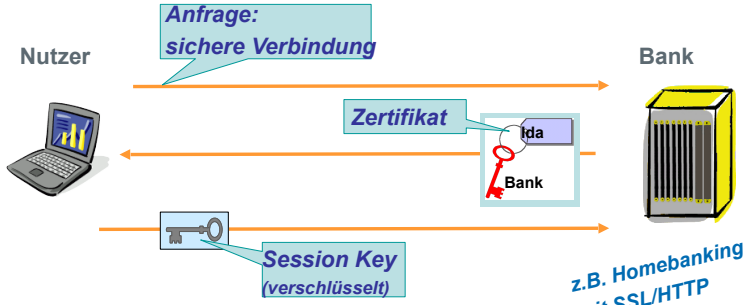
*) Signatur: mit dem privaten Schlüssel von Alice verschlüsselte Prüfsumme des Dokumentes

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

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

Aufbau verschlüsselter Verbindungen

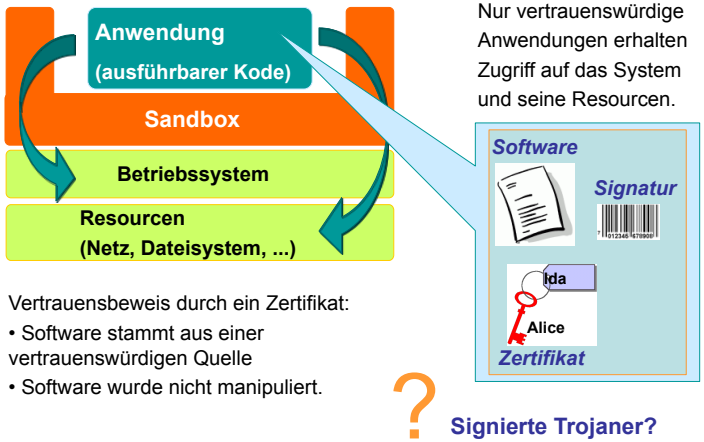
DHBW Stuttgart



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.

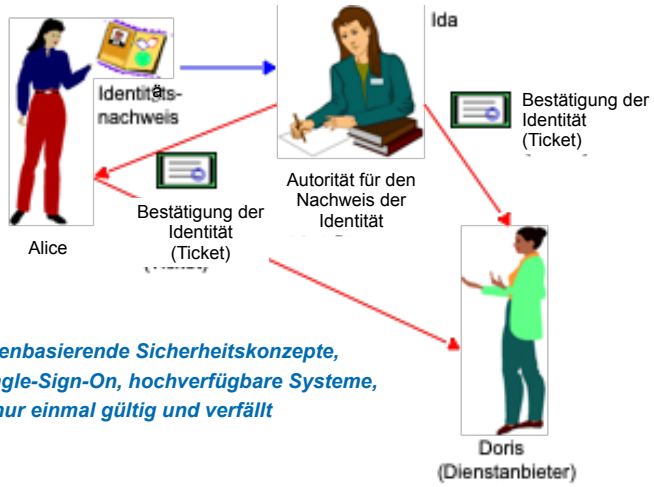
Vertrauensbeweis durch ein Zertifikat:

- 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

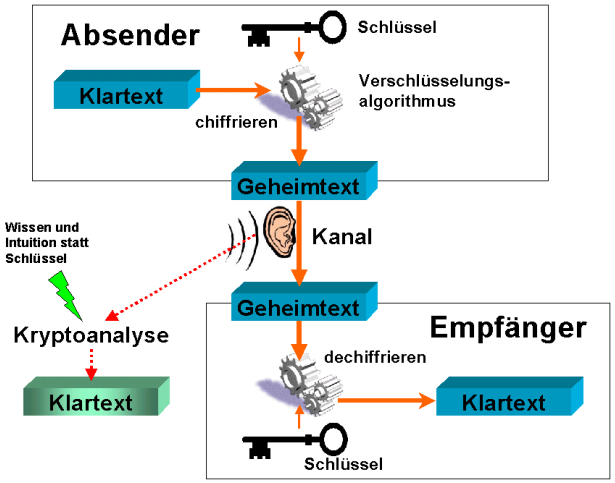
DHBW Stuttgart

Sicherheit

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

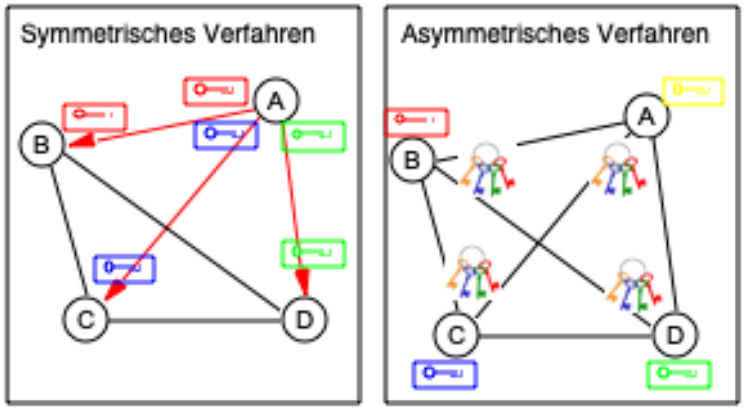
Verschlüsselung und Entschlüsselung

DHBW Stuttgart



Schlüssel und Schlüsselpaare

DHBW Stuttgart

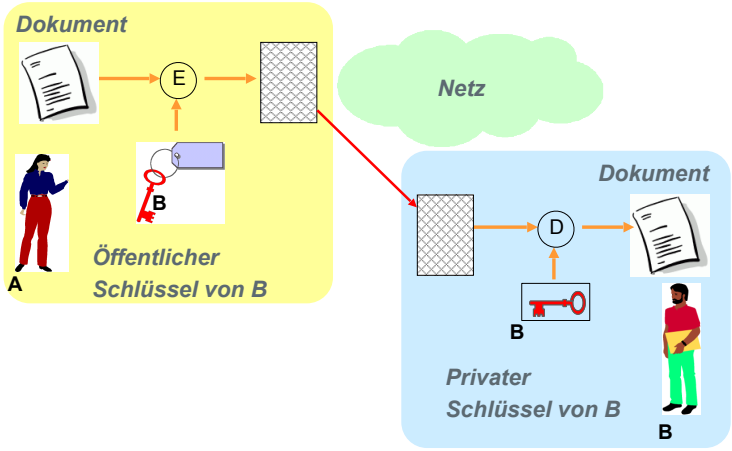


Schnelle Verfahren, aber Verteilung der Schlüssel problematisch

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.

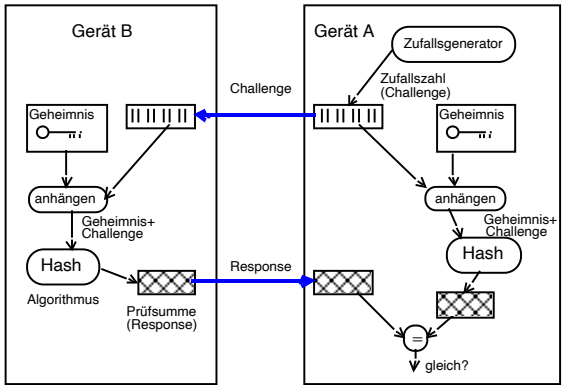
Prüfsumme (*hash*) lässt sich als Integritätsnachweis für Nachrichten und Dokumente verwenden, sowie in Kombination mit einem privaten Schlüssel als Ursprungsnachweis (z.B. Signatur bzw. message authentication codes).

DHBW Stuttgart

Gymnastik

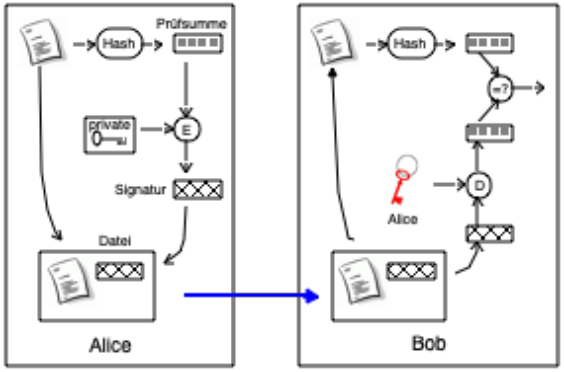
authentisieren,
verschlüsseln und signieren

DHBW Stuttgart



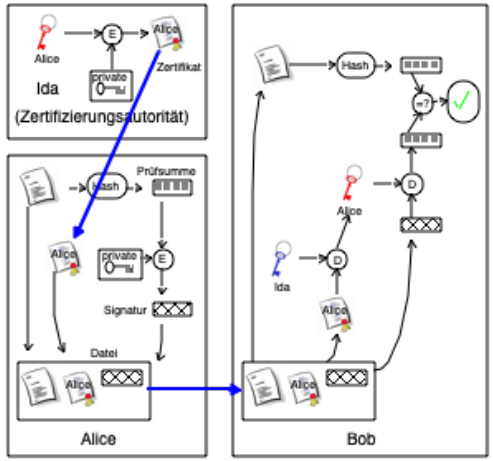
- Worin liegt der Vorteil gegenüber einfachem Authentisieren mit User-ID und Passwort? (Hinweis: was wird im Klartext übermittelt? Was wird beim nächsten Mal im Klartext übermittelt?)

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?

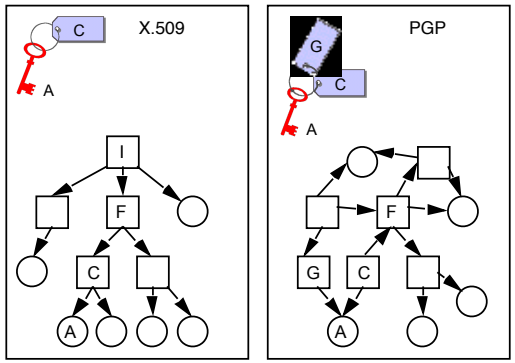
DHBW Stuttgart



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

Vertrauensbeziehungen bei Zertifikaten

DHBW Stuttgart



- 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

DHBW Stuttgart

Sicherheit

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

Was ist Redundanz?

DHBW Stuttgart

Department of
Redundancy Department

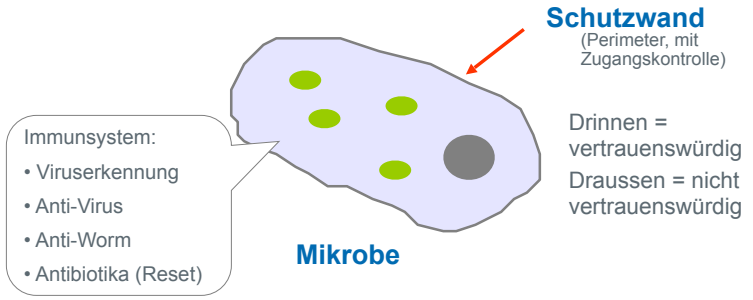
Office hours

Mo – Fr: 8am – 5pm, 9am – 6pm

Tu – Mo: 9am – 4pm

Was ist Kapselung?

DHBW Stuttgart



Kapselung = Perimeter-basierender Schutz

(ein fundamentales Konzept und ganz alter Hut)

Inhalt

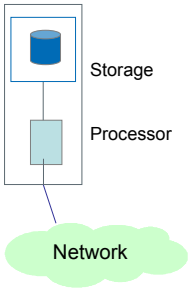
DHBW Stuttgart

Sicherheit

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

Redundanz: Grundlagen

DHBW Stuttgart



Zu schützen:

- Zustände (States) im Prozessor
- Daten im Speicher

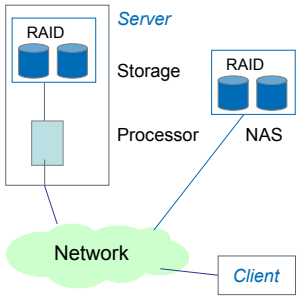
Lösungen:

- 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

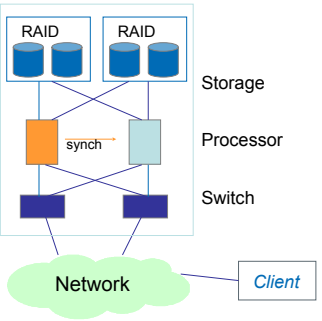
Lösung:

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

- Reicht für kleine Netze (nicht wirklich hochverfügbar)

Doppelt genäht hält besser

DHBW Stuttgart



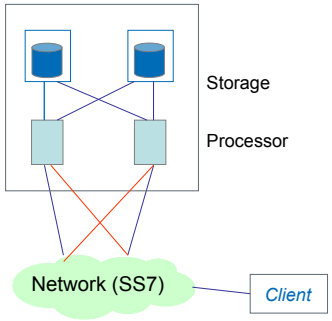
Systemarchitektur

- 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

DHBW Stuttgart



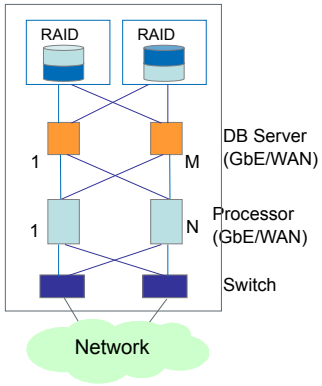
Systemarchitektur

- 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

DHBW Stuttgart



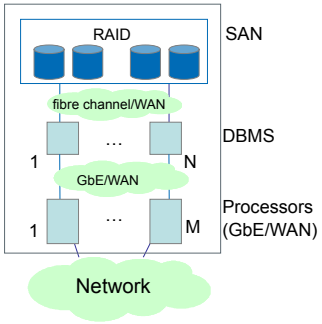
Systemarchitektur

- 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

DHBW Stuttgart



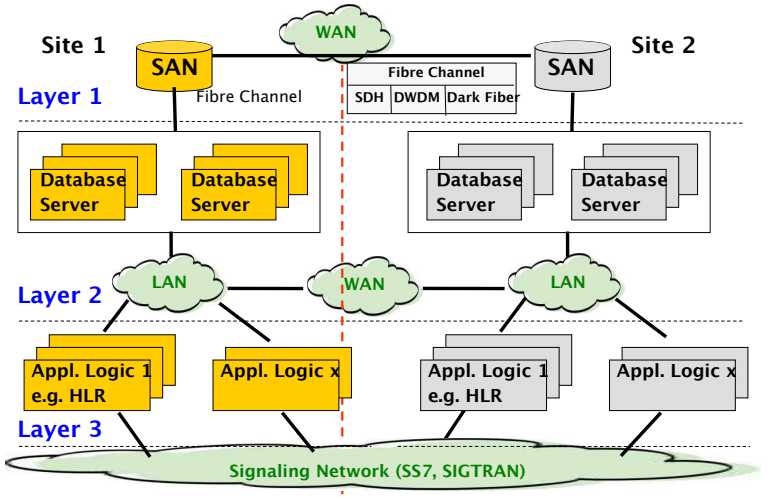
Systemarchitektur

- 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.

ENDE Teil 5

Sichere Kommunikation

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

DHBW Stuttgart

Kommunikationssysteme
Teil 6 – Funktionale Sicherheit (Safety)

Stephan Rupp
Masterstudium Informations- und Kommunikationstechnik

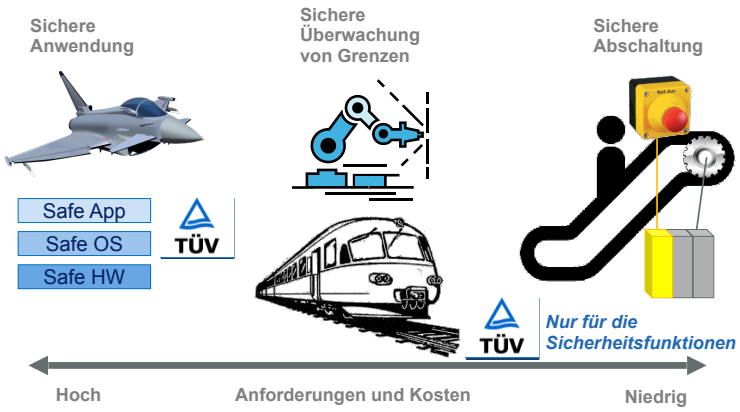
www.dhbw-stuttgart.de

Inhalt

Funktionale Sicherheit

- Lösungsansätze
- Realisierungsbeispiel
- Methoden

Lösungsansätze

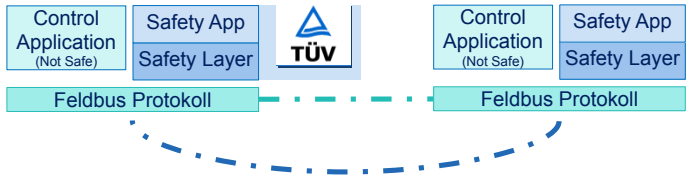


Im Mittelfeld

Sichere Abschaltung und Überwachung von Grenzen

Konzept:

- Nicht sichere Steuerung (Hauptprozessor)
- Sichere Überprüfung von Grenzen, Steuerung der Sicherheitsfunktionen durch sicheren Schaltkreis (Nebenprozessor bzw. CPU-Segment)



- Ethernet basierender Feldbus
- Mit eingebetteten Safety-Nachrichten (Tunnel bzw. Black Channel)
- Safety-Controller in einkanaliger bzw. zweikanaliger Ausführung

Sicherheitsprotokoll für Feldbusse

DHBW Stuttgart

Safety Layer: Fehlerfälle und Sicherheitsmaßnahmen

	Maßnahme			
Fehler	Sequenz Nummer	Watchdog	Connection ID	CRC (Prüfsumme) Berechnung
Unbeabsichtigte Wiederholung	x			x
Verlust	x	x		x
Eingefügte Nachricht	x			x
Inkorrekte Sequenz	x			x
Verfälschung				x
Unakzeptable Verzögerung		x		
Maskerade		x		x
Memory Fehler in Switches	x			x
Inkorrekte Weiterleitung zwischen Segmenten			x	

Anforderungen an den Safety Controller

DHBW Stuttgart

- Alle Komponenten sind auf erweiterten Temperaturbereich ausgelegt.
- Agiert als Feldbus Slave-Controller bzw. verfügt über eine Feldbus-Schnittstelle (zum Rücklesen von Nachrichten).
- Safety-Schaltkreis mit folgenden Funktionen
  - Überwachung von Spannungen
  - Überwachung von Temperaturen
  - Watchdog Timer
  - Failsafe Circuit
- Isolierter Aufbau mit getrennter Stromversorgung.
- Programmierschnittstelle (API) mit Safety-Funktionen.
- Kundenspezifische Safety-Anwendung, Zertifizierung zusammen mit der Kundenanwendung

Inhalt

DHBW Stuttgart

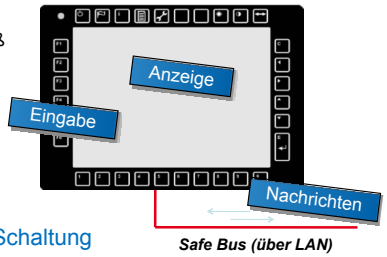
Funktionale Sicherheit

- Lösungsansätze
- Realisierungsbeispiel
- Methoden

Sicheres Anzeigeinstrument

DHBW Stuttgart

- Ziel: Ehrliche Anzeige
  - Zeigt immer des korrekten Status gemäß der am Feldbus empfangenen Nachrichten
  - Sendet stets korrekte Nachrichten gemäß der Bedienelemente (Tasten, Bildschirm)
  - Geht andernfalls in den sicheren Zustand über.

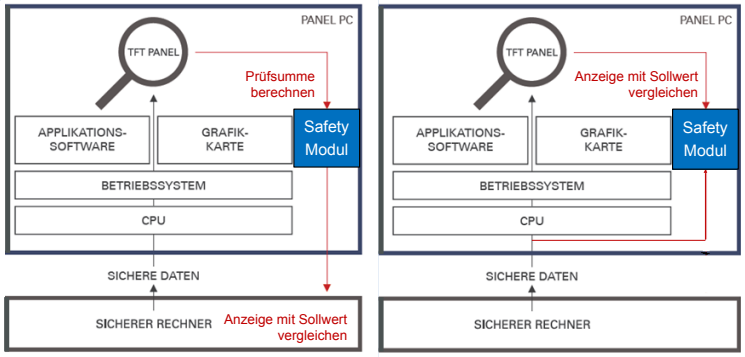


- Konzept: Hauptprozessor & Safety-Schaltung
- Hauptprocessor
  - Nicht sicher (e.g. x86 processor with Linux)
  - Tunnel für Nachrichten des Safety Layers vom Feldbus an den Safety Processor
- Safety-Schaltung
  - Terminiert das Safety Protocol
  - Überprüft die Integrität der Anzeige (bzw. Eingaben) gegen Nachrichten am Bus
  - Inititiiert ggf. den Übergang in den sicheren Zustand

Funktionsprinzip der sicheren Anzeige

DHBW Stuttgart

Rücklesen



Generische Lösung | Autonome Lösung

Quelle: Deuta Werke

Inhalt

DHBW Stuttgart

Funktionale Sicherheit

- Lösungsansätze
- Realisierungsbeispiel
- Methoden

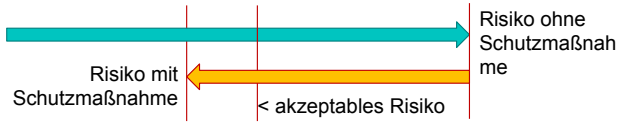
Funktionale Sicherheit (engl. Safety)

DHBW Stuttgart

- Ziel: Gefahren für Menschen und Umwelt durch Maschinen und Anlagen vermeiden.

  Maschinen und Anlagen sind derart auszulegen, dass Fehler und Defekte keine Gefährdung nach sich ziehen.

- Risiko = Schadenshäufigkeit * Schadensausmaß



- Prinzip: Senkung des Risikos auf ein akzeptables Maß durch Sicherheitsmaßnahmen.

Schutz der Integrität

DHBW Stuttgart

- Integrität (Unversehrtheit) der Funktion: Fehlfunktionen im Betrieb werden erkannt und vermieden (Beispiel: Bordcomputer).
- Sicherheit über den gesamten Lebenszyklus
  - Entwicklung, Prototypenfertigung, Nullserie
  - Serienfertigung, Installation, Inbetriebnahme

  } vorwiegend systematische Fehler

  - Betrieb mit Sicherheitsmaßnahmen
  - Reparaturen, Änderungen, Wartung, Fehlerbehebung
  - Stillsetzen, Entsorgen

  } besonders gefahrvoller Bereich

- Fehlermodelle: systematisch (Software), zufällig (Hardware)
- Verwandter Begriff: Sicherheit (englisch: Security) im Sinne von Schutz der Vertraulichkeit, Integrität und Verfügbarkeit

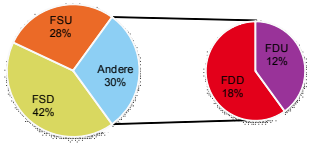
Safety Integrity Levels (SIL)

DHBW Stuttgart

Level	Rate tolerierbarer gefährlicher Fehler/ Stunde
SIL 4	10^{-9} bis 10^{-8}
SIL 3	10^{-8} bis 10^{-7}
SIL 2	10^{-7} bis 10^{-6}
SIL 1	10^{-7} bis 10^{-5}

Referenz für die Risikoakzeptanz:
Sterblichkeit für Jugendliche in Europa > 10^{-4} pro Jahr (pro Person), d.h. > 10^{-8} pro Stunde

- Fehlerkategorien und Ausfallraten
- Ungefährliche Ausfälle (**s**icher, safe): λ_S
  - Entdeckte ungefährliche Fehler: λ_{SD}
  - Unentdeckte ungefährliche Fehler: λ_{SU}
- Gefährliche Ausfälle (**d**angerous): λ_D
  - Entdeckte gefährliche Fehler: λ_{DD}
  - Unentdeckte gefährliche Fehler: λ_{DU}



FSD: λ_{SD} ungefährlich, endeckt
FSU: λ_{SU} ungefährlich, unentdeckt
FDD: λ_{DD} gefährlich, entdeckt
FDU: λ_{DU} gefährlich, unentdeckt

Sicherheitsanforderungen …

DHBW Stuttgart

… und deren Umsetzung:

- Beschreibung der Anforderungen, Maßnahmen im Fehlerfall und der tolerierbaren Fehlerraten
- Erstellen des Sicherheitskonzepts
- Ausfalleffektanalyse (englisch: FMEA - Failure Modes and Effects Analysis)
- Für alle sicherheitsspezifischen Komponenten festzulegen:

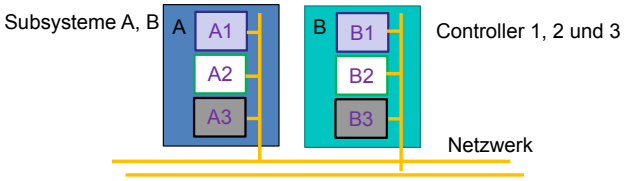
Komponente:	Fehlermodell:	Anforderungen:	Maßnahmen:
Register, RAM	Daten/Adressen	DC > 90%	Speichertests
pc, stack pointer	Datenfehler	DC > 90%	Prüfsumme
Bus	Time Out	DC > 90%	Time out
…	…	…	…

- Diagnoseabdeckung (englisch DC – Diagnostic Coverage): Anteil der entdeckten gefährlichen Fehler (λ_{DD} / (λ_{DD} + λ_{DU}))

Hardware-Fehlertoleranz

DHBW Stuttgart

- Mehrkanalige Ausführungen
  - fehlerhafter Zweig kann ignoriert werden
  - dadurch erhöhte Verfügbarkeit (z.B. Flugzeug vs. Rolltreppe)
  - Fehlererkennung (z.B. durch Prüfsummen, bzw. Mehrheitsvotum, beispielsweise 2 aus 3)
- Beispiel: Stellwerk, zweikanaliges System aus Subsystemen A und B mit diversitär aufgebauten Controllern (unterschiedliche Prozessoren und Betriebssysteme)



Einstufung mehrkanaliger Systeme

DHBW Stuttgart

Anteil der sicheren Ausfälle (SFF)	Hardwarefehlertoleranz (redundante Kanäle)		
	0	1	2
< 60%	nicht erlaubt	SIL 1	SIL 2
60% bis 90%	SIL 1	SIL 2	SIL 3
90% bis 99%	SIL 2	SIL 3	SIL 4
> 99%	SIL 3	SIL 4	SIL 4

- Anteil der sicheren Ausfälle (englisch: SFF- Safe Failure Fraction): (λ_S + λ_{DD}) / (λ_S + λ_{DD} + λ_{DU})
- Weitere Definitionen:
  - Restfehlerrate (Residual Failure Rate): λ_{DU}
  - MTBDF (Mean Time Before Dangerous Failure): 1/ λ_{DU}
  - MTBF (Mean Time Between Failure): 1 / λ = 1 / (λ_S + λ_{DD} + λ_{DU})

Definitionen

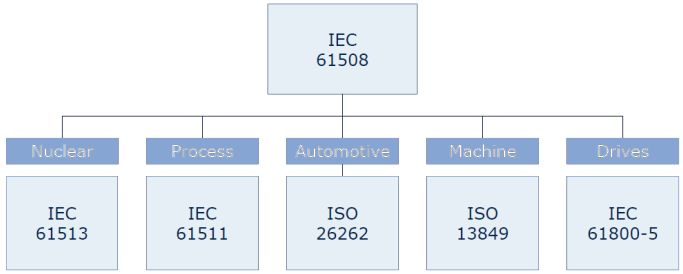
DHBW Stuttgart

Ausfallraten und MTBF (Mean Time Between Failure)

- Funktion: $R(t) = e^{-\lambda t}$ mit $1/\lambda$ = MTBF
- Fehlfunktion: $P(t) = 1 - R(t) = \lambda t$ (Taylor Reihe $e^{-\lambda t}$ für $\lambda t << 1$)
- Zeitbezug: fit = $1 / 10^9$ Stunden
- MTBF Berechnung für Systeme: durch Summation der Ausfallraten der Komponenten
- Verfügbarkeit: (Zeitintervall – Ausfallzeit) / Zeitintervall
- Ausfallzeit: Fehler plus Reparaturzeiten im Zeitintervall
- Redundanz erhöht die Verfügbarkeit des Gesamtsystems (Beispiel: RAID-System aus 2 Festplattenlaufwerken mit 90% Verfügbarkeit pro Tag)

Normatives Umfeld

DHBW Stuttgart



- Bahnanwendungen: EN50126 (RAMS), EN50128 (Software), EN50129 (Systeme und Hardware), EN50159 (Kommunikationssysteme)
- Medizintechnik: IEC 62304 (Software), EN60601 (Geräte); ISO 14971 (Risikomanagement), ISO 13485 (Qualitätsmanagement), ISO 14155-1/2 (klinische Prüfung an Menschen)

Zusammenfassung

DHBW Stuttgart

- Unterschiedliche Lösungsansätze mit unterschiedlichem Aufwand
  - Für industrielle Steuerungen und zur Steuerung von Fahrzeugen ist eine Abgrenzung des sicherheitsrelevanten Bereiches möglich.
  - Die Steuerung der Sicherheitsfunktionen und Überwachung von Grenzen des Hauptcontrollers erfolgt durch den Safety-Controller.
- Für die Hardware findet sich ein Strickmuster mit Anpassungen an unterschiedliche Feldbusse, sowie mit anwendungsspezifischer Programmierschnittstelle (Safety-API).
- Die Zertifizierung erfolgt zusammen mit der kundenspezifischen Anwendung.
- Übersicht über die Methoden: Ziel ist die Restfehlerrate durch Aufdeckung gefährlicher Fehler zu minimieren.

ENDE Teil 6 – Funktionale Sicherheit (Safety)