Motivierende Fragen

- Warum gibt es geschichtete Kommunikationsarchitekturen? Welche Kommunikationsschichten gibt es?
- Wie lässt sich die Medienzugriffssteuerung bei drahtgebundenen Netzen realisieren?
- Welche Funktionalität kann man bei Brücken finden?
- Welche Routingprotokolle gibt es im Internet?
- Was versteht man unter Round-Trip-Time? Warum ist diese Größe für TCP wichtig?
- Welche Transparenzprinzipien sollen durch Middleware realisiert werden? Wie lassen sich Web Services charakterisieren?
- Welche Sicherheitsdienste gibt es? Wie können die Sicherheitsziele sichergestellt werden? Wie sind Zertifikate aufgebaut, und wie werden sie eingesetzt?

Lehrstuhl für Netzarchitekturen und Netzdienste
Institut für Informatik – Technische Universität München
Prof. Dr.-Ing. Georg Carle

Grundlagen: Rechnernetze und Verteilte Systeme

Zusammenfassung

Rückblickender Überblick über Kapitel 1-12

Prof. Dr.-Ing. Georg Carle
Lehrstuhl für Netzarchitekturen und Netzdienste
Technische Universität München
carle@net.in.tum.de
http://www.net.in.tum.de

TECHNISCHE UNIVERSITÄT MÜNCHEN

Ankündigungen zu Vorlesungen im Wintersemester

- **Vorlesung Netzsicherheit - IN2101**
  - ECTS 5.0
  - Sprache Deutsch
  - Vorläufige Termine
    - Mi 14:15 - 16:00 MI 00.08.038 ab 21.10.2009 wöchentlich
    - Do 14:15 - 16:00 MI 00.08.038 ab 22.10.2009 wöchentlich

- **Vorlesung Masterkurs Rechnernetze - Internet-Protokolle - IN2097**
  - ECTS 5.0
  - Sprache Englisch / Deutsch
  - Vorläufige Termine
    - Mo 16:15 - 17:45 MI HS 2 ab 19.10.2009 wöchentlich
    - Fr 10:15 - 11:45 MI HS 2 ab 23.10.2009 wöchentlich

Ankündigung Internet-Praktikum

- **Internet-Praktikum**
  - Im Praktikum haben Sie Gelegenheit, vieles von dem, was Sie theoretisch in der Vorlesung kennen gelernt haben, praktisch auszuprobieren.
  - Nach Teilnahme am Praktikum sind Sie in der Lage, Ihr eigenes „Internet“ aufzubauen oder wissen umgekehrt, warum vieles funktioniert oder auch nicht funktioniert, da Sie es selbst ausprobiert haben.

Ankündigung Seminare

- **Proseminar „Network Hacking“**
  Im Wintersemester wöchentlich
  Freitags 14:00 - 16:00 Uhr in Raum 03.07.023

- **Seminar „Innovative Internet-Technologien und Mobilkommunikation“**
  Im Wintersemester wöchentlich
  Montags 14:00 – 16:00 im Raum 03.07.023

- **Blocksseminar „Future Internet“**
  Das Seminar findet am Mo 12. und Di 13. Oktober 2009 statt.

Prüfungsmodalitäten

Klausurtermin

- Klausur: Di 28.07.2009 14:00-16:30 MW2001
- Nachholtermin: Di 13.10.2009 14:00-16:30 MW2001
- Die Bearbeitungszeit beträgt 90 Minuten.
- Die reguläre Anmeldung zur Klausur sollte erfolgt sein.
- Studenten, die sich aufgrund ihres Studiengangs nicht anmelden können, schicken bitte eine Mail an rnvs@net.in.tum.de mit folgenden Daten:
  - Matrikelnummer
  - Vorname Nachname
  - Studiengang
  - Geburtsdatum
  - Semester

Zur Klausur zugelassene Materialien

- Ausdruck der Vorlesungsfolien (Markierungen und Anmerkungen im Rahmen dessen, was in der Vorlesung gesagt wurde, sind erlaubt)
- Post-Its/Indexstreifen zum schnelleren Auffinden von Kapiteln (Kapitelnummern und -überschriften sind erlaubt)
- zwei beidseitig und handschriftlich beschriebene A4-Blätter mit Notizen und Formelsammlung
- Taschenrechner (nicht programmierbar)

Notenbonus

- Der Notenbonus gilt für die Klausur und die Wiederholungsklausur.

  Er gilt auch wenn man die Hauptklausur nicht besteht für die Nachklausur.
  Er gilt also für beide Klausuren, die wir zur Vorlesung dieses Semesters abhalten und verfällt auch nicht bei einmaligem "Einsatzversuch".

- Er findet allerdings nur Anwendung, wenn man besteht, also besser als 4.0 hat.

- Er gilt nicht im nächsten Semester.

Hinweise zur Klausur

- Leistung = Arbeit / Zeit
  - Also: zügige (aber nicht schlampige) Bearbeitung ist wichtig
- Verständnis ist wichtig
  - Erklären von Sachverhalten üben (was man im Kopf oder im Gespräch mit einem Kommilitonen bereits einmal vorformuliert hat, kann man auch schriftlich in guter Qualität reproduzieren)
- Charakter der Prüfungsfragen
  - Die Übungsaufgaben sind ein gutes Beispiel dafür, wie die Aufgaben in der Klausur gestellt werden
  - Motivierende Fragen zu Beginn der Vorlesung sollen das Nachdenken anregen, sind aber nicht als Beispiele für Prüfungsaufgaben gedacht
- Aufgaben lösen können ist wichtig
  - Wer an Übung nicht teilgenommen hat, soll trotzdem Lösen von Aufgaben üben

Lehrstuhl für Netzarchitekturen und Netzdienste
Institut für Informatik – Technische Universität München
Prof. Dr.-Ing. Georg Carle

Grundlagen: Rechnernetze und Verteilte Systeme

Rückblickender Überblick über Kapitel 1-12

Prof. Dr.-Ing. Georg Carle
Lehrstuhl für Netzarchitekturen und Netzdienste
Technische Universität München
carle@net.in.tum.de
http://www.net.in.tum.de

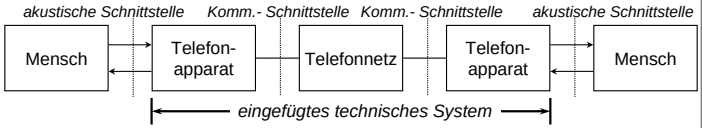
TECHNISCHE UNIVERSITÄT MÜNCHEN

Zusammenfassung

1. Einführung und Motivation
   - Bedeutung, Beispiele
2. Begriffswelt und Standards
   - Dienst, Protokoll, Standardisierung
3. Nachrichtentechnik
   - Daten, Signal, Medien, Physik
4. Bitübertragungsschicht
   - Codierung
   - Modems
5. Direktverbindungsnetze
   - Fehlererkennung, Protokolle
   - Ethernet
6. Vermittlung
   - Vermittlungsprinzipien
   - Wegwahlverfahren
7. Internet-Protokolle
   - IP, ARP, DHCP, ICMP
   - Routing-Protokolle
8. Transportprotokolle
   - UDP, TCP
9. Verkehrssteuerung
   - Kriterien, Mechanismen
   - Verkehrssteuerung im Internet
10. Anwendungsorientierte Protokolle und Mechanismen
    - Netzmanagement
    - DNS, SMTP, HTTP
11. Verteilte Systeme
    - Middleware
    - RPC, RMI
    - Web Services
12. Netzsicherheit
    - Kryptographische Mechanismen und Dienste
    - Protokolle mit sicheren Diensten: IPSec etc.
    - Firewalls, Intrusion Detection

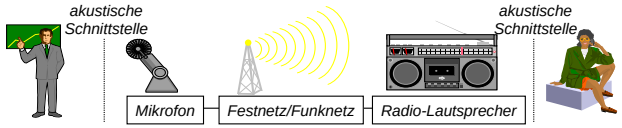
1. Einführung
Kommunikation mit technischer Mitteln - Telekommunikation

- Die klassische Nachrichtentechnik / Telekommunikationstechnik ist von der Sprachkommunikation (Telefon) geprägt - technisch und wirtschaftlich
- Menschen als Kommunikationspartner:



Modell einer Telefonkommunikation

⇨ Das technische System wird in den - ansonsten weitgehend unveränderten - Kommunikationsablauf eingefügt.



Modell einer Rundfunkkommunikation

2. Begriffe - Motivierende Fragen

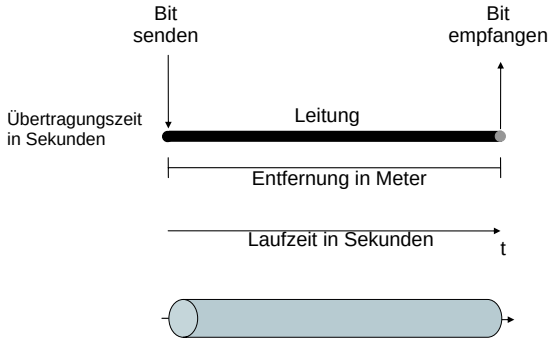
- Wie kann ein Protokoll eindeutig beschrieben werden?
- Welche Grundmechanismen können in Protokollen identifiziert werden?
- Wie können Nachrichten übermittelt werden und mit welchen Problemen muss man rechnen?
- Welche Schichten gibt es im Kommunikationsmodell?

2. Begriffe - Kapitelgliederung

2.2. Grundlegende Problemstellungen der Kommunikation

- Regelung des Kommunikationsablaufs
  → Protokolle, Protokollschichten
- Ressourcenverteilung bei mehreren Kommunikationspartnern
  → Vielfachzugriff (Multiple Access)
- Kommunikation über Zwischenknoten
  → Vermittlung (Switching)
- Abarbeitung paralleler Kommunikationsvorgänge
  → Scheduling
- Identifikation von Kommunikationspartnern
  → Namen und Adressen
- Wahl des besten Kommunikationspfades
  → Routing
- Umgang mit Übertragungsfehlern
  → Fehlerkontrolle (Error Control)
- Anpassung der Übertragungsgeschwindigkeit
  → Flusskontrolle (Flow Control)

2.4. Technischer Hintergrund - Technische Leistung

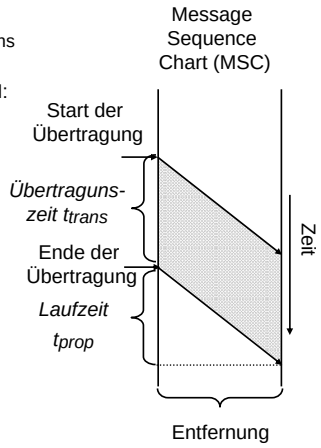


Durchsatz (auch: Datenrate bzw. Bandbreite)
= Anzahl der pro Sekunde übertragenen Bits
[Einheit bit/s]

Bandbreiten-Verzögerungs-Produkt
= Speicherkapazität einer Leitung

Signalausbreitung im Medium, Datenspeicherung

- Senden einer Nachricht benötigt Übertragungszeit (transmission delay) t_{trans}
  - Übertragungszeit abhängig von Datenrate **r** and Länge der Nachricht N: $t_{trans} = N / r$
- Signale erreichen nach Laufzeit (propagation delay) t_{prop} ihr Ziel
  - Abhängig von Entfernung und Ausbreitungsgeschwindigkeit im Übertragungsmedium
- Über die Laufzeit t_{prop} werden $r * t_{prop}$ bit generiert
  - Gespeichert im Medium
- Gesamtverzögerung:
  $t = t_{trans} + t_{prop} (+ t_{proc} + t_{queue})$
  - t_{proc} : Verarbeitungszeit (processing delay)
  - t_{queue} : Wartezeit (queuing delay)

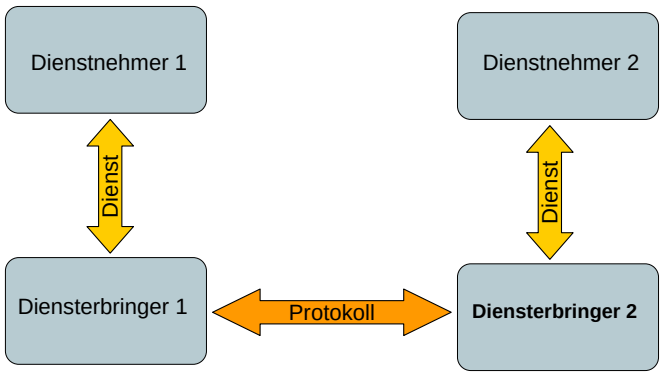


2.5. Kommunikationsarchitekturen

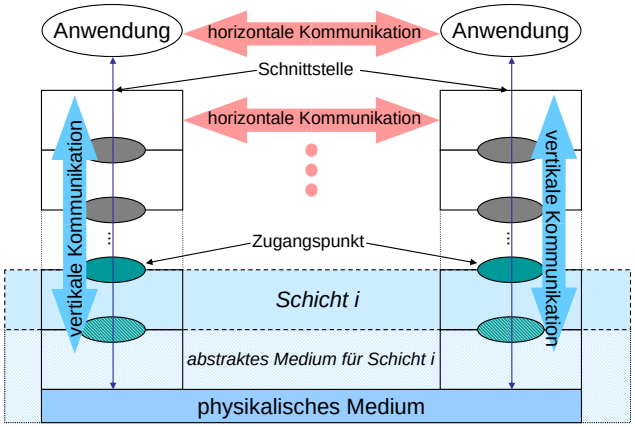
- Zur Realisierung von Kommunikationsvorgängen wird eine Kommunikationsarchitektur benötigt für:
  - physikalische Konnektivität
    Verbindung über Kupferkabel, Lichtwellenleiter, Luftschnittstelle, ...
  - Kommunikationsfunktionalität
    - Steuerung des Ablaufs
    - Adressierung der Kommunikationspartner
    - Garantie einer geforderten Qualität
    - Anpassung unterschiedlicher Formate
    - ...
  - Schnittstelle zu den Anwendungen

- Aufgrund der *unterschiedlichen Aufgaben:*
  - Kommunikationsarchitektur mit geschichtetem Aufbau üblich
  - eine Schicht nutzt die Funktionalität der darunter liegenden Schicht, um ihre eigenen Funktionen zu realisieren

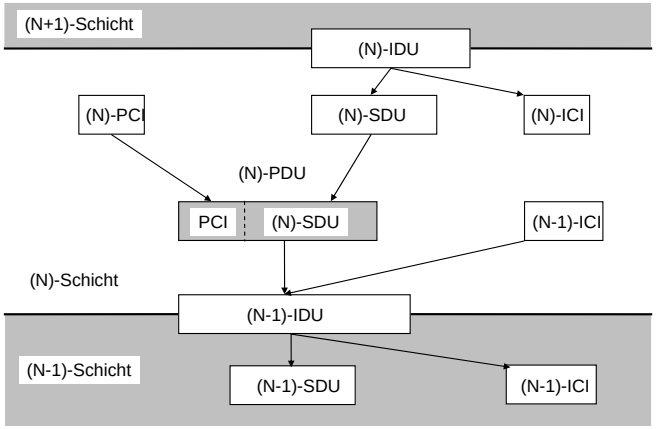
Dienst und Protokoll



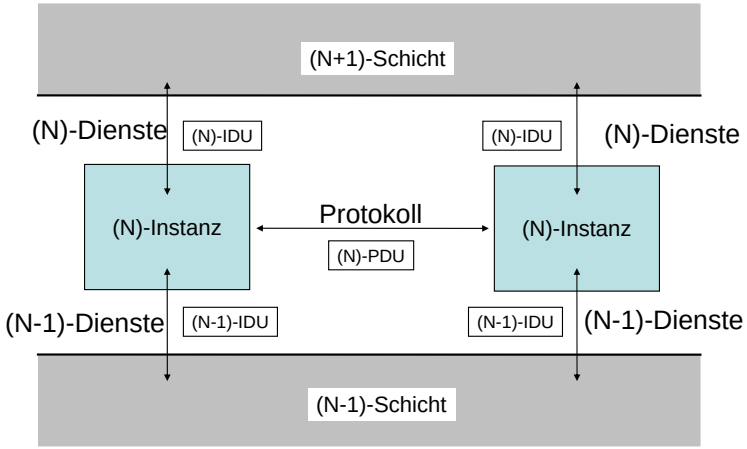
Geschichtetes Kommunikationssystem



Generische OSI-Kommunikationseinheiten



Kommunikation innerhalb und zwischen OSI-Systemen



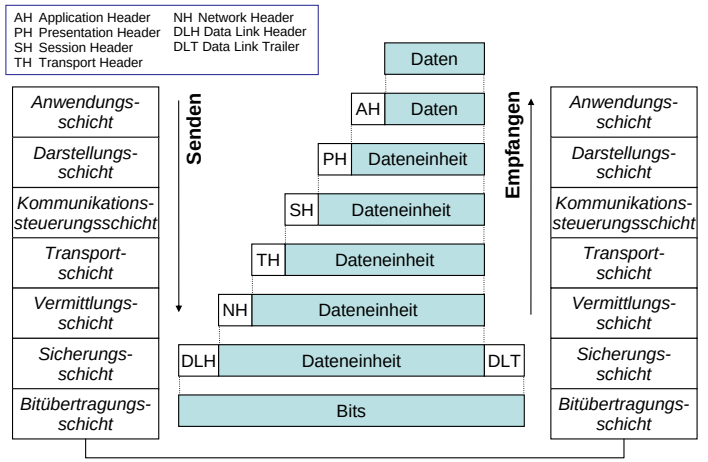
Protokollmechanismen

- Ein Protokollmechanismus ist ein Verfahren, welches abgeschlossene Teilfunktion innerhalb des Protokollablaufs beschreibt: generischer Charakter (ähnlich 'Systemfunktion').
- In verschiedenen Kommunikationsarchitekturen verwendet.
- Oft in mehreren Protokollen/Schichten einer Kommunikationsarchitektur anzutreffen.

- Multiplexen / Demultiplexen
- Teilung / Vereinigung
- Segmentieren / Reassemblieren
- Blocken / Entblocken
- Verkettung / Trennung
- (Mehrfach-)Kapselung
- Fehlerbehandlung
- Sicherung (ggf. fehlererkennend)
- Sequenzüberwachung
- Quittierung (Acknowledgement)

- Zeitüberwachung (Timeout)
- Wiederholen; Rücksetzen
- Flusskontrolle (Sliding window)
- Routing (Wegewahl, Weiterleiten)
- Medienzuteilung für geteilte Medien
- Synchronisation
- Adressierung
- Verbindungsverwaltung
- Datentransfer

Einkapselung von Daten

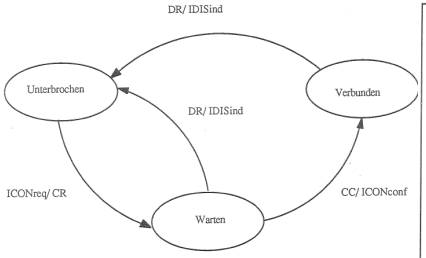


2.7. Protokollspezifikation mit SDL

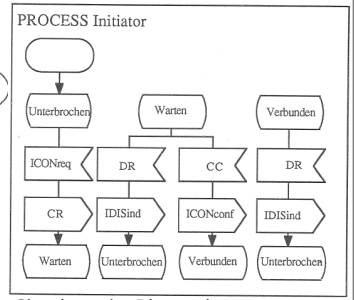
- Prozess als Grundelement
  - erweiterter endlicher Automat (Extended Finite State Machine - EFSM)
  - kommuniziert mit anderen Prozessen durch den Austausch von Nachrichten (Signalen) über Verbindungswege (Kanäle)
  - mehrere Prozesse arbeiten parallel und existieren gleichberechtigt nebeneinander
- Vordefinierte und benutzerdefinierte Datentypen
- Zwei äquivalente Darstellungsformen:
  - SDL/GR (Graphical Representation)
  - SDL/PR (Phrase Representation)
- Vorteile einer formalen Sprache
  - Exakte Spezifizierung
  - Möglichkeit von Werkzeugen - Editoren, Simulatoren, Prototyp-Generatoren, Testfall-Generatoren, Werkzeuge zur formalen Verifikation
    - Generatoren (Compiler) zur direkten Übersetzung von SDL in ausführbare Programme oder Programmgerüste

Übersetzbarkeit von Automaten in SDL-Graphen

Beispiel ⇨ InRes-Protokoll (InRes= Initiator-Responder), c.f. Folie 81



Zustandsgraph



Prozess in SDL/GR

Signale von/zu Dienstnehmer
- ICONreq: InRes-Connection-Request
- ICONconf: InRes-Connection-Confirm
- IDISreq: InRes-Disconnection-Request
- IDISind: InRes-Disconnection-Indication

Signale von/zu entfernter Instanz
- CC, DR, ...

aus: Hogrefe, „ESTELLE, LOTOS und SDL“, Springer Compass, 1989, S.121ff

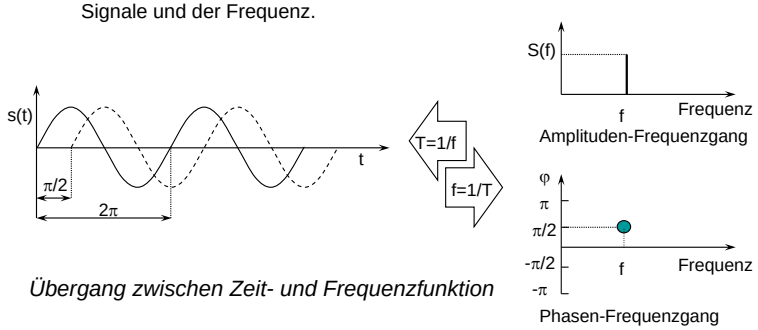
11. Nachrichtentechnik - Motivierende Fragen

- Welche Arten von Signalen gibt es?
- Wie werden Signale übertragen?
- Welche Übertragungsmedien existieren?
- Was versteht man unter Pulse-Code-Modulations-Technik (PCM)?
- Welche Signalkonversionen gibt es?

11. Nachrichtentechnik - Kapitelgliederung

11.1.2. Beschreibung von Signalen Zeitdarstellung/Frequenzdarstellung

- **Zeitfunktion (Zeitdarstellung):**
  - Die Zeitfunktion ist eine Zuordnung von Signalwert und Zeit.
- **Frequenzfunktion (Frequenzgang, Spektrum):**
  - Die Frequenzfunktion ist eine Zuordnung von Werten sinusförmiger Signale und der Frequenz.



Übergang zwischen Zeit- und Frequenzfunktion

Schritt- versus Übertragungsgeschwindigkeit

- **Schrittgeschwindigkeit** v_S (**symbol rate**, modulation rate, digit rate)
  - Gibt - anschaulich - die Zahl der ggf. nur potenziellen Signalparameter-Zustandswechsel an (Schrittumschläge).
  - Für isochrone Digitalsignale gilt: $\mathbf{v_S = 1/T}$ (T: Schrittdauer)
  - **Einheit: 1/s = baud** (Abk. bd)

- **Übertragungsgeschwindigkeit** Φ (**Einheit: bit/s**)
  - Für zweiwertige Signale (binäre Signale):
    Jeder Schrittumschlag codiert ein Bit. Deshalb gilt in diesem Fall:
    $\mathbf{v_S}$ *(in baud)* $\mathbf{= \Phi}$ *(in bit/s)*
    Die Übertragungsgeschwindigkeit wird in diesem Fall als *Bitrate (bit rate)* bezeichnet.
  - Für mehrstufige Signale (mit n möglichen Wertestufen):
    Übertragungsgeschwindigkeit Φ (in bit/s): $\mathbf{\Phi = v_S * ld(n)}$
    Bei DIBIT-Codierung: 1 baud = 2 bit/s (quaternäres Signal)
    Bei TRIBIT-Codierung: 1 baud = 3 bit/s (oktonäres Signal)

Nyquist-Kriterium und Shannon-Kanalkapazität

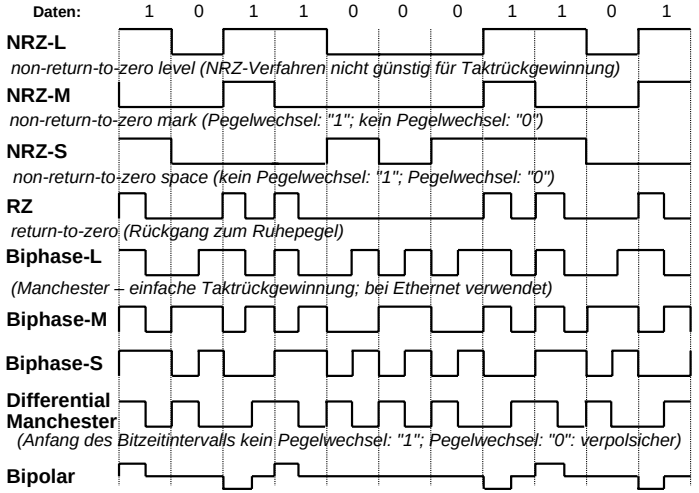
- 1924, H. **Nyquist**:
  Maximale Schrittgeschwindigkeit v_S für einen **Kanal mit eingeschränkter Bandbreite**:
  $\mathbf{v_S = 2\ B}$
  mit B = Bandbreite des Kanals
- Daraus ergibt sich eine maximale Datenrate für einen **rauschfreien** Kanal:
  max. Datenrate $\mathbf{= v_s\ ld(n)}$
  $\mathbf{= 2\ B\ ld(n)}$ **[bit/s]**
  mit n = Anzahl diskreter Signalstufen
- Bsp.: Kanal mit 3.000 Hz Bandbreite, binäres Signal
  → max. Datenrate: 6.000 bit/s

- 1948, C. **Shannon**:
  (auch bekannt als *Shannon-Hartley-Gesetz*)
  Kanalkapazität = informationstheoretische obere Grenze für die Information (in Bit), die in einem Schritt **fehlerfrei** über einen Kanal mit **weißem Rauschen** übertragen werden kann
- Daraus ergibt sich eine maximale Datenrate, die mit einer hypothetischen optimalen Kanalkodierung erreichbar ist:
  max. Datenrate = B ld(1+S/N) **[bit/s]**
  mit S/N = Signal-Rauschverhältnis
- Bsp.: Kanal mit 3.000 Hz Bandbreite, S/N = 1000 = 30dB [1)]
  → max. Datenrate: 30.000 bit/s
  Durch Verwendung von fehlererkennenden bzw. –korrigierenden Codes (Redundanz!) wird aber mit höherer Rate gesendet!

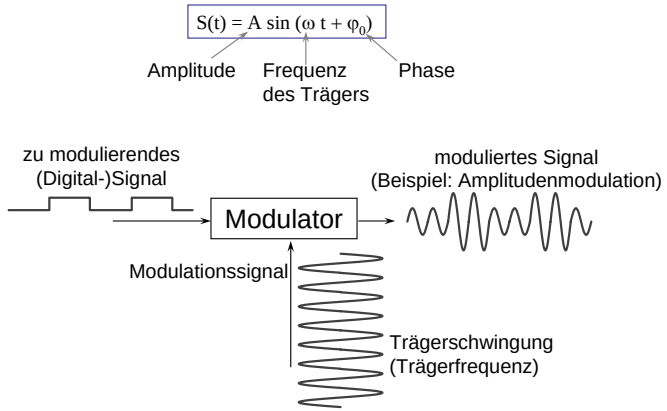
[1)] Signal-Rauschverh. in dB = $10 \log_{10}(S/N)$ [dB]

Achtung: Da für einen Kanal stets beide Sätze gelten, ergibt sich die fehlerfrei erreichbare maximale Datenrate aus dem *Minimum* der beiden Ergebnisse!

Moderne Basisbandverfahren - Beispiele



Prinzip der Schwingungsmodulation



Schwingungsmodulation: analoger Signalträger ist Sinusschwingung

11.4.3. Mehrfachnutzung von Übertragungswegen

- Zusammenfassung von Übertragungskanälen auf einem Übertragungsweg: Bündelung oder Multiplex
  - Richtungsmultiplex
  - Raummultiplex
  - Frequenzmultiplex
  - Zeitmultiplex
  - Codemultiplex

11.5 PCM-Technik

- Abtasttheorem von Shannon und Raabe (1939)
  Abtasttheorem: Eine Signalfunktion, die nur Frequenzen im Frequenzband B (bandbegrenztes Signal) enthält, wobei B gleichzeitig die höchste Signalfrequenz ist, wird durch ihre diskreten Amplitudenwerte im Zeitabstand $\mathbf{t_0 = 1/(2B)}$ vollständig bestimmt.
- Abtastung des PCM-Fernsprechkanal: Frequenz, Periode
- Quantisierung
- Codierung
- Segment-Kompressorkennlinie

11.4.4. Digitale Übertragung analoger Daten - Abtasttheorem

Abtasttheorem von Shannon und Raabe (1939):

- Zur fehlerfreien Rekonstruktion des Signalverlaufs der abgetasteten Analogsignale ist eine Mindestabtasthäufigkeit (Abtastfrequenz f_A) erforderlich (bei periodischem Abtastzyklus).
- **Abtasttheorem:** Eine Signalfunktion, die nur Frequenzen im Frequenzband B (bandbegrenztes Signal) enthält, wobei B gleichzeitig die höchste Signalfrequenz ist, wird durch ihre diskreten Amplitudenwerte im Zeitabstand $\mathbf{t_0 = 1/(2B)}$ vollständig bestimmt.
- Andere Formulierung: Die Abtastfrequenz f_A muss mindestens doppelt so hoch sein wie die höchste im abzutastenden Signal vorkommende Frequenz f_S .

12. Bitübertragungsschicht - Motivierende Fragen

- Was versteht man unter der Bitübertragungs- und Sicherungsschicht ?
- Welche Bedeutung haben die einzelnen Schnittstellen ?
- Was verbirgt sich hinter einem Modem ?
- Was versteht man unter einem Breitbandkabelnetz ?
- Wie funktioniert die Datenübertragung über die Telefonleitung (xDSL) ?

12. Bitübertragungsschicht - Kapitelgliederung

Modemtechnologien

- **Kabelmodems:**
  Datenübertragung über das Breitbandkabel („Kabelfernsehen“) der Kabelnetzbetreiber,
  - Erweiterung des Frequenzbandes im Kabel auf bis zu 860 MHz
  - Datenraten (je nach Technik) theoretisch bis zu 2 Gbit/s, aber (mit anderen Benutzern) geteiltes Medium!
- **Powerline-Communications (PLC) Modems:**
  Datenübertragung über das Energieverteilnetz („Stromnetz“)
  - Einkopplung hochfrequenter Träger (16-148 kHz sowie 1-30 MHz)
  - Datenraten bis zu 1 Mbit/s, aber ebenfalls geteiltes Medium
  - Anwendbar für öffentliche Datennetze, Datenverteilung im Haus, sowie Telematik-Anwendungen der Energieversorger (z.B. Stromzähler auslesen)
- **DSL-Modems:**
  Höhere Datenraten über herkömmliches Telefonkabel
  - Telefonkabel bleibt gleichzeitig für Telefonie nutzbar
  - Typische Datenraten bei 6-8 Mbit/s

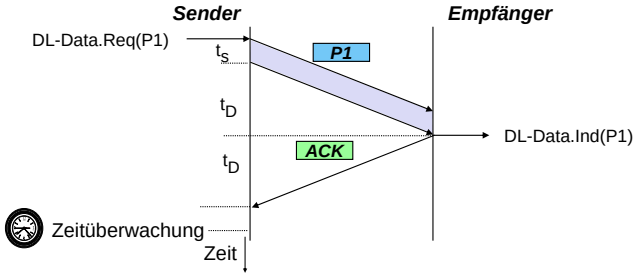
3. Direktverbindungsnetze - Motivierende Fragen

- Wie werden Daten und Signale übermittelt ?
- Welche Fehler können auftreten ?
- Welche Fehlerbehandlungen existieren ?
- Welche Zugriffsverfahren gibt es ?
- Welche Protokolle gibt es in der Sicherungsschicht ?
- Was versteht man unter Fast-Ethernet-Standard ?

3. Direktverbindungsnetze - Kapitelgliederung

Leistungsbetrachtung

- Die unterschiedlichen Protokolle können je nach Kanal zu großen Leistungsunterschieden führen



Bsp:

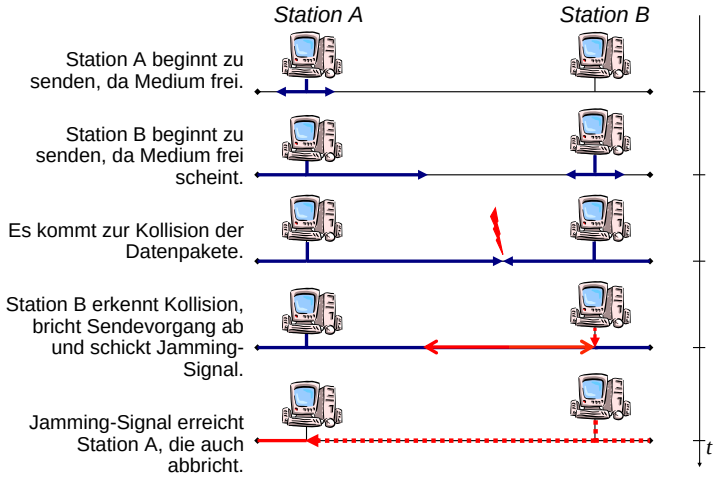
l_R	Rahmenlänge [bit]	l_R =1000 bit
Ü	Übertragungskapazität [bit/s]	Ü = 500 kbit/s
t_S	Sendezeit [s]	$t_S = l_R$ / Ü = 2 ms
t_D	Übertragungsverzögerung [s]	t_D = 240 ms
η	Kanalausnutzung (Effizienz)	$\eta = t_s / (t_s + 2\,t_D) \approx 0{,}4\%$

⇨ Effizienzsteigerung durch Schiebefensterprotokolle

Schicht-2-Protokolle: Konkrete Aufgabenstellung

- Datenblockformate:Festlegung und Erkennung
- Zeichenorientierten Protokolle: Vereinbarung Übermittlungsalphabet
- Übermittlungsprotokolle: Übermittlungssteuerungsverfahren
- Codetransparenz:
- Fehlererkennung und Fehlerbehebung:
  - Bitprüffolge mit CRC
  - Vorwärtsfehlerkorrektur
  - Go-back-N
  - Selektive Wiederholung
- Datenflusskontrolle:
  - Stop-and-Wait
  - Sliding Window
- Zugriffsregelung:
  - u.a. TDMA mit konkurrierendem Zugriff (Aloha vs. CSMA/CD)

Ablaufbeispiel CSMA/CD

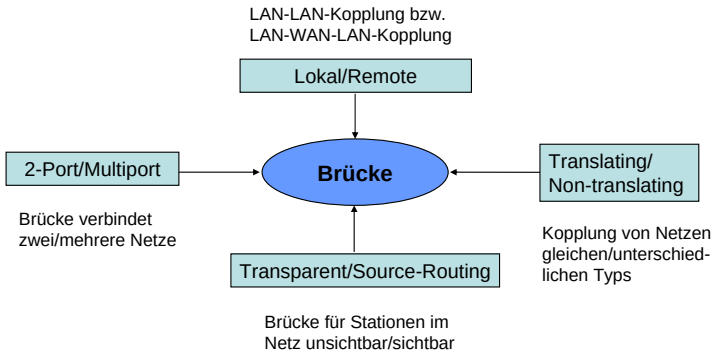


4. Vermittlung - Motivierende Fragen

- Was versteht man unter Repeater und Brücken ?
- Wie funktioniert ein LAN ?
- Was versteht man unter einer strukturierten Verkabelung ?
- Welche Arten von Vermittlungen in globalen Netzen gibt es ?
- Was ist ein Router und wie funktioniert er ?

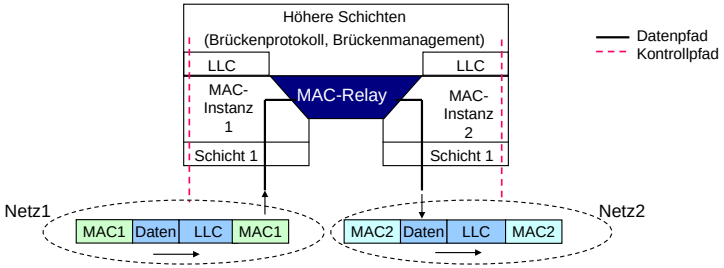
4. Vermittlung - Kapitelgliederung

Brücken – Übersicht



Transparente Brücke (MAC-Bridge)

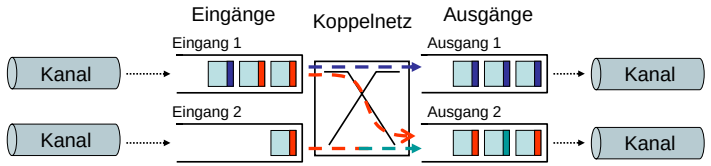
- Merkmale:
  - Lokale, translating Bridge
  - Für jedes Netzwerk eine eigene Schicht-1- und MAC-Instanz
  - Die MAC-Instanzen werden über ein MAC-Relay verbunden; dieses nimmt die Weiterleitungs- und Filterfunktion wahr
  - LLC-Instanzen nur für die höheren Schichten der Brücke (Brückenprotokoll, Brückenmanagement)



Spanning-Tree-Algorithmus

- Voraussetzungen:
  - Gruppenadresse zur Adressierung aller Brücken im Netzverbund
  - Eindeutige Brückenkennungen (MAC-Addresse)
  - Eindeutige Anschlusskennungen in jeder Brücke (MAC-Addresse)
  - Kosten an allen Anschlüssen einer Brücke („Anschlusskosten)
- Ablauf:
  1. Bestimmen der Root-Brücke (Wurzel des Baumes):
     - Zuerst nimmt jede Brücke an, dass sie Root-Brücke ist
     - Root-Brücken senden regelmäßig Hello-Pakete mit ihrer Brückenkennung aus
     - Bei Erhalt eines Hello-Pakets mit kleinerer Brückenkennung ordnet sich eine Root-Brücke der anderen unter und sendet das Paket als Broadcast
  2. Bestimmen der Root-Ports
     - Root-Port einer Bücke = Port über den der günstigste Pfad Richtung Root-Brücke (nur Kosten für Ausgangsports berücksichtigen!) verläuft
     - Summe über alle Anschlusskosten auf dem Weg zur Root-Brücke ist zu minimieren
     - Übertragungsgeschwindigkeit kann als Kostenfunktion dienen
  3. Bestimmen der Designated-Brücke:
     - Brücke mit günstigstem Root-Anschluss in einem Netzwerk wird als Designated-Brücke bestimmt
     - Root-Brücke ist Designated-Brücke für alle an sie angeschlossenen Netze

Vermittlungsknoten für virtuelle Verbindungen



- Verbindungskontext gespeichert in Weiterleitungstabellen

Eingang 1:

Eing.-VCI	Ausgang	Ausg.-VCI
A	1	A
B	2	B
...	...	...

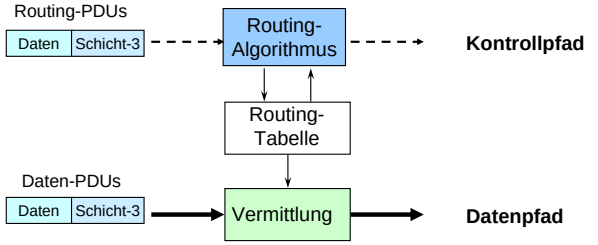
Eingang 2:

Eing.-VCI	Ausgang	Ausg.-VCI
B	2	C
...	...	...

VCI geändert, um Kollision zu vermeiden
⇨Label Swapping

- Weiterleitungsentscheidung wird anhand eines VCI (Virtual Circuit Identifier) getroffen
- Virtuelle Verbindungen müssen vorher aufgebaut werden

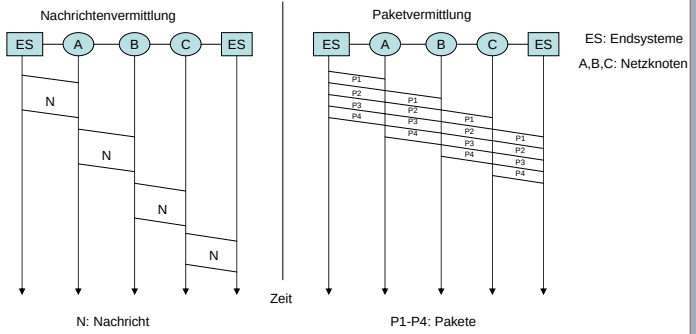
Router: Kontroll- und Datenpfad



- Datenpfad auf Netzwerkschicht
- Kontrollpfad darüber (Routing-PDUs sind in N-PDUs oder T-PDUs gekapselt)
- Gewinnung von Routinginformationen durch das **Routing-Protokoll**
- **Routing-Algorithmus** verwaltet die Routing-Tabelle bzw. Forwarding-Tabelle (Einfügen/Löschen/Ändern von Einträgen) auf der Basis der gewonnenen Routinginformation
- **Routing-Tabelle** bzw. Forwarding-Tabelle enthält Routinginformationen
- Wegewahl bei der Vermittlung wird anhand der Routing-Tabelle bzw. Forwarding-Tabelle durchgeführt

Nachrichtenvermittlung vs. Paketvermittlung

- Hauptunterschied zwischen Nachrichten- und Paketvermittlung
  - Paketvermittlung: Inhaltlich zusammengehörende Transfereinheiten (Transport-Datenblöcke der Schicht 4) werden in Pakete nach den Vorschriften des Paketvermittlungsnetzes segmentiert
  - Nachrichtenvermittlung: Wiederherstellung der Transfereinheiten in jedem Vermittlungssystem aus den Segmenten



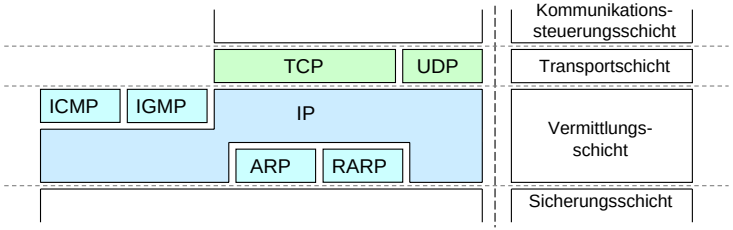
5. Internet-Protokolle - Motivierende Fragen

- Welche Protokolle gehören zur TCP/IP-Familie ?
- Welche IP-Dienste gibt es ?
- Wie ist die Routing-Hierarchie aufgebaut ?
- Was steckt hinter IPv6 ?
- Wie lassen sich Internet und Mobilität vereinen ?

5. Internet-Protokolle - Kapitelgliederung

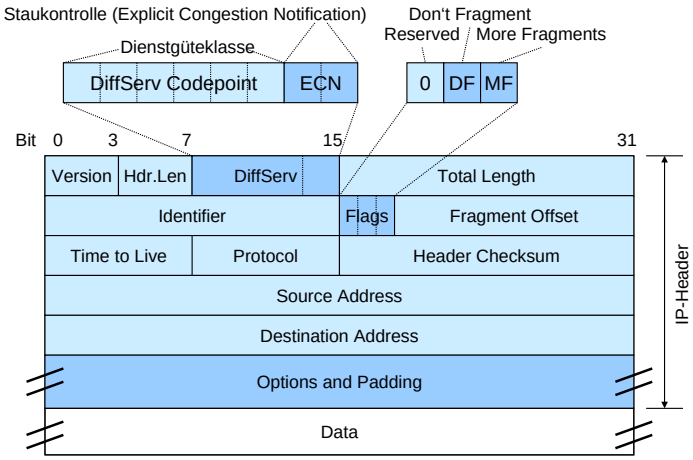
Die TCP/IP-Protokollfamilie – Überblick

- Die Bezeichnung TCP/IP wird häufig als Synonym für die gesamte Protokollfamilie verwendet
- Einordnung der Internetprotokolle in das ISO/OSI-Referenzmodell:



- Obwohl die IP-Steuerungsprotokolle ICMP und IGMP den IP-Dienst nutzen, werden sie dennoch der Vermittlungsschicht zugeordnet
- In den anwendungsbezogenen Schichten 5-7 werden im Internet Protokolle wie z.B. FTP, TELNET oder SMTP eingesetzt (Schichten 5-7 im Internet zusammengefasst zur Anwendungsschicht)

IP Datagramm: Aufbau



Übersicht: IP-Routing Protokolle

- **IGP** (Interior Gateway Protocol): zur Wegewahl *innerhalb* einer Verwaltungseinheit (Administrative Domain oder Autonomous System)
  - **RIP** (Routing Information Protocol) basierend auf Distance-Vector-Algorithmus (überall verfügbar, aber veraltet)
  - **OSPF** (Open Shortest Path First) basierend auf Link-State-Algorithmus (neuer Standard)
- **EGP** (Exterior Gateway Protocol): Wegewahl *zwischen* Verwaltungseinheiten, sog. „politische Firewall“
  - **BGP** (Border Gateway Protocol, derzeit Version BGP4, RFC 1654)
    - Wegewahl zwischen autonomen Systemen (AS) unter Berücksichtigung besonderer politischer, wirtschaftlicher oder sicherheitsbezogener Regeln (Policies).

5. Internet-Protokolle - Themen

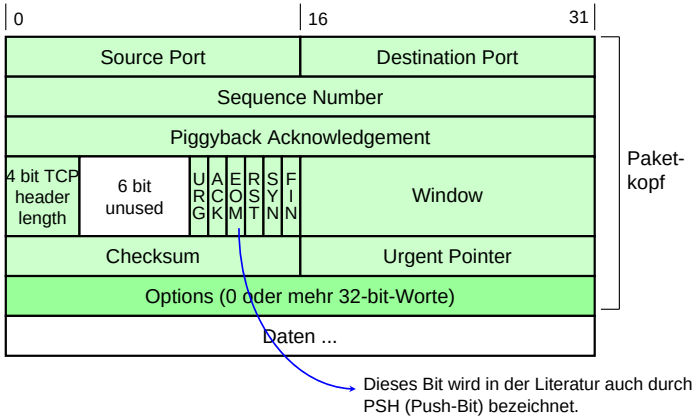
- IP-Adressen / Adressklassen (klassisch betrachtet)
- CIDR: Classless Inter-Domain Routing
- Network Adress Translation (NAT)
- Optionale IP-Dienste
- ICMP
- IGMP
- ARP
- IPv6
  - **Adressklassen**:
    - Unicast-, Anycast-, Multicast-Adressen
  - Unterscheidung von **Adresstypen**:
    - Link-Local Address, Site-Local Address, Aggr. Global Unicast Address
- Mobile IP

6. Transport-Protokolle - Motivierende Fragen

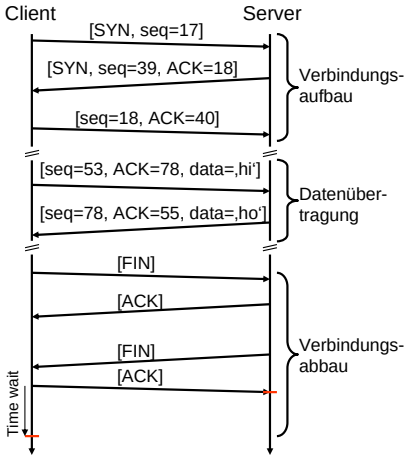
- Welche Transportdienste gibt es ?
- Welche Probleme können beim Transport entstehen ?
- Welche Aufgaben werden von der Transportschicht erledigt ?
- Wie funktioniert TCP ?
- Wie funktioniert UDP ?

6. Transport-Protokolle - Kapitelgliederung

TCP-Paketformat: Aufbau



TCP-Verbindungsaufbau/Datenübertragung/ Verbindungsabbau



- Verbindungsaufbau
  - 3-Wege-Handshake
  - Aushandlung von Fenstergröße, Sequenznummern
- Datenübertragung
  - Bestätigung im Huckepack
- Verbindungsabbau
  - Bestätigt
  - Ressourcenfreigabe auf Client-Seite erst nach time-wait (frozen reference), typisch sind 30 s, 1 min, 2 min – beeinflusst stark die Leistungsfähigkeit!

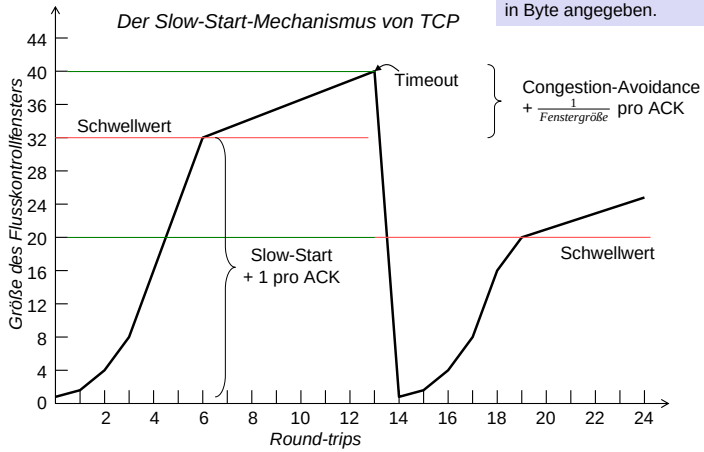
7. Verkehrssteuerung - Motivierende Fragen

- Was versteht man unter Lastkontrolle ?
- Wo können Engpässe in der Kommunikation entstehen ?
- Wie funktioniert die Flusssteuerung ?
- Was passiert bei einer Netzüberlastung ?
- Was versteht man unter Verkehrs-, Stau- und Ratenkontrolle ?
- Was versteht man unter der Dienstgüte (QoS)?

7. Verkehrssteuerung - Kapitelgliederung

Beispielablauf der Staukontrolle

Der Einfachheit halber stellen wir hier die Fenstergröße in Paketen dar.
Tatsächlich wird sie bei TCP in Byte angegeben.



Dienstklassen (QoS-Klassen)

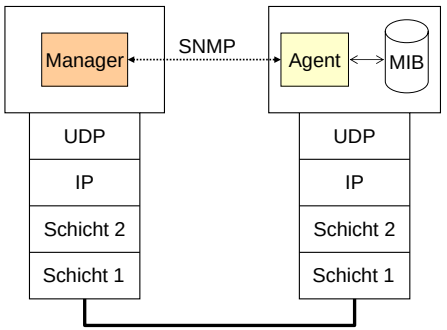
- **Deterministische Klasse:**
  - vorgegebene Schranken der QoS-Parameter werden exakt eingehalten
  - Ressourcen stehen einem Nutzer exklusiv zur Verfügung
  - keine Konflikte möglich, aber „Besetztfall“ (keine Ressourcen mehr übrig)
- **Statistische Klasse:**
  - vorgegebene Schranken müssen mit einer gewissen Wahrscheinlichkeit eingehalten werden
    z.B.: die Ende-zu-Ende-Verzögerung muss für 95% der Pakete unter 100ms liegen.
  - Ressourcen werden bis zu einem gewissen Grad überbelegt
  - Konflikte möglich (je höher die Wahrscheinlichkeit der Garantie, desto geringer sind Ressourcenkonflikte)
- **„Best Effort“-Klasse („so gut es geht“):**
  - es werden keinerlei Garantien für Dienstgüteparameter gemacht
  - keine explizite Ressourcenreservierung für einzelne Verbindungen

8. Anwendungen - Motivierende Fragen

- Welcher Netzmanagement-Standard wurde für das Internet entwickelt?
- In welcher Darstellung werden dabei Daten übermittelt?
- Wie funktioniert e-mail?
- Wie funktioniert das Web?
- Wie funktioniert die Abbildung von Namen auf Adressen im Internet?

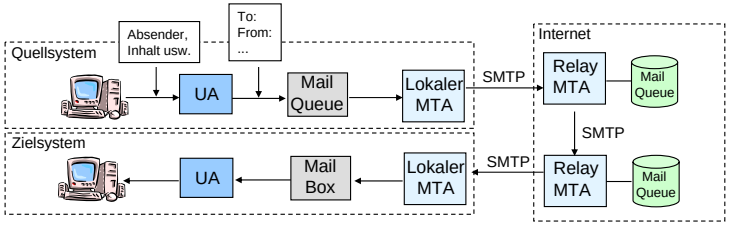
8. Anwendungen - Kapitelgliederung

Internet-Netzwerkmanagement

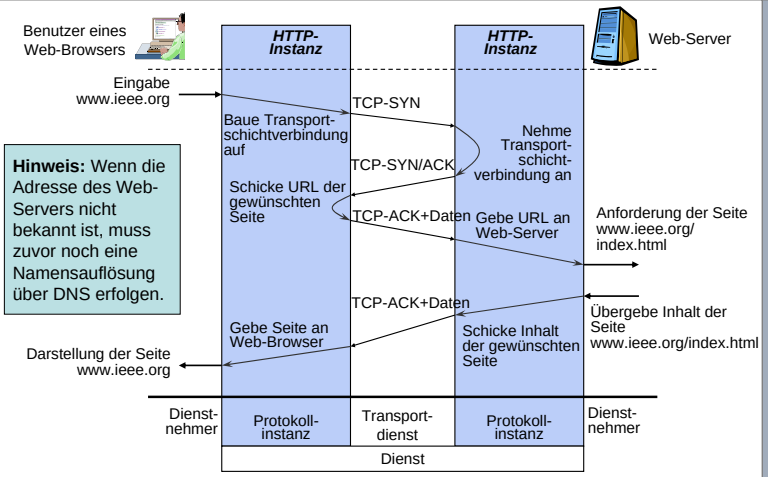


Internet Mail: Das SMTP-Modell

- SMTP dient der E-Mail-Übermittlung
  - zeichenorientiertes Protokoll, basierend auf 7-Bit-ASCII
  - nur wenige Kommandos, z.B. HELO, MAIL, RCPT, DATA, QUIT
- UA erhält alle notwendigen Angaben vom Benutzer
  - Mitteilung wird über Mail-Queue zum lokalen MTA übertragen
- MTAs übertragen die Mitteilung zum Zielrechner
  - Auslieferung einer E-Mail erfolgt über eine TCP-Verbindung (Port 25) zum Ziel-MTA (MTA unter UNIX: sendmail)
  - Relay-MTAs dienen als zentrale E-MAIL-Verteiler (z.B. Informatik-Institut)



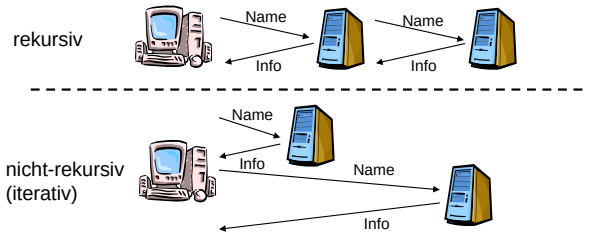
Beispiel: Surfen im Internet



Hinweis: Wenn die Adresse des Web-Servers nicht bekannt ist, muss zuvor noch eine Namensauflösung über DNS erfolgen.

DNS: Nameserver (NS)

- Jede Zone hat einen primären und beliebig viele sekundäre Nameserver
  - Jeder NS kennt nur einen Ausschnitt des gesamten Namensraums
  - Jeder NS kennt die IP-Adressen der NS seiner direkt untergeordneten Sub-Domains
  - Jeder NS führt Caching bereits bekannter Einträge durch
  - Sekundäre NS führen ein periodisches Update („Zonentransfer“) ihrer Datenbasis durch (basierend auf den Daten des primären NS)
- Anfragen können rekursiv oder nicht-rekursiv beantwortet werden:



9. Verteilte Systeme - Motivierende Fragen

- Welche Dienste soll eine Middleware bereitstellen?
- Wie lassen sich Anwendungen zwischen Server und Client verteilen?
- Wie funktioniert ein entfernter Prozeduraufruf?
- Was ist beim Aufruf entfernter Methoden zu beachten?
- Was versteht man unter SOA - Service Oriented Architectures?
- Was sind die Grundprinzipien von CORBA?
- Wie können Web-Anwendungen implementiert werden?
- Was sind die Unterschiede von HTML und XML?
- Was sind Web Services?
- Was versteht man unter SOAP, WSDL, SAX, UDDI?

Gliederung - Kapitel 9: Verteilte Systeme

Kapitel 9 - Teil 1

9.1 Grundlagen

9.2 Middleware

9.3 RPC

9.4 RMI

Kapitel 9 - Teil 2

9.5 Service Oriented Architectures

9.6 Corba

9.7 Web-Anwendungen

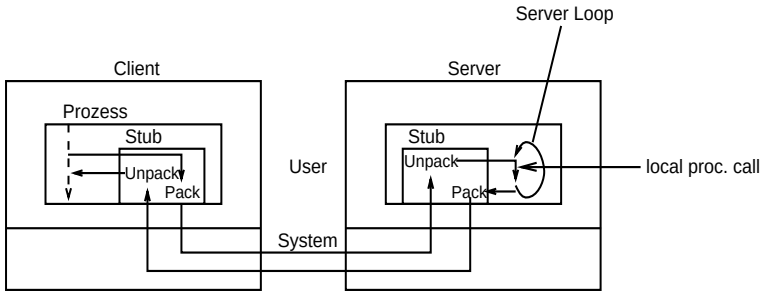
9.8 HTML und XML

9.9 Web Services

Ziele für Verteilte Systeme

- Benutzer und Ressourcen verbinden
  - Den Benutzern ermöglichen, auf entfernte Ressourcen zuzugreifen
  - Unterstützung für kontrollierte gemeinsame Benutzung
- Transparenz
  - Zugriff – verbirgt Unterschiede in der Datendarstellung
  - Position – verbirgt Ort der Ressource
  - Migration – verbirgt Möglichkeit, Ressource an anderen Ort zu verschieben
  - Relokation – verbirgt Verschiebung von Ressource während Nutzung
  - Replikation – verbirgt, dass eine Ressource repliziert ist
  - Nebenläufigkeit – verbirgt gleichzeitige Nutzung konkurrierender Benutzer
  - Fehler – verbirgt Ausfall und Wiederherstellung einer Ressource
  - Persistenz – verbirgt Speicherart (Hauptspeicher oder Festplatte)
- Offenheit
  - Vollständige Schnittstellenspezifikation (⇨ Schnittstellendefinitionssprache IDL – Interface Descrption Language)
- Skalierbarkeit

Schema des RPC

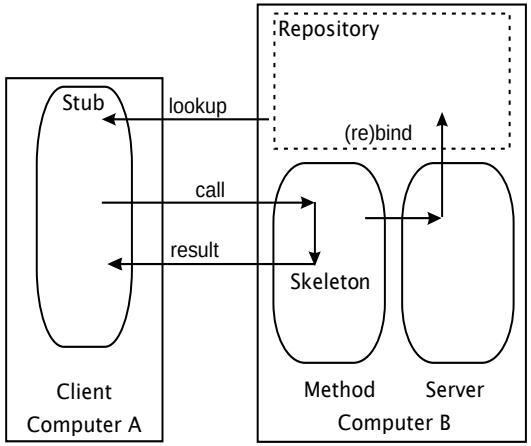


Fehlerbehandlung in RPC-Systemen

- Durch die Entkopplung zwischen Klient und Server kann es zu folgenden Fehlern kommen:

  1. Der Klient findet den Server nicht.
  2. Die Auftragsnachricht Klient/Server geht verloren.
  3. Die Antwortnachricht Server/Klient geht verloren.
  4. Der Server stürzt nach Auftragserhalt ab.
  5. Der Klient stürzt nach Auftragsvergabe ab.

RMI – Schema



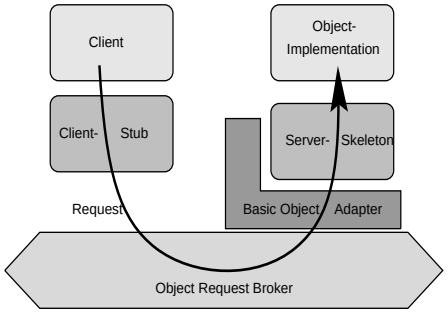
Inhalte von Kapitel 9, Teil 2

- Service-Orientierte Architekturen
- Corba
- Web-Technologien
  - Java Server Pages
  - Java Servlets
- Sprache XML
  - XML Tags
  - Name Spaces
  - XML-Schemata
  - Validierung von XML-Dokumenten
  - Werkzeugunterstützung für XML
  - Transformation in andere XML-Formate, oder andere Sprachen
- Web Services
  - Schichtenarchitektur
  - SOAP-Mechanismus zur Repräsentation/zum Austausch von Daten
  - Web Services Description Language WSDL
  - Universal Description and Integration UDDI

9.5 Definition Service Oriented Architectures

- SOA ist ein Paradigma für die Strukturierung und Nutzung verteilter Funktionalität, die von unterschiedlichen Besitzern verantwortet wird.
  [Organization for the Advancement of Structured Information Standards (OASIS) , 2006] c.f. oasis-open.org
- Dienste in einer Service-Orientierten Architektur haben (idealerweise) folgende Eigenschaften
  - Dienst ist in sich abgeschlossen und kann eigenständig genutzt werden.
  - Dienst ist über ein Netzwerk verfügbar.
  - Dienst hat eine veröffentlichte Schnittstelle. Für die Nutzung reicht es, die Schnittstelle zu kennen. Kenntnisse über die Details der Implementierung sind hingegen nicht erforderlich.
  - Dienst ist plattformunabhängig, d.h. Anbieter und Nutzer eines Dienstes können in unterschiedlichen Programmiersprachen auf verschiedenen Plattformen realisiert sein.
  - Dienst ist in einem Verzeichnis registriert.
  - Dienst ist dynamisch gebunden, d.h. bei der Erstellung einer Anwendung, die einen Dienst nutzt, muss der Dienst nicht vorhanden sein. Er wird erst bei der Ausführung lokalisiert und eingebunden.

Grundprinzip von CORBA



- Mit Hilfe der IDL wird ein Interface definiert.
- IDL-Compiler erzeugt aus dieser Schnittstellenbeschreibung Sourcecode in der gewünschten Sprache. Für den Client **Stub** und für den Server **Skeleton**.
- Server wird implementiert und ist über das Skeleton für andere Objekte zugänglich. Über den *Basic Object Adapter* (**BOA**) meldet sich der Server beim ORB an und ist jetzt bereit, Aufrufe anderer Objekte zu empfangen.
- Der Client kann nun über den Stub auf den Server zugreifen. Dieser Zugriff läuft über den ORB.

9.9 Definition von Web Services

A Web service is a software system designed to support interoperable machine-to-machine interaction over a network.

*It has an interface described in a machine-processable format (specifically **WSDL**).*

*Other systems interact with the Web service in a manner prescribed by its description using **SOAP** messages, typically conveyed using HTTP with an **XML** serialization in conjunction with other Web-related standards.*

David Booth et al.: *Web Service Architecture*
W3C Working Group Note 11 February 2004
http://www.w3.org/TR/ws-arch/

Web Services

- Web Services
  - basieren auf offenen Protokollen bzw. Spezifikationen
  - Heterogene Plattformen (J2EE, .Net etc.) werden unterstützt
  - Spezifikation über XML-Grammatiken
    - Universelle Beschreibungssprache
    - Selbst-dokumentierend
    - Robust gegen Änderungen: Empfänger überliest irrelevante Einträge
  - Beschreibung der Schnittstelle: WSDL (Web Service Description Language)
    - Interface Beschreibung von Diensten (analog CORBA IDL)
  - Kommunikation: SOAP (Simple Object Access Protocol)
    - Kommunikation zwischen Diensten („XML-RPC“)
    - Transportiert XML-serialisierte Werte und Methoden-Aufrufe
  - Finden von Diensten: UDDI (Universal Description Discovery and Integration)
    - Suchen von Diensten
    - Weltweiter Verzeichnisdienst für Web Services

10. Netzsicherheit - Motivierende Fragen

- Welche Kommunikation ist abhörbar?
- Wie kann man sich davon überzeugen, dass ein Kommunikationspartner der ist, der er vorgibt zu sein?
- Wie kann man sicherstellen, dass eine Nachricht vom angegebenen Sender stammt?
- Wie kann man sicherstellen, dass eine Nachricht seit dem Versenden nicht modifiziert wurde?
- Was ist ein Zertifikat? Und wie wird es eingesetzt?

10. Netzsicherheit - Kapitelaufbau

- Sicherheitsziele und Bedrohungen
- Sicherheitsmechanismen
- Firewalls
- Virtuelle Private Netze

Sicherheitsdienste

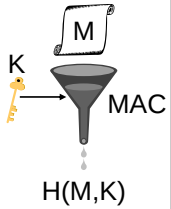
- Authentisierung
  - Authentisierung der Kommunikationspartner (Entity Authentication)
  - Authentisierung des Datenursprungs (Data Origin Authentication)
- Zugriffskontrolle
  - Schutz einer Ressource vor unberechtigtem Zugriff
- Abhörsicherheit
  - kein Fremder soll Daten mitlesen können
- Verbindlichkeit bzw. Nicht-Zurückweisbarkeit (Non-Repudiation)
  - Sender bzw. Empfangen kann nachgewiesen werden
- Datenintegrität (Fälschungssicherheit)
  - Echtheit der Daten soll garantiert sein

- Verfügbarkeit
  - Schutz eines Dienstes vor Blockierung
- Privatheit
  - Anonymisierung bzw. Pseudonymisierung ist möglich
- Autorisierung
  - darf jemand mit der vorgegebenen Kennung einen Dienst nutzen?
- Vertraulichkeit
  - Schutz der Daten vor unberechtigter Offenlegung

Authentisierung (1)

- **Kryptographische Hash-Funktion**
  (Modification Detection Code bzw. Message Digest Code, MDC):
  - Nachricht M (beliebig lang) → Hash-Wert H(M)
  - Wichtig: „Einweg"-Eigenschaft:
    keine Kollisionen effizient erzeugbar
    Kollision: M, M' mit H(M)=H(M')
  - Beispiele: MD5, SHA-1, RIPEMD-160

- **Schlüsselabhängige Hash-Funktion**
  (Message Authentication Code, MAC):
  - Nachricht M, Schlüssel K → Hash-Wert H(M,K)
  - kann aus MDC konstruiert werden:
    HMAC (RFC 2104), z.B. HMAC-MD5
    $H(K \text{ xor } pad_1, H(K \text{ xor } pad_2, M))$



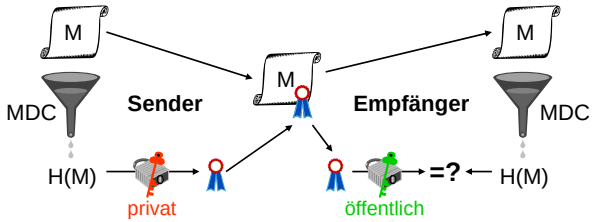
Verschlüsselung (asymmetrisch)

- Asymmetrische (Public-Key-) Verschlüsselungsalgorithmen
  - minimale derzeit sichere Schlüssellänge: 1024 bit
  - als sicher geltender Algorithmus: RSA
  - relativ langsam

- In der Praxis: Hybride Systeme
  - Zunächst: Benutzer-Authentisierung und Austausch eines Sitzungsschlüssels (symmetrisch oder Public-Key)
  - Danach: Authentisierung/Verschlüsselung der Nutzdaten mit Sitzungsschlüssel (symmetrisch)
  - Bei langen Sitzungen sollte Sitzungsschlüssel gelegentlich ausgewechselt werden (z.B. stündlich)

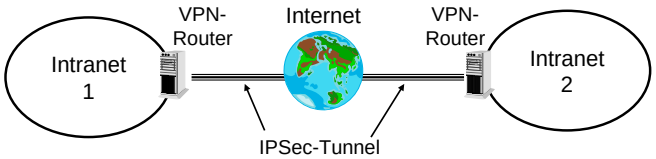
Authentisierung (2)

- **Digitale Signatur**
  - Hash-Wert H(M) wird mit privatem Schlüssel signiert
  - Empfänger überprüft Signatur mit öffentlichem Schlüssel
  - kann auch Verbindlichkeit garantieren
  - wichtigste Algorithmen: RSA, DSA, ElGamal
  - min. Schlüssellänge: 1024 bit
    (160 bit bei DSA-Variante mit elliptischen Kurven)



IP Security (IPSec)

- Aufgabe: sicheres Tunneln von IP-Paketen
  - Verschlüsselung am Tunneleingang, Entschlüsselung am Ausgang
  - kann z.B. für das gesamte VPN automatisch durchgeführt werden oder nur für bestimmte Anwendungen
- Beispiel: IP Security
  - Funktionsweise:
    - MAC und/oder symm. Verschlüsselung
    - 2 Paketformate: AH (RFC 2402), ESP (RFC 2406)
  - Produkte:
    - FreeS/WAN (www.freeswan.org)
    - Cisco VPN-Produkte
    - Windows VPN-Funktionen



IPSec: Authentication Header und Encapsulaing Security Payload

- Authentication Header

  Authentifizierung, Datenintegrität durch MAC
  - Transportmodus
    - Keine Veränderung der Adressen, falls direkte Kommunikation
  - Tunnelmodus
    - Neue IP-Adressen, zwischen beliebigen Partnern

Transportmodus

Tunnelmodus

- Encapsulating Security Payload
  - Authentifizierung, Datenintegrität, Privatheit durch Verschlüsselung und/oder MAC
  - Transportmodus
  - Tunnelmodus

Transportmodus

Tunnelmodus

Übersicht

1. Einführung und Motivation
   - Bedeutung, Beispiele
2. Begriffswelt und Standards
   - Dienst, Protokoll, Standardisierung
3. Direktverbindungsnetze
   - Fehlererkennung, Protokolle
   - Ethernet
4. Vermittlung
   - Vermittlungsprinzipien
   - Wegwahlverfahren
5. Internet-Protokolle
   - IP, ARP, DHCP, ICMP
   - Routing-Protokolle
6. Transportprotokolle
   - UDP, TCP
7. Verkehrssteuerung
   - Kriterien, Mechanismen
   - Verkehrssteuerung im Internet
8. Anwendungsorientierte Protokolle und Mechanismen
   - Netzmanagement
   - DNS, SMTP, HTTP
9. Verteilte Systeme
   - Middleware
   - RPC, RMI
   - Web Services
10. Netzsicherheit
    - Kryptographische Mechanismen und Dienste
    - Protokolle mit sicheren Diensten: IPSec etc.
    - Firewalls, Intrusion Detection
11. Nachrichtentechnik
    - Daten, Signal, Medien, Physik
12. Bitübertragungsschicht
    - Codierung
    - Modems