Arbeiten am Lehrstuhl Fliege

Absicherung der Datenübertragung ‚zwischen' Kanalcodierung und Kryptographie

Markus Grimm, Sommerschule 2003

UNIVERSITÄT MANNHEIM

Lehrstuhl für Elektrotechnik
Prof. Dr.-Ing. Dr. h.c. N. Fliege

Übersicht

- Einführung: Schichtenmodelle
- Zugriffsverfahren
- Datensicherungsverfahren
- Datenflusssteuerung
- Wegelenkung (Routing)
- Transportfunktionen
- Anwendung: Ethernet und TCP/IP
- Forschung: Protokollkonverter IPx-10

Einführung: Schichtenmodelle

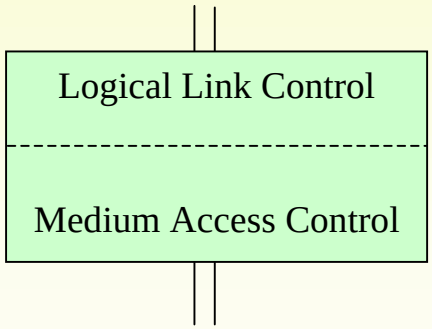
- ISO-OSI-Schichtenmodell („Theorie“)
  - Von der ISO 1978 in Genf vorgeschlagen
  - Ziel: Vereinheitlichung von Schnittstellen, Kompatibilität der Produkte verschiedener Hersteller
  - OSI = Open System Interconnection
  - ISO = International Standardisation Organisation
- Internet- (TCP/IP-) Schichtenmodell („Praxis“)
  - Älter als das OSI-Schichtenmodell
  - Protokolle werden laufend weiterentwickelt:
    - *Internet Engineering Task Force* (IETF), *Request for Comments* (RFC)

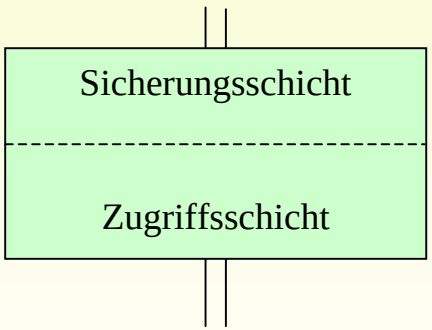
ISO-OSI-Schichtenmodell

7	Application Layer	FTP, HTTP, SMTP, POP3, NFS, SNMP, NTP, ...	Anwendungsschicht
6	Presentation Layer	ASN.1, SSL	Präsentationsschicht
5	Session Layer		Sitzungsschicht
4	Transport Layer	TCP, UDP	Transportschicht
3	Network Layer	IP	Netzschicht
2	Datalink Layer	Ethernet, HDLC, PPP	Verbindungsschicht
1	Physical Layer	CU, LWL	Physikal. Schicht

Unterteilung der Schicht 2

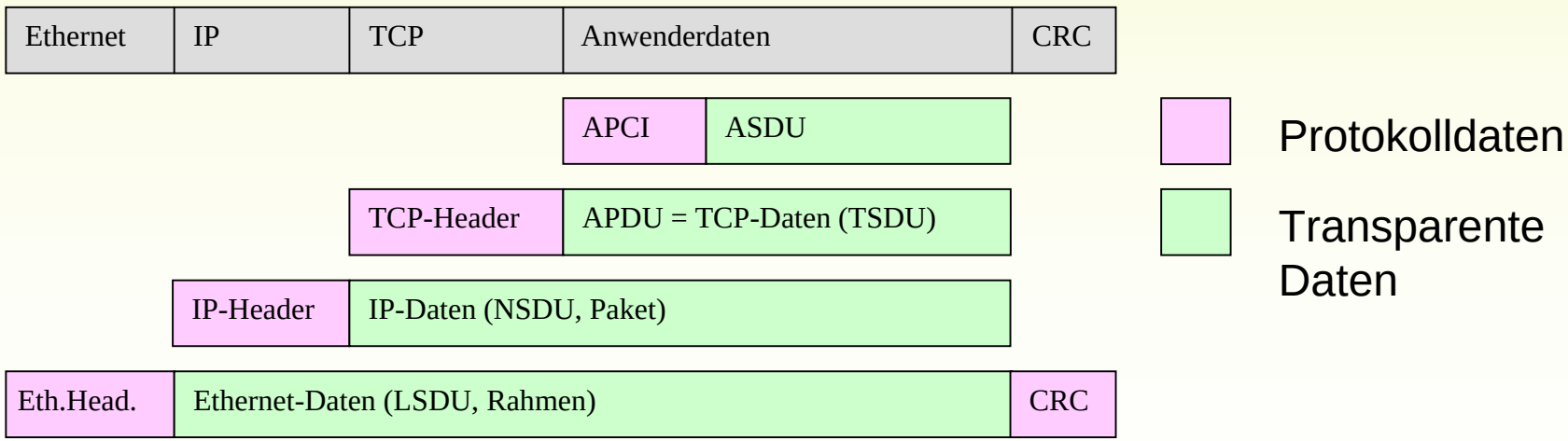
- *Data Link Control* (DLC) enthält ‚zuviel' Funktionalität, daher Unterteilung in untere und obere Teilschicht:





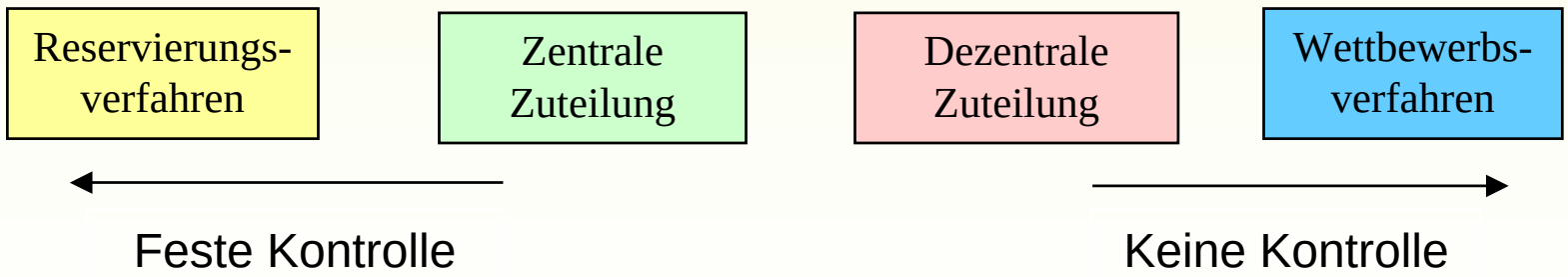
Kommunikation in Schichten

- SDU = *Service Data Unit*
  - Dienstdateneinheit (die eigentlichen Daten)
- PCI = *Protocol Control Information*
  - Protokollsteuerinformation (*Header*)
- SDU + PCI = PDU = *Protocol Data Unit*
  - Protokolldateneinheit



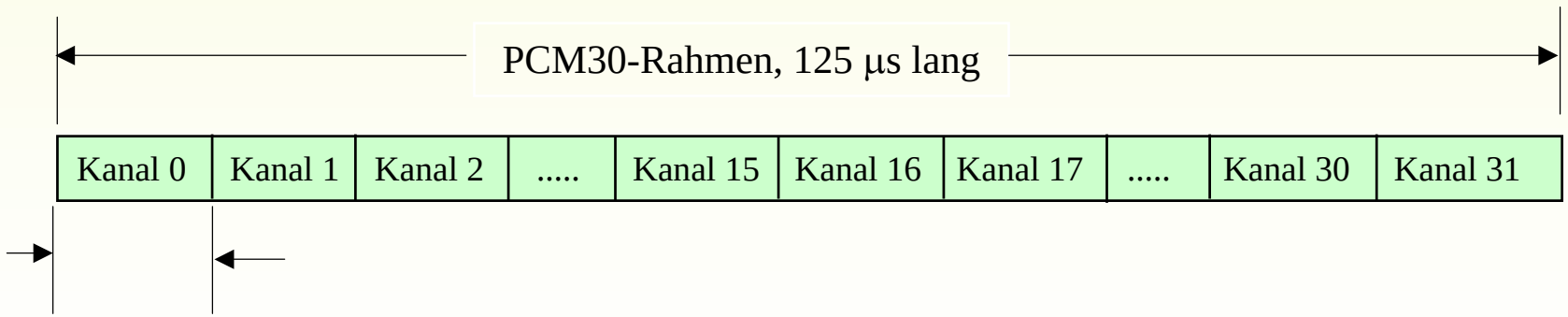
Zugriffsverfahren

- Problem: Zugriff eines Teilnehmers auf ein Übertragungsmedium
  - Zugriff = Sendezugriff
- Wichtig: Art der Zusammenschaltung verschiedener Teilnehmer = *Netz-Topologie*
- Ordnung der Verfahren nach Kontrolle der Teilnehmer über das Medium:



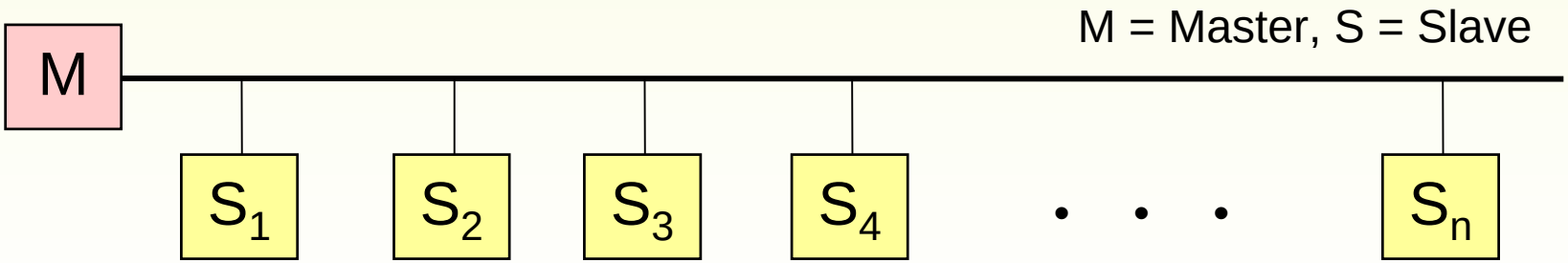
Reservierungsverfahren

- *Fixed Assignment Techniques*
- Durch Konfiguration festgelegte Zuordnung Teilnehmer ⇔ Übertragungskanal
- Multiplextechnik (Mehrfachnutzung von Übertagungsmedien)
- Beispiele: FDMA (Rundfunk), TDMA (PCM30)



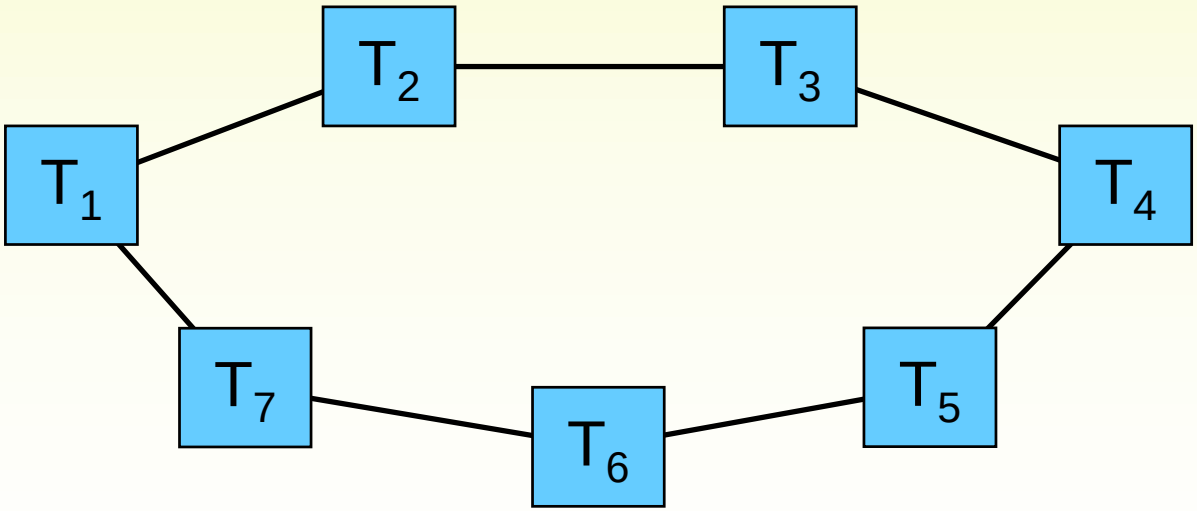
Zentrale Zuteilung

- *Demand Assignment With Centralized Control*
- Die Leitung wird den Teilnehmern von Zeit zu Zeit von einer Zentrale befristet zugewiesen
- In der Regel Bus-Topologie mit Master-Slave-Betrieb
- Beispiel: Aufrufbetrieb (Polling)



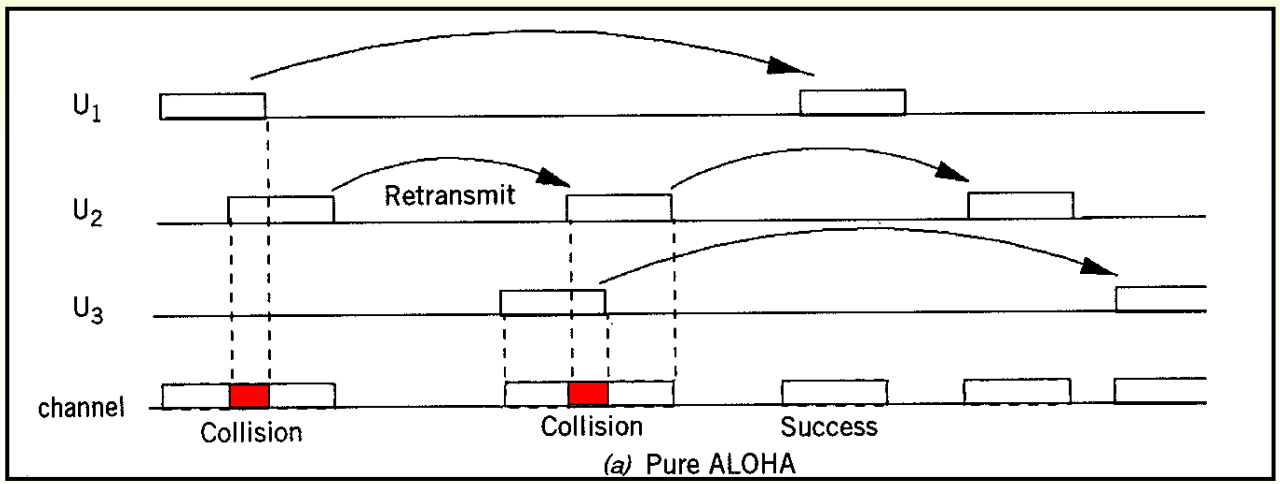
Dezentrale Zuteilung

- *Demand Assignment With Distributed Control*
- Alle Teilnehmer sind gleichberechtigt
- Zugriff auf die Leitung nach bestimmten Regeln
- Beispiel: Token-Passing in einer Ring-Topologie



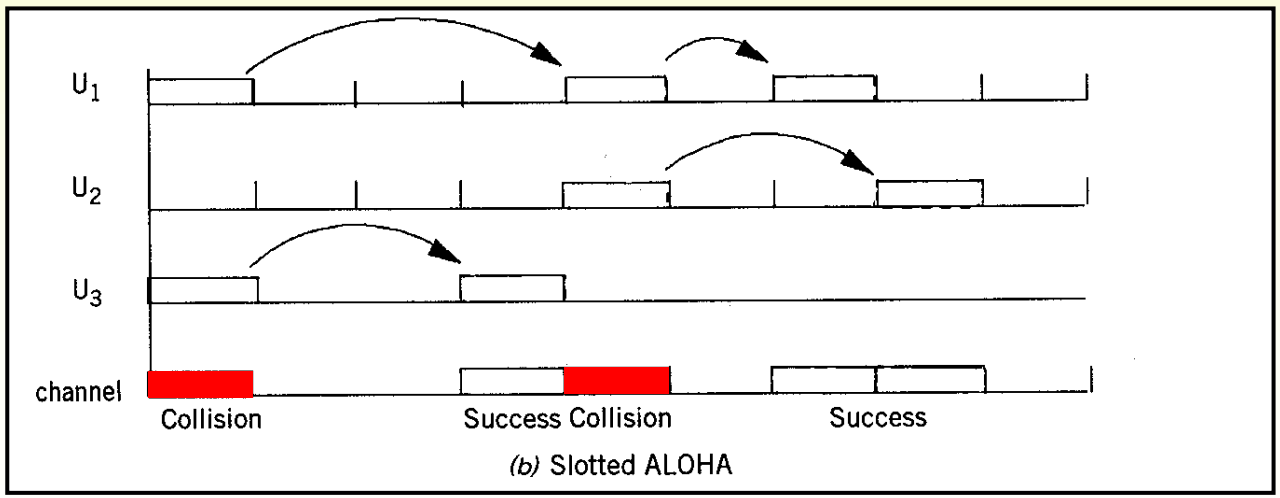
Wettbewerbsverfahren

- *Random Access*
- Weder Zentrale noch Zugriffsregeln, daher sind Kollisionen typisch
- Beispiele: ALOHA, CSMA/CD (Ethernet)



Wettbewerbsverfahren

- *Random Access*
- Weder Zentrale noch Zugriffsregeln, daher sind Kollisionen typisch
- Beispiele: ALOHA, CSMA/CD (Ethernet)



Datensicherungsverfahren

- Rahmenerkennung und -synchronisation
- Transparenz
  - alle Zeichen erlaubt?
- Initialisierungskontrolle
  - beide Seiten bereit?
- Fehlerkontrolle
  - Erkennung und Korrektur
- Überwachung anormaler Zustände
  - *Time-Out*

Rahmensynchronisation

- RS232: Start-Stop-Telegramme
  - Kann zu Fehlsynchronisationen führen
- Ethernet: Synchronisations-Präambel und Lücke
  - Lücke (Sendepause) = spezielles Zeichen im Sende-Alphabet
- HDLC: Rahmenflag (01111110) und Bit-Stopfen

Sender: `...011111X..` → `...0111110X..`

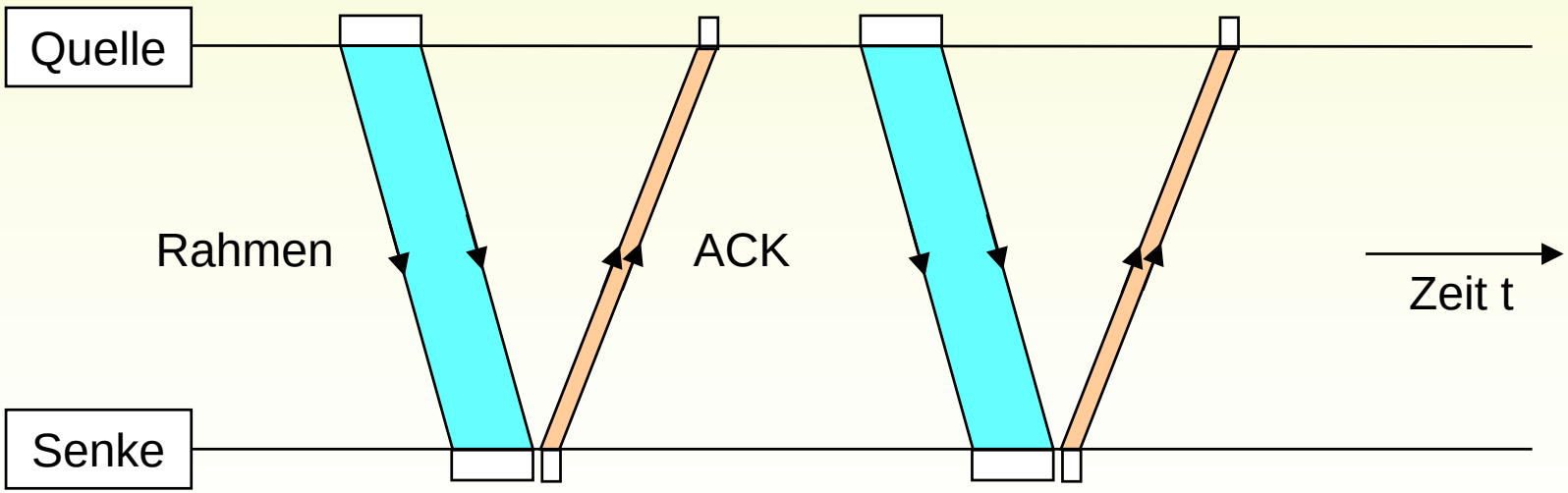
Empfänger: `...0111110X..` → `...011111X..`

Vorwärtsfehlerkorrektur

- *Forward Error Correction* (FEC)
- **Kanalcodierung:** Erkennung von Bitfehlern
  - Methoden: Paritätsbits, Prüfsummen, Blockcodes (z. B. CRC, Reed-Solomon)
- In Fällen ohne Rückkanal muss FEC angewendet werden
- FEC ist meist schwierig und aufwändig
- Fehler, die nicht mit FEC korrigierbar sind:
  - Fehlende Telegramme
  - Wiederholte Telegramme oder
  - Falsche Reihenfolge der Telegramme

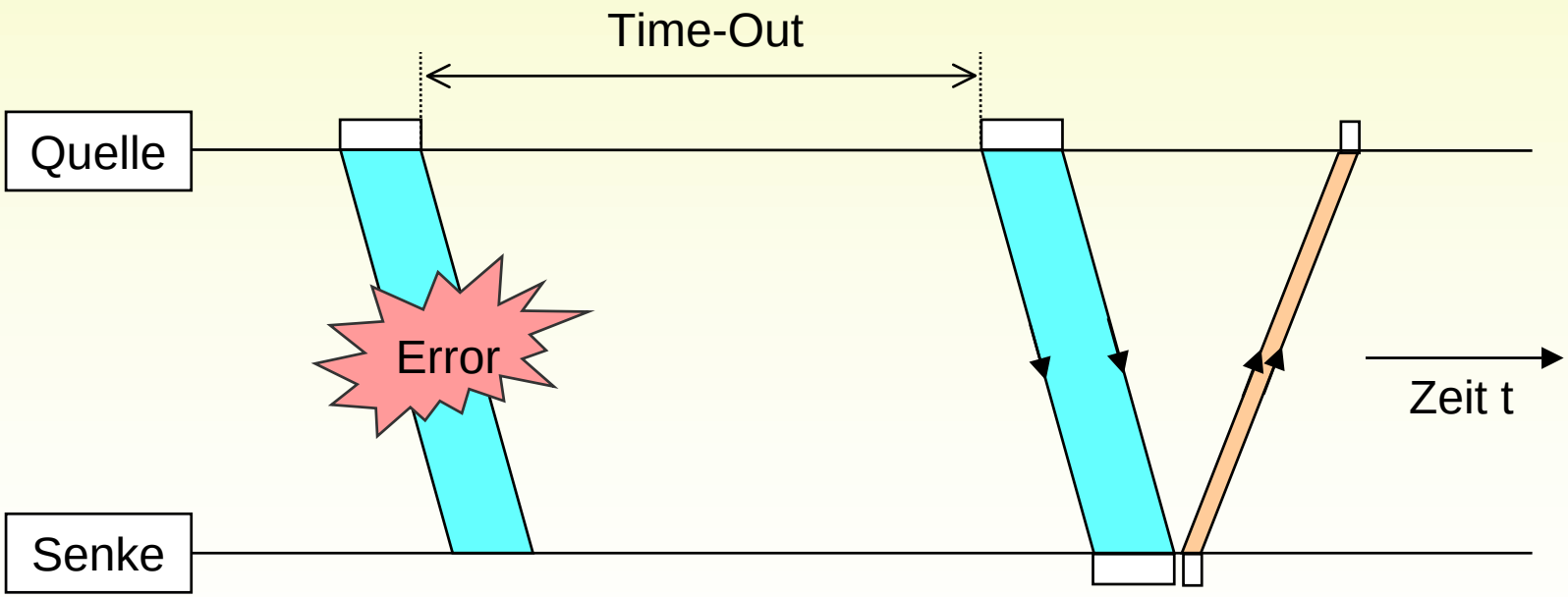
Automatische Wiederholungsanforderung

- *Automatic Repeat Request* (ARQ)
- Wird bei bidirektionalen Verbindungen bevorzugt
- Stop-And-Wait-ARQ:



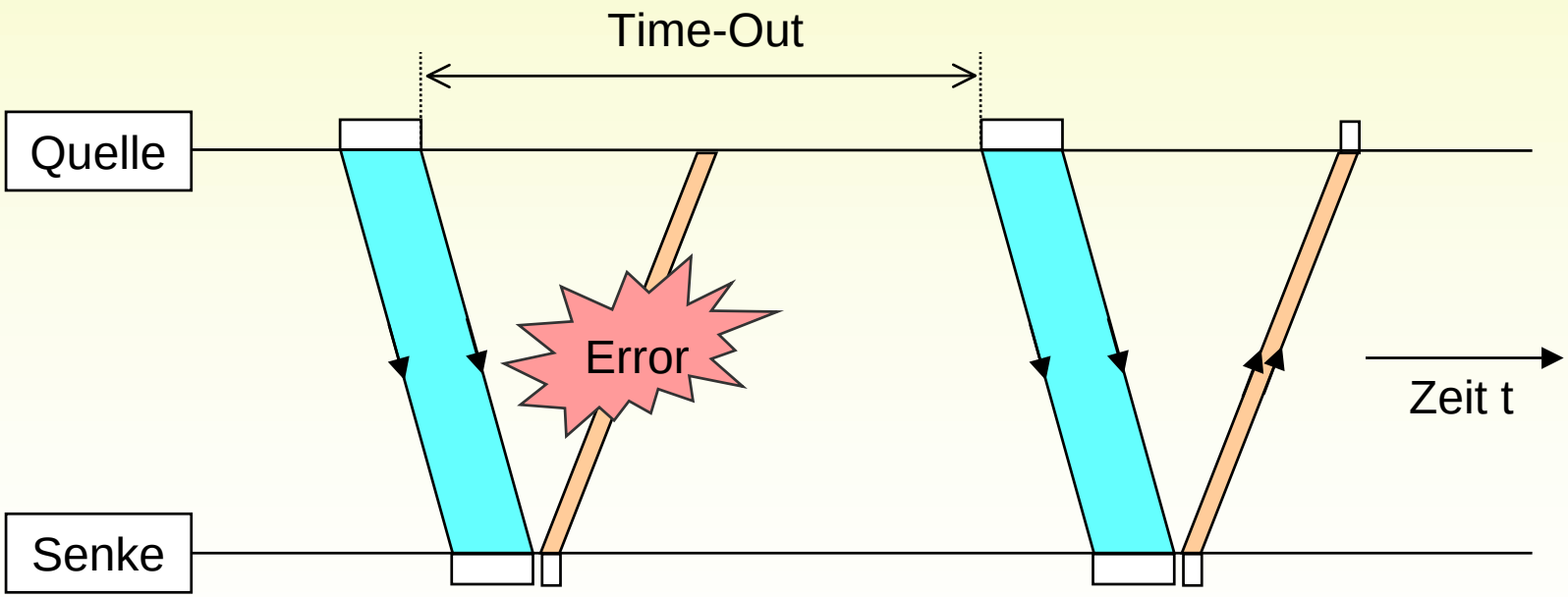
Automatische Wiederholungsanforderung

- Stop-And-Wait-ARQ: Fehler im Telegramm



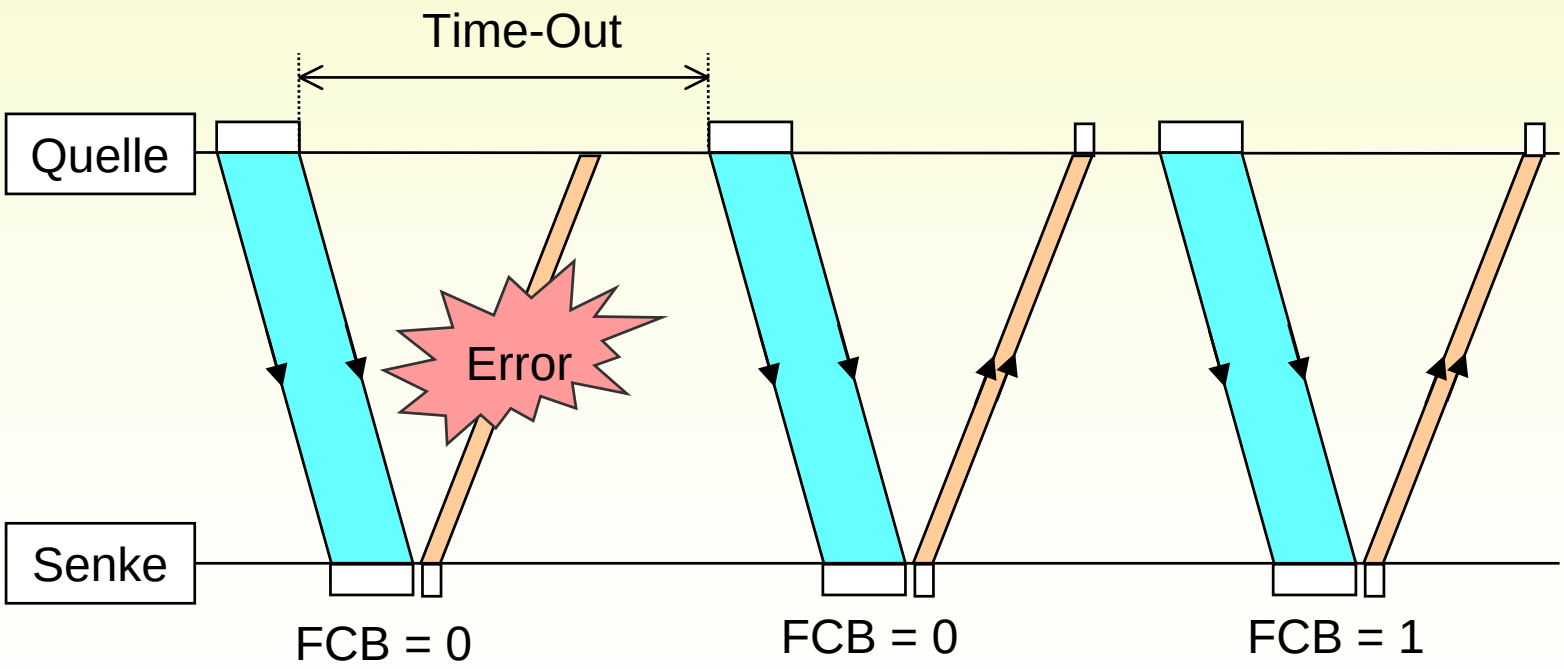
Automatische Wiederholungsanforderung

- Stop-And-Wait-ARQ: Fehler in der Quittung

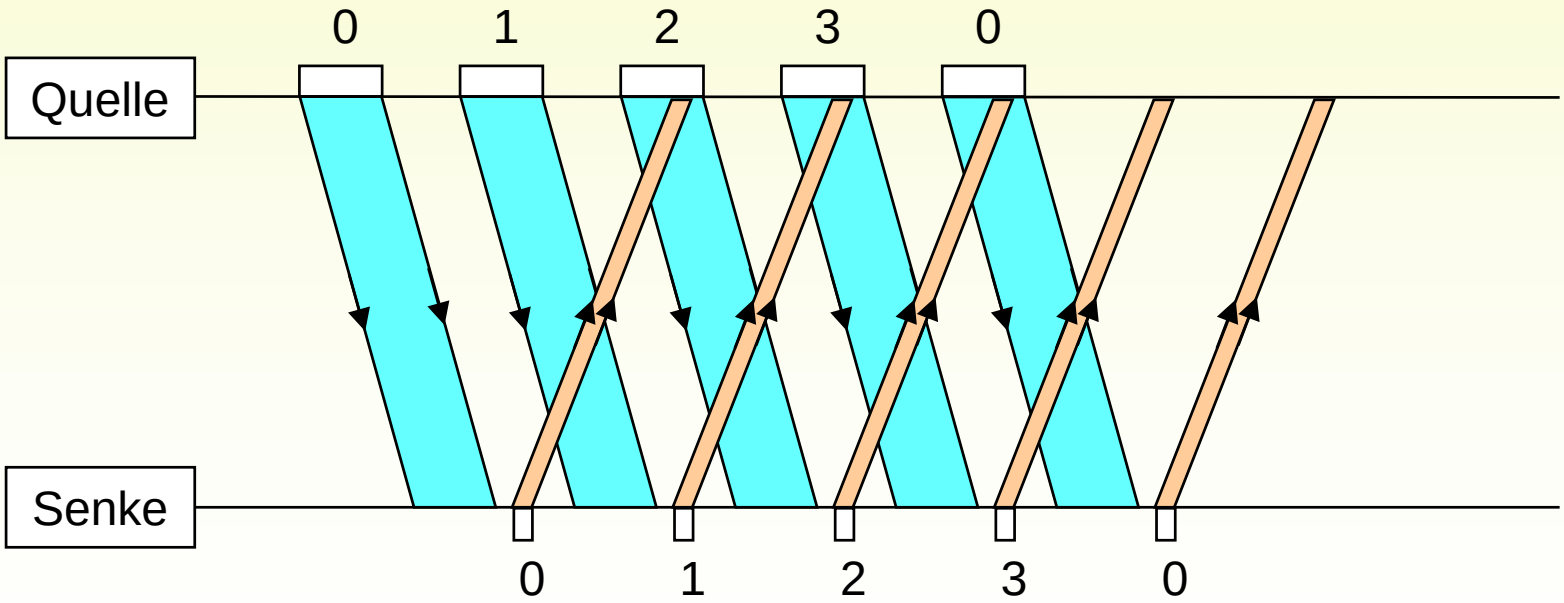


Automatische Wiederholungsanforderung

- Stop-And-Wait-ARQ: Sequenznummern
  - FCB = *Frame Count Bit*

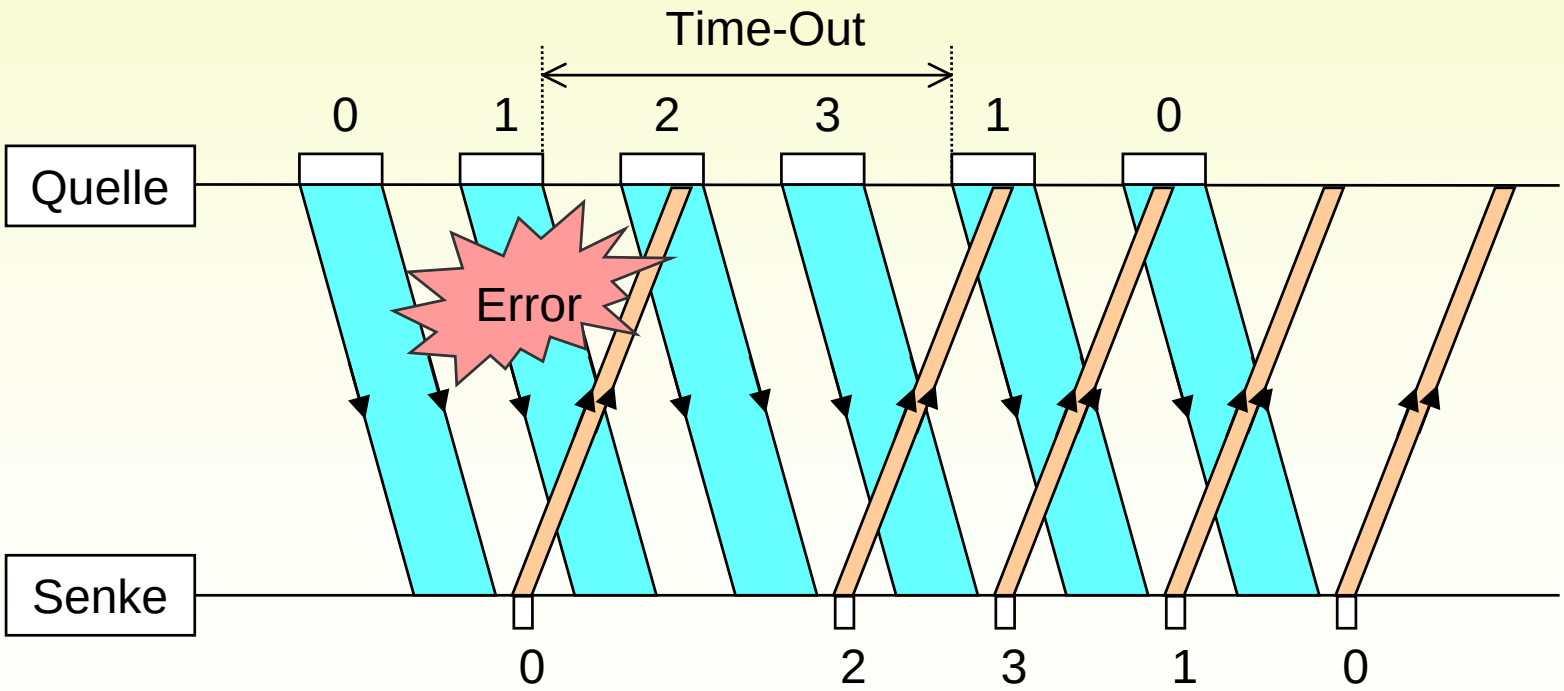


Kontinuierliches ARQ



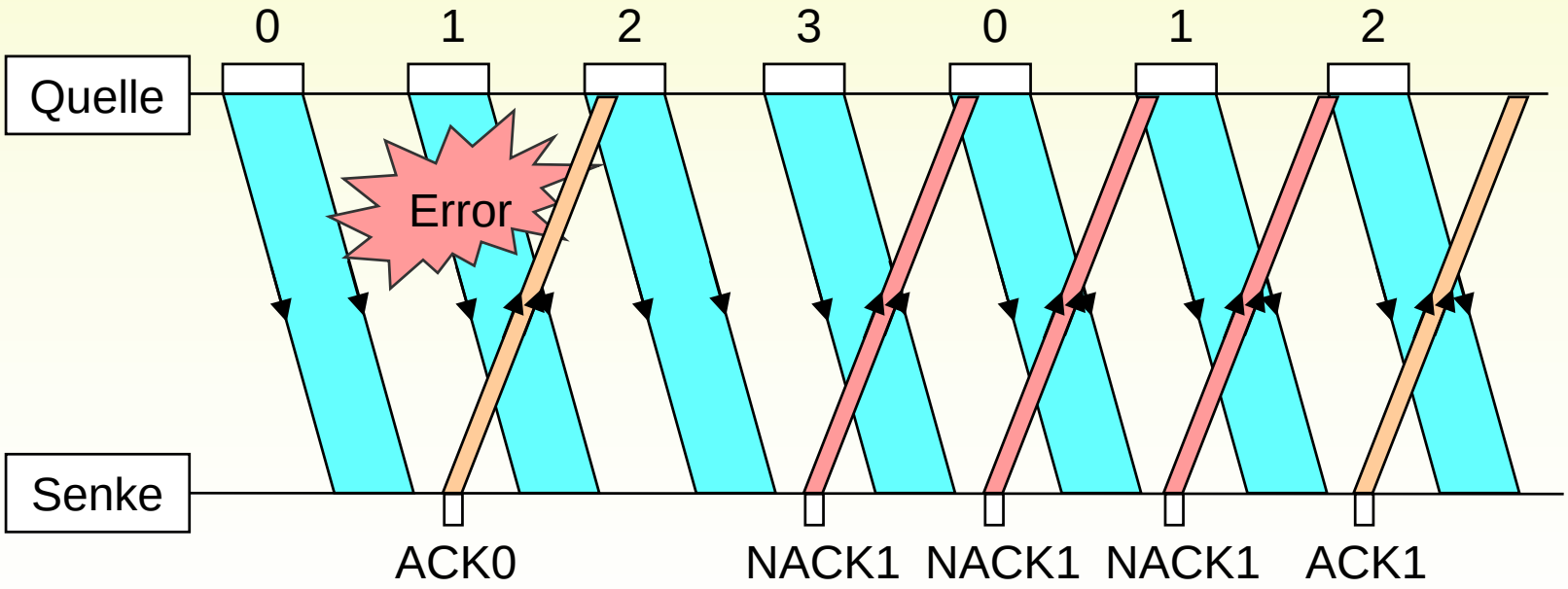
Kontinuierliches ARQ

- Select-Reject-Fehlerbehandlung



Kontinuierliches ARQ

- Select-Reject-Fehlerbehandlung
- Go-Back-N-Fehlerbehandlung



Datenflusssteuerung

- Flusssteuerung = Flusskontrolle (*Flow Control*)
  - End-zu-End-Datenverkehr von der Datenquelle zur Datensenke (Transportschicht)
  - Knoten-zu-Knoten-Datenverkehr (*Hop-To-Hop*, Linkschicht)
- Fenstertechnik
  - Bestätigung bei Weitergabe
  - Bestätigung bei Eintreffen
  - Getrenntes ACK und CREDIT

Wegelenkung (I)

- Vermittlungstechniken:
  - Leitungsvermittlung (*Circuit Switching*)
  - Virtuelle Leitung (*Connection-Oriented Service*)
  - Datagramme (*Connectionless Service*)
- Kriterien für die Qualität der Wegelenkung
  - Datensicherheit:
    - Fehlerwahrscheinlichkeit
    - Verlorengegangene Pakete
    - Kopierte Pakete
  - Durchlaufzeit
    - Übertragungszeit (Anzahl der Bits x Übertragungsrate)
    - Wartezeiten im Netzknoten (Warteschlangen)
    - Verarbeitungszeit in der CPU

Wegelenkung (II)

- Klassifizierung der Wegelenkungsverfahren
  - Tabellengestützt / nicht tabellengestützt
  - Statisch / dynamisch
  - Zentral / dezentral
- Zentrale statische Wegelenkung (*static routing*)
  - Bellman'sches Optimalitätsprinzip
  - Dijkstra-Algorithmus (*Shortest Path Routing*)
- Dezentrale dynamische Wegelenkung (*adaptive routing*)
  - Distanz-Vektor-Algorithmus (Bellman-Ford-Algorithmus)
    - RIP (*Routing Information Protocol*)
  - Link-State-Exchange-Algorithmus
    - OSPF (*Open Shortest Path First*)

Internet-Protokoll (IP)

- Verbindungsloser Dienst (Datagramm-Dienst)
- Verschiedene Protokolle auf Verbindungsebene
  - Ethernet, PPP, Token Ring
  - ARP-Protokoll zur Kommunikation mit Linkschicht
- Fragmentierung und Wiederzusammensetzung
  - ID, More-Flag, Offset
- IP garantiert keine zuverlässige Ablieferung der Pakete beim Empfänger
- Begrenzung der Lebensdauer
  - TTL (*Time To Live*)

Transportfunktionen

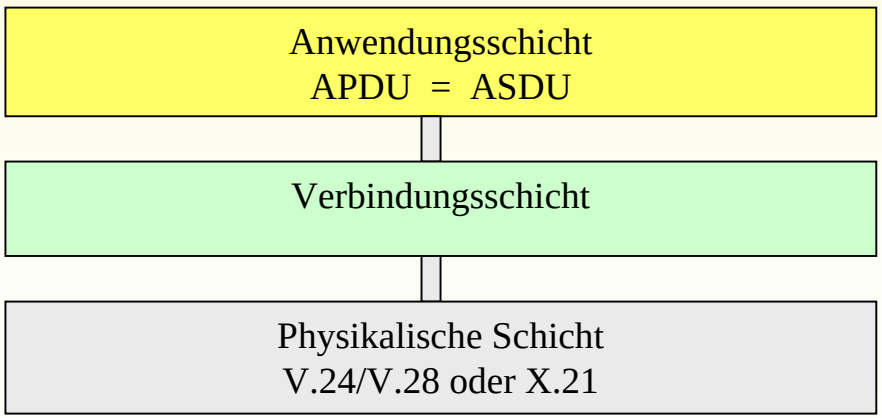
- Datensicherung
  - Dienstqualität (*Quality of Service, QoS*)
  - Fehlgeleitete, fehlende oder gedoppelte Pakete, Reihenfolge der Pakete
  - Flusskontrolle
- Verbindungsorientierung
- Multitasking
  - Mehrere Verbindungen von einem Client zum selben Server

Transport Control Protocol (TCP)

- Datenflusssteuerung:
  - Push- und Urgent-Funktionen
  - 32 Bit breite Sequenznummern (SSN, ASN)
  - variable Fensterbreite (*Sliding Window*)
- Verbindungsorientiert
  - Client-Server-Modell
  - Verbindungsaufbau mit 3-Schritte-Handshake
- Byte-orientiert
  - Paketgrenzen beim Absenden müssen nicht eingehalten werden

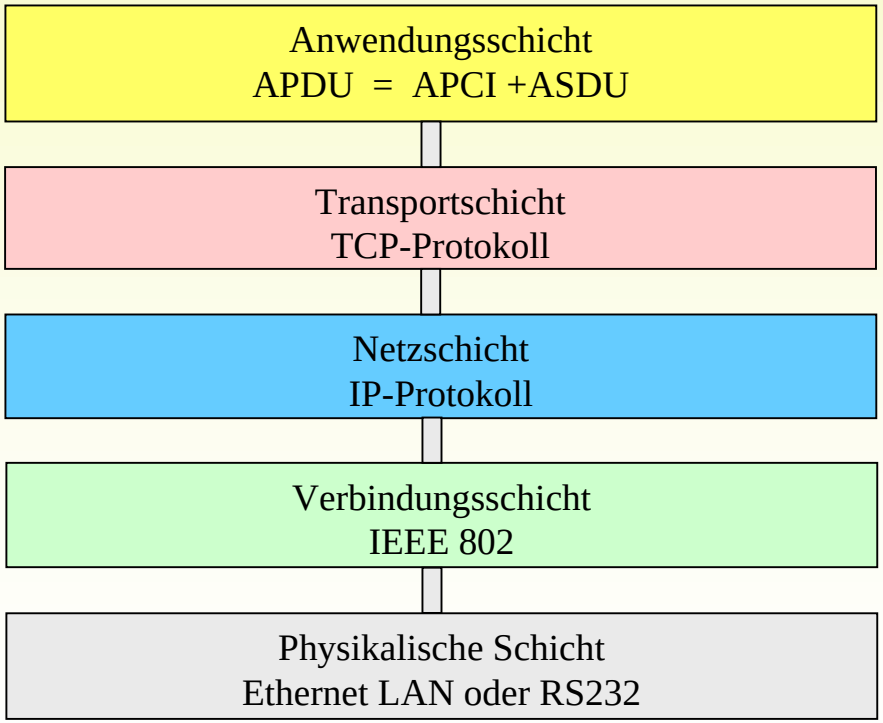
Fernwirkprotokoll IEC 60870-5-101

- Kommunikation von Fernwirk-Unterstationen mit einer oder mehrere Zentralen
  - Strom- oder Gaszähler
- Konzipiert für Bus- oder Sterntopologie über serielle Schnittstelle oder X.21



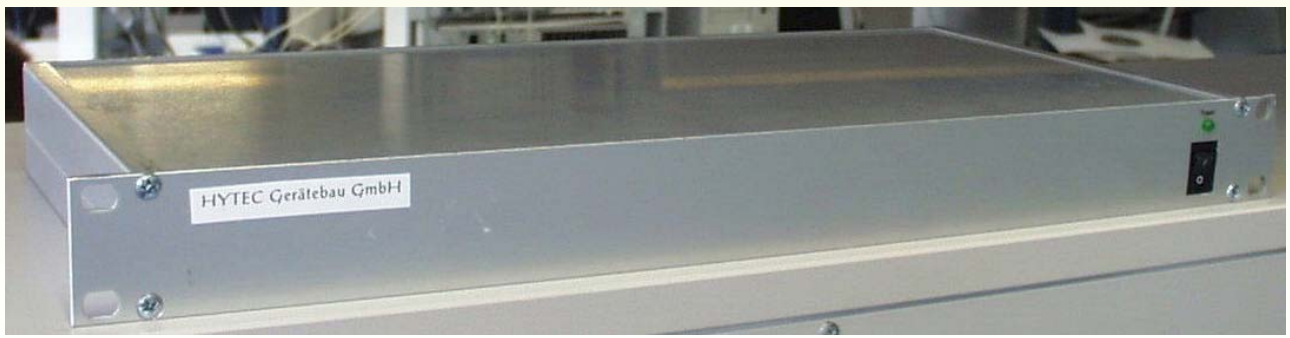
Fernwirkprotokoll IEC 60870-5-104

- Komplexere Anforderungen an Fernwirknetze
- Einsatz von Methoden der Internet-Technik in der Fernwirkkommunikation



Protokollkonverter IPS-10

- Ursprünglich dazu gedacht, um Daten von IEC-101 über TCP/IP zu übertragen
- Ermöglicht langsame Umstellung von IEC-101 auf IEC-104 bzw. TCP/IP-Netz
- Beinhaltet Routing-Funktionalität (OSPF) und wird um Prioritäten-Management erweitert
  - Nutzung des Fernwirknetzes für andere Dienste

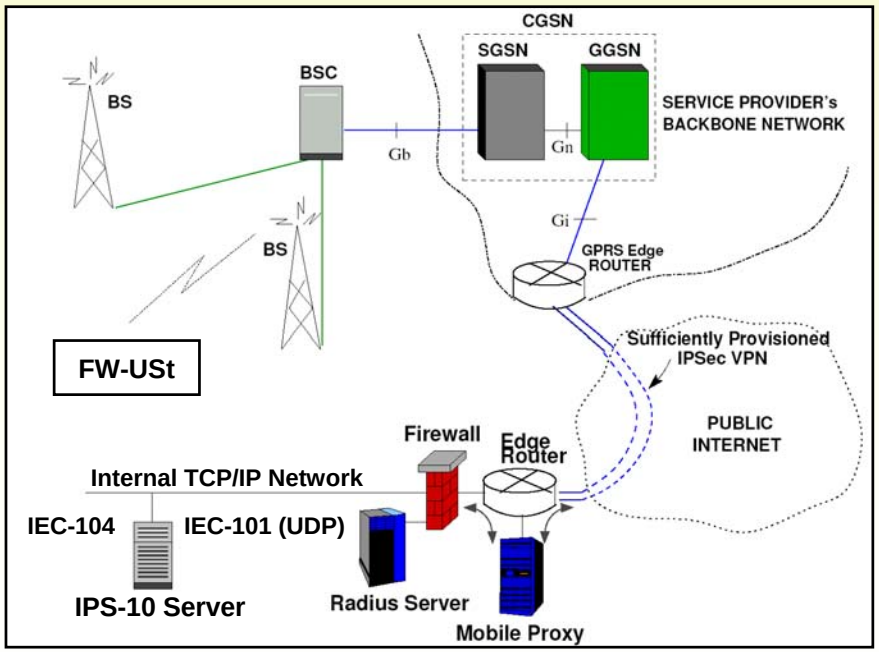


Prozeßdaten-Gateway IPG-10

- Beide Protokolle lassen Freiheiten
  - Größe des Adressfeldes und diverser anderer Felder im Header
  - Vergabe der Adressen an Stationen
- Umsetzung von Parametern und Adressen bei Fusion von Netzen oder Durchleitung von Daten durch ein Fremdnetz
  - Energieversorger

Fernwirkdaten über GPRS und UDP

- Modularer Aufbau des Codes: Datenfluß von Schnittstelle ⇔ Protokoll ⇔ Protokoll ⇔ Schnittstelle
  - Schnittstellen: RS232, UDP, TCP, Abtastung
  - Protokolle: IEC-101, IEC-104, Rohdaten



Innenleben

- Single-Board-PC: Geode-Prozessor (300 MHz)
- Keine mechanischen Teile
  - Passive Kühlung
  - Flash-Speicherkarte statt Festplatte
- Speziell optimiertes *Linux From Scratch* (12 MB)

Literaturverzeichnis

- Larry L. Peterson, Bruce S. Davie
  Computernetze – Ein modernes Lehrbuch
  dpunkt Verlag, 2000
- W. Richard Stevens
  Unix Network Programming
  Vol. 1: Networking APIs - Sockets and XTI
  Vol. 2: Interprocess Communication
  Prentice Hall, 1999 (2. Auflage)
- Wehrle, Pählke, Ritter, Müller, Bechler
  Linux Netzwerkarchitektur (zu Kern 2.4)
  Addison-Wesley, 2002