

K1. Einführung

Begriff: 1. Datennetz: Verarbeitung und Transport von digitalen Daten zwischen Computern und/oder andere Geräte.

2. Information:

Daten.

Signale: physikalische Darstellung von Daten.

3. Netz: LAN (local area netz), PAN (personal area netz), Internet.

Grundlagen: 1. Dienst: Sammlung von Kommunikationsfunktionalität, die eine Kommunikation mit bestimmten Bedingungen ermöglicht. ("was", Also. beschreiben die Funktionalität)

2. Protokoll: Eine mögliche Implementierung eines Dienstes, welche die Funktionalität umsetzt. ("wie", beschreiben: Implementierung eines Dienst)

- Dienstanbieter (SAP) Dienstbinder (SAP) Dienstzugangspunkt (server access point). Schnittstelle zur Dienstanwendung.



- Dienstfunktion: CONNECT, DISCONNECT, DATA, ABORT.

Dienstprimitive:

Grundfunktionen der Kommunikationsschnittstelle. (Basisbausteine der Dienst)

Name der Schicht / Anwendung

HTTP

Dienstleistung

Conn.Ind (Con)

Data (Dat)

Abort (Abor)

Dienstgattung

Request (Req)

Indication (Ind)

Response (Rsp)

- Dienstablauf (Weg-Zeit-Diagramme / Zeitablaufdiagramme).

- (Bereitigter: Sender bekommt Rückmeldung. Unbereiteter: keine Rückmeldung.

Verbindungslos: Dienstleistung ohne Kontext. Jede Paketansicht wird isoliert betrachtet.

Verbindungsorientiert: vier Betriebsphasen: Ruhezustand, Verbindungsaufbau, Verbindungsaufrechterhaltung, Verbindungsaufgabe.

Zusätzlich:

(1) Con. Req → Con. Ind → Con. Rsp

con. Conf ← Con. Rsp

(2) Data. Req → Data. Ind

Prüfung abbruch: PAbor. Ind → PAbor. Ind.

Nutzer abbruch: UAbor. Req → UAbor. Ind.

- Zustandsübergangsdiagramm:



Ergebnis: ausgeliefert Aktion. ausgeliefertes Dienstprimitive; künftiges Dienstprimitive.

2. Protokoll: Eine mögliche Implementierung eines Diensts, welche die Funk. umsetzt.

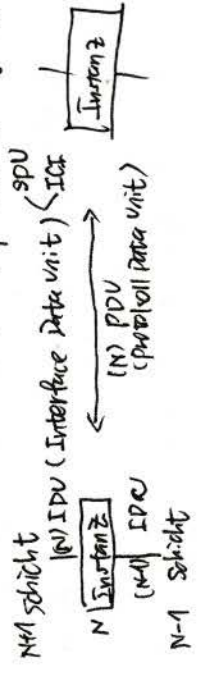
("Wie", implementieren Dienst)

Vertikale Kommunikation:

Kommunikation zwischen zwei benachbarten Schichten auf dem gleichen Rechner (z.B. TCP segment mit IP zur Versendung weitergeben)

Horizontal: Kommunikation zwischen zwei Instanzen der gleich Schicht auf zwei Rechnern.

(z.B. TCP sendet Signale an TCP Empfänger, senden eines Pakets durch IP)



Alternating Bit Protocol

3. Architektur:

ISO/OSI
7: Anwendung (AH)
6: Darstellung (PH)
5: Sitzung (SH)
4: Transport (TH)
3: Vermittlung (IP-Adresse/gleich) (NH)
2: Sicherung (kannst nur lokal) (DL)
1: Präsentation (MAC-Adresse)
des Betriebs/Standardisiert durch die IETF

区别: 先有模型后有协议

有明确的分层概念: (1) Dienst, (2) Schnittstelle, (3) Protokoll

相同: ① 层功能类似

② 以协议栈为基础 (Protocol stack)
③ 传输层上实现数据传输应用于用户. User Oriented.

Zuordnung: Anwendung, Transport, Vermittlung direkt, untere beide OSI auf Host-to-Netzwerk, evtl nach Schicht 5 und 6 zu Anwendung hin, ist aber eigentlich nicht nötig.

作用:

TCP/IP
4: Anwendung / Application-Layer
(4)
(4)
3: Transport-Layer
2: Internet-Layer
1: Host-to-Netzwerk-Layer

Anwendung spezifische Funktion zusammenfasst
Im Anwendungsprotokoll
End-zu-End-Datenübertragung zwischen zwei Endsystem
Isoliert lokaler Netz Wegwahl im Netz
Schnittstelle zum physikalischen Medium

共有协议与有模型

vertikal via TCP

K2 Bitübertragungsschicht (physical Layer / PHY)

目的: 与 Sicherungsschicht (Data Link Layer) 相同, gemeinsam für eine fehlerfreie Datenübertragung zwischen benachbarten Rechnern.

作用: bietet als Medium nachrichtentechnische Kanäle, die einen ungesicherten, längenbeschränkten, ungeprüften Nachrichtenaustausch zwischen einer beschränkten Anzahl von angeschlossenen Einrichtungen unterstützen.

- Defines mechanical properties
 - > Medium: Copper, optical fiber, air
 - > Connectors: form and pin assignment
- Defines electrical/optical properties:
 - > Voltage 电压
 - > Frequencies
 - > Band 波谱率
 - > Bit encoding: RZ, NRZ, Manchester, AMZ, Mod. AMZ

(nur schrittweise, nicht die entsprechenden Protokoll)

Medien: - Ethernet
- UTP
- V.11

Hardware: - Cable, connector, terminator
- Transceiver, hub, repeater


4B/5B:
- 5: 偶数, 0 变 1
- 1: 相同

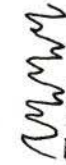
基本知识点: (多数为计算用) - Bitrat: $\text{Schrittgeschwindigkeit in baud} = \text{Übertragungsschwindigkeit in bit/s} = \text{Schrittgeschwindigkeit} \cdot \text{Id}(n)$

Effizienz, Bit / schritt
(coding)

- Robustheit: Wie kann man eine Fehlinterpretation eines empfangenen Signals aufgrund von Verzerrungen vermeiden?
 也何避免因异步时钟造成的误码产生误解?
 - Synchronisation / Taktsynchronisation: 是时钟同步时与数据一起传输
 - Gleichstromfreiheit: 直流电压不能远端传输, 必有电平变化

- Amplitudenmodulation: sehr störtauglich (抗) 振幅变化 

- Frequenzmodulation: 

- Phasenmodulation: bestes Verfahren / komplex. 

- QAM (Quadraturamplitudenmodulation) - Singelwert: 2^n 2^n: 16-QAM 4 bit

- Schritt: zeitintervall

- schrittggeschwindigkeit: Singel / s

- Datenrate: Bit/s

- Ausbreitungsgeschwindigkeit / singelgeschwindigkeit: Singel auf dem Medium ausbreitet
 - Latenz / singelzeit: Singelzeit

- Bandbreite: [dB] = 10 · log₁₀ (S₁/S₂)

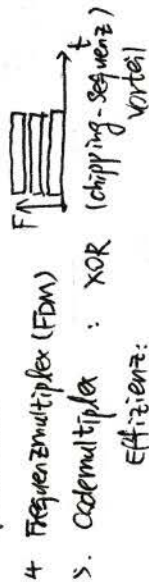
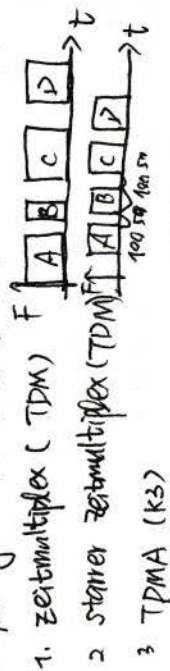
- Nyquist und Shannon-Theorem: > Nyquist: störungsfreier Kanal

Max. Datenrate $[Bit/s] = 2 \cdot B \cdot \log_2(n)$

Shannon: zufälligen Rauschen

Max. Datenrate $[Bit/s] = B \cdot \log_2(1 + S/N)$

Kanalmultiplexing: * Multiplexing. - ein Kanal-Transportkanal für ein oder mehrere Datenströme



Nachteil:

Effizienz:

- RZ: 0: 0, 1: 1, 0
- NRZ: 0: 0, 1: 1
- Differential NRZ: 0: 1, 1: 0
- Mandster: 0: 1, 1: 0
- Differential Mandster: 0: 1, 1: 0
- AMI: 0: 0, 1: 1, 0: 0
- Mod. AMI: 0: 1, 1: 0
- 4B/5B: 1: 1, 0: 0
- S: 1: 1, 0: 0
- L: 1: 1, 0: 0

ineffizienter Entwurf: 1. Selbsttaktung, 2. Gleichstromfreiheit

ist eine Eigenschaft bestimmter Codierverfahren für die Übertragung digitaler Daten, die eine weitere zusätzlich Synchronisation. Die Zeit zur Auswertung der digitalen Info im Signal selbst enthalten ist.

Abtasttheorem von Shannon und Nyquist: Die Abtastfrequenz f_a muss mindestens doppelt so hoch sein wie die höchste im abgetasteten Signal vorkommende Frequenz f_m . $f_a \geq 2 \cdot f_m$

K3 Sicherungsschicht (Data Link-Layer) (lokale Netze)

Wirkung:

- Sicherungsschicht erweitert einen nachrichtentechnischen Kanal zum eigenständigen, abstrakten Medium, gesichert Kanal'
 → fehlerfrei
- Encapsulates data (bits) into Frames (Synchronisation, Strukturierung der Datenströme) 抽象
 - Fehlererkennung und -behandlung (Alternativ Bit Protocol) 必要 (Notwendig)
 - Flusskontrolle (Vermeidung der Überlastung / Pufferüberlauf des Empfängers) und Pufferung
 - Media access control

Bit-Übertragung (物理):

- Bit-Übertragung: - realisiert einen nachrichtentechnischen Kanal zur Übertragung von Bitfolgen. (physikalisches Medium)
 - können bei der Übertragung Fehler auftreten.
 - Übertragung unstrukturierter Bitfolgen / keine Adressierung / keine Adressing

Switch. Bridge

1. Logical Link Control (LLC)

- Protocol Data Units (rahmen)
 - Fehlererkennung und -behandlung
- Flusskontrolle
 - stop and wait
 - sliding window.

2. Medium Access Control

- LAN-Topologien
- MAC
- Ethernet

Reguliertes access to a shared medium 调节对共享介质的访问

- Geregelter Zugriff:
 - Polling
 - Token Ring
- konkurrierender Zugriff:
 - Aloha
 - CSMA / CD, (with collisions)

Logical Link Control

1. Protocol Data Unit:
 - 1. Rahmenbildung. Payload + Kontrollinfo. PCI + PDU + PCI Beginn und Ende eines Rahmens.
 - 2. Erkennung von Rahmenbeginn/ende: Verwendung einer Längenangabe. einfach, aber Verlust der Synchronisation.
 - 2) STX / ETX
 - 3) warte nützliche Info. auf schicht 1.
 - 4) character-stuffing: DLE STX + Payload + ETX
 - 5) bit-stuffing: Flag + Payload + Flag

2. Fehlererkennung / behandlung

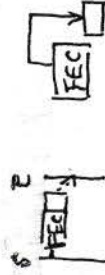
- Fehlerursache:
1. Störeinflüsse → falsch detektierten Bits
 2. Hardwarebedingte Fehler { Einzelbitfehler
Fehlerhaufen
 3. Synchronisierungsfehler.

Fehlerhäufigkeit: Bitfehlerrate (BER) = $\frac{\text{Summe gestörter Bits}}{\text{Summe übertragene Bits}}$

Fehlererkennung: erzeugte "Muster" im Block.
(reagiere auf erkannten Fehler durch Neuübertragung)

Fehlerbehandlung:

1. Reaktiv: automatische Repeat Request (ARQ)
2. Proaktiv: Error correcting codes (FEC) :
(Blöcke enthalten ausreichend Redundanzen zur Korrektur)



(Redundanzen)
Hamming Abstand D:

Fehlererkennung: { Paritätsüberprüfung: Gerade oder ungerade Parität.
CRC (Cyclic Redundancy Check): 冗程 (冗余)

Kreuzparität

Zeichen / Spaltenparität
Block / Längparität

Fehlerkorrektur: Forward Error Correction (FEC): XOR

Hammingcode

Strategien: stop-and-wait, ACK (Bestätigung)
NACK (transmission error)
Timeout (transmission lost)

Ineffizient:
Sinnvoller

Glo-Back-N: 从错误的地方全部重传

Selective Repeat: 仅重传错误部分

3. Flusscontrol. Aufgabe: Der Empfänger wird vor einem zu großen Zufluss von Rahmen eines Senders geschützt.

1. Halt und WEITER

2. Sliding Window

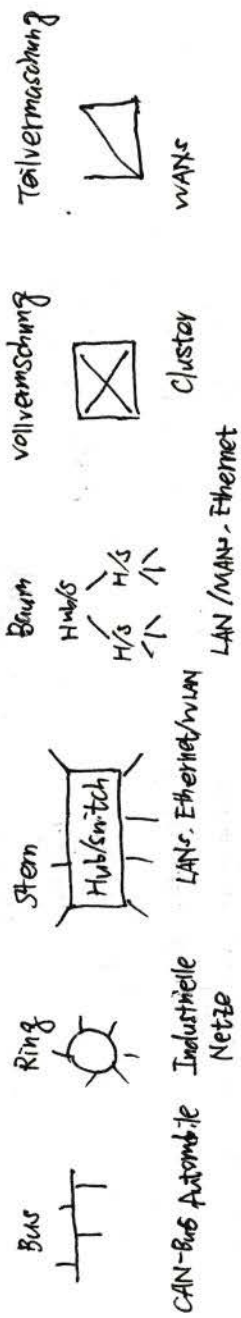
Bitstuffing + CRC Prüfsumme

CRC+ARQ: Piggybacking von Quittung

PPP (point to point Protocol) Flusscontrol: Sliding window.

K3. Medien Access Kontroll

1. Verbindungstopologien.



Teil:

Broadcast-Netz:
- Shared Medium.

- Gleicherzeitiges senden zweier Station \rightarrow Kollision: Regelung des Medienzugriffs nötig.

- Hub: Empfang and Auffrischung von Signalen (wie Repeater oder Verstärker)
(No Bridging) 把收到的信号广播到所有其他接口, 每次只有一个设备发送.

- Switch: 1 Punkt-zu-Punkt Verbindung

(Prüfung + Sicherung) 2. Lernt die Adress angeschlossener Stationen

3. Prüfer für jede Port \rightarrow Keine Kollision.

4. Hoher Durchsatz als Hub

5. Realisiert durch hochrangigen internen Bus.

Koordiniert

2. MAC: zentrale Protokoll: ① Polling. (Bluetooth, USB)

(Token Ring): - Punkt-zu-Punkt verbunden.
- Repeater

- Garantiert Medienzugriff innerhalb einer bestimmten Zeitperiode.
Nicht koordiniert (Ethernet WLAN)

① konkurrierendem Zugriff: ALOHA
- 2 Stationen

最大碰撞时间为: 传输最大长度的帧时间两倍.

>

Slotted ALOHA: zeitlos

②

CSMA/CD

1. bereite ALOHA
2. kanten bevor Talk
3. prüfe auf Kollision

4. Carrier Sense

2. Übertragen

3. prüfe auf Kollision

4. Carrier Sense

2. Übertragen

3. prüfe auf Kollision

4. Carrier Sense

2. Übertragen

3. prüfe auf Kollision

4. Carrier Sense

2. Übertragen

3. prüfe auf Kollision

4. Carrier Sense

2. Übertragen

3. prüfe auf Kollision

4. Carrier Sense

2. Übertragen

3. prüfe auf Kollision

4. Carrier Sense

2. Übertragen

3. prüfe auf Kollision

4. Carrier Sense

2. Übertragen

3. prüfe auf Kollision

4. Carrier Sense

2. Übertragen

3. prüfe auf Kollision

4. Carrier Sense

2. Übertragen

3. prüfe auf Kollision

4. Carrier Sense

2. Übertragen

3. prüfe auf Kollision

4. Carrier Sense

2. Übertragen

3. prüfe auf Kollision

4. Carrier Sense

2. Übertragen

3. prüfe auf Kollision

4. Carrier Sense

2. Übertragen

3. prüfe auf Kollision

4. Carrier Sense

2. Übertragen

3. prüfe auf Kollision

4. Carrier Sense

2. Übertragen

3. prüfe auf Kollision

4. Carrier Sense

2. Übertragen

3. prüfe auf Kollision

4. Carrier Sense

2. Übertragen

3. prüfe auf Kollision

4. Carrier Sense

2. Übertragen

3. prüfe auf Kollision

4. Carrier Sense

2. Übertragen

3. prüfe auf Kollision

4. Carrier Sense

2. Übertragen

3. prüfe auf Kollision

4. Carrier Sense

2. Übertragen

3. prüfe auf Kollision

4. Carrier Sense

2. Übertragen

3. prüfe auf Kollision

4. Carrier Sense

2. Übertragen

3. prüfe auf Kollision

4. Carrier Sense

2. Übertragen

3. prüfe auf Kollision

4. Carrier Sense

2. Übertragen

3. prüfe auf Kollision

4. Carrier Sense

2. Übertragen

3. prüfe auf Kollision

4. Carrier Sense

2. Übertragen

3. prüfe auf Kollision

4. Carrier Sense

2. Übertragen

3. prüfe auf Kollision

4. Carrier Sense

2. Übertragen

3. prüfe auf Kollision

4. Carrier Sense

2. Übertragen

3. prüfe auf Kollision

4. Carrier Sense

2. Übertragen

3. prüfe auf Kollision

4. Carrier Sense

2. Übertragen

3. prüfe auf Kollision

4. Carrier Sense

2. Übertragen

3. prüfe auf Kollision

4. Carrier Sense

2. Übertragen

3. prüfe auf Kollision

4. Carrier Sense

2. Übertragen

3. prüfe auf Kollision

4. Carrier Sense

2. Übertragen

3. prüfe auf Kollision

4. Carrier Sense

2. Übertragen

3. prüfe auf Kollision

4. Carrier Sense

2. Übertragen

3. prüfe auf Kollision

4. Carrier Sense

2. Übertragen

3. prüfe auf Kollision

4. Carrier Sense

2. Übertragen

3. prüfe auf Kollision

4. Carrier Sense

2. Übertragen

3. prüfe auf Kollision

4. Carrier Sense

2. Übertragen

3. prüfe auf Kollision

4. Carrier Sense

2. Übertragen

3. prüfe auf Kollision

4. Carrier Sense

2. Übertragen

3. prüfe auf Kollision

4. Carrier Sense

2. Übertragen

3. prüfe auf Kollision

4. Carrier Sense

2. Übertragen

3. prüfe auf Kollision

4. Carrier Sense

2. Übertragen

3. prüfe auf Kollision

4. Carrier Sense

2. Übertragen

3. prüfe auf Kollision

4. Carrier Sense

2. Übertragen

3. prüfe auf Kollision

4. Carrier Sense

2. Übertragen

3. prüfe auf Kollision

4. Carrier Sense

2. Übertragen

3. prüfe auf Kollision

4. Carrier Sense

2. Übertragen

3. prüfe auf Kollision

4. Carrier Sense

2. Übertragen

3. prüfe auf Kollision

4. Carrier Sense

2. Übertragen

3. prüfe auf Kollision

4. Carrier Sense

2. Übertragen

3. prüfe auf Kollision

4. Carrier Sense

2. Übertragen

3. prüfe auf Kollision

4. Carrier Sense

2. Übertragen

3. prüfe auf Kollision

4. Carrier Sense

2. Übertragen

3. prüfe auf Kollision

4. Carrier Sense

2. Übertragen

3. prüfe auf Kollision

4. Carrier Sense

2. Übertragen

3. prüfe auf Kollision

4. Carrier Sense

2. Übertragen

3. prüfe auf Kollision

4. Carrier Sense

2. Übertragen

3. prüfe auf Kollision

4. Carrier Sense

2. Übertragen

3. prüfe auf Kollision

4. Carrier Sense

2. Übertragen

3. prüfe auf Kollision

4. Carrier Sense

2. Übertragen

3. prüfe auf Kollision

4. Carrier Sense

2. Übertragen

3. prüfe auf Kollision

4. Carrier Sense

2. Übertragen

3. prüfe auf Kollision

4. Carrier Sense

2. Übertragen

3. prüfe auf Kollision

4. Carrier Sense

2. Übertragen

3. prüfe auf Kollision

4. Carrier Sense

2. Übertragen

3. prüfe auf Kollision

4. Carrier Sense

2. Übertragen

3. prüfe auf Kollision

4. Carrier Sense

2. Übertragen

3. prüfe auf Kollision

4. Carrier Sense

2. Übertragen

3. prüfe auf Kollision

4. Carrier Sense

2. Übertragen

3. prüfe auf Kollision

4. Carrier Sense

2. Übertragen

3. prüfe auf Kollision

4. Carrier Sense

2. Übertragen

3. prüfe auf Kollision

4. Carrier Sense

2. Übertragen

3. prüfe auf Kollision

4. Carrier Sense

2. Übertragen

3. prüfe auf Kollision

4. Carrier Sense

2. Übertragen

3. prüfe auf Kollision

4. Carrier Sense

2. Übertragen

3. prüfe auf Kollision

4. Carrier Sense

2. Übertragen

3. prüfe auf Kollision

4. Carrier Sense

2. Übertragen

3. prüfe auf Kollision

4. Carrier Sense

2. Übertragen

3. prüfe auf Kollision

4. Carrier Sense

2. Übertragen

3. prüfe auf Kollision

4. Carrier Sense

2. Übertragen

3. prüfe auf Kollision

4. Carrier Sense

2. Übertragen

CSMA/CD

Taken Ring.

V: Einfach Protokoll

hohe Effizienz / Durchsatz

Passiv Kabel

Erdszeitkabel möglich

Installation einfach

Priorität möglich

N: keine Prioritäten

Komplex Fehlermanagement

kein Erdszeitkabel möglich.

unmäßige Verzögerung unter niedriger Last.

geringe Effizienz durch viele Kollisionen

↳ drahtlose Netze (无线网络)

A B C

Hidden-Station Problem.



改进: CSMA/CA: Carrier Sense Multiple Access with collision Avoidance (Kollision zu vermeiden)

3. Ethernet: Implementierung von CSMA/CD

Datenrate: 10 MBit/s Fast 100 Gigabit 1000

Signalübertragung: Manchester-code 485 B 8B/6T 8B/10B

Topologie: Bus oder Stern Stern

*4 Vermittlungsschicht: (IP, Routing) ① lokalen Punkt-zu-Punkt Verbindung.

(作用): Vermittlungsschicht stellt ~~also~~ eine Adressierung zur Verfügung, die die weltweit eindeutig Identifikation einzelner System möglich (IP-Adressen) und anhand derer eine geeignete Wegwahl durchgeführt werden kann. ②

Im lokalen Netz muss diese Adressierung dann von der Vermittlungsschicht wieder auf die MAC-Adressen der S. 2 abgebildet werden.
与 Sicherungsschicht: ① Vermittlung: beteiligten System nicht benachbart.

相同: viele Protokollmechanismen der Schicht 2 können auch in Schicht 3 finden. ~~Etwa~~ Verfahren zur Flusskontrolle und Datensicherung.

Aufgabe: (was) - Übertragung von Paketen über Netzgrenzen hinweg.

Verknüpfung von Punkt-zu-Punkt- zu Endsystemverbindungen.

- > ① Einheitliche und Eindeutige Endsystem-Adressierung. Adressbildung auf Adressen der Sicherungsschicht.
- > Fragmentierung

- > Wegwahl (Routing & Forwarding)

- > Evtl. Fluss/Staukontrolle, wählbare Übertragungsqualität.

Vermittlung: Leistungsvermittlung oder Speicher-/Paketvermittlung.
verbindungsorientierte / verbindungslose Vermittlungstechniken.

Vermittlung Arten:

① Leistungsvermittlung. (Circuit Switching 电路切换)

Netzverknüpfungsverfahren: 1. Raummultiplex
2. Zeitmultiplex.

② Speicher/Paketvermittlung (Packet Switching)

- "Store & Forward"-Prinzip, zeitlich unabhängig.

(z.B. Briefpost.)

- verbindungslose Paketvermittlung:

- + Verbindungsaufbau, - Überwachung und -abbau entfallen.
- + Bessere Nutzung der Netzkapazität möglich.
- Einzelne Datagramme können unterschiedliche Wege nehmen.
- Reihenfolgeentwärtige Auslieferung beim Empfänger ist nicht gesichert.

① Bsp: Telephonnetz

- Stare Leistungsbeziehung

- schlechtes Verhalten im Fehlerfall

- Überlast kann Verbindung verhindern.

+ kein Header-Overhead

+ Reihenfolge-Treue

+ Exakte Leistungsvorhersage

(Priorität, Latenz...)

② Bsp: Internet.

+ Effizienz

+ Flexible Fehlerbehandlung

+ geringe Implementierungskomplexität.

- Header-Overhead

- kein Reihenfolge-Treue

- keine Leistungsvorhersage möglich:

(Paketverlust, Schwankende Latenz...)

③ z.B. ATM

+ Effizienz

- hohe Implementierungskomplexität.

- Header-Overhead

+ Reihenfolge-Treue

+ Exakte Leistungsvorhersage

(Paketverlustrate, Paket-Late, Latenz...)

③ - verbindungsorientierte Paketvermittlung:

① Virtuelle Leistung (VC)

z.B. ATM

: Kombinierte Vorteil von CS-Netz und Paketvermittlung.

K4.

Vermittlungsschicht im Internet (IP)

IPv4 - Adress, Subnetz, CIDR, NAT
 IPv4 - Header
 Hilfsprotokoll: ARP, DHCP, ICMP
 IPv4 vs IPv6
 Netzwerk zu schaffen.

TCP/IP: zweck ein möglichst ausfallsicheres Netzwerk zu schaffen.

IP-Protokoll zentrale Aufgabe:

Zuweisung von Paketen an einen entfernten Rechner, transparente Ende-zu-Ende-Kommunikation zu (Sicher)
 → definiert ein Adressschema, Regeln zur verbindungslosen Paketverarbeitung und -weiterleitung
 entsprechende Headerinformation.



- ① Pakettransfer: über ein globales Netz: Adressing, Paketformat, Regeln zur Paketverarbeitung (Forwarding)
- ② Wegwahl: durch die Zwischenknoten (Routing)
- ③ Hilfsprotokoll: z.B. Austausch von Info. über den Netzstatus. (Fehlermeldung, Signalisierung)

ICMP, ARP, RARP

IPv4: - Paketvermittlung, verbindungslos, unzuverlässig.

- keine Flusskontrolle, keine Sequenzkontrolle

- Mit ICMP (Internet Control Message Protocol) eine Möglichkeit zur Fehleranzeige.

- Kopplung von Teilnetz und Aufbau eines öffentlichen Netzes.

- ① Adress
 - > 32 bit
 - > Hierarchische Struktur
 - > z.B.: 157.226.12.221
- ② Paketformat
 - > Header mit Kontrollinfo.
 - > Max. Paketgröße: 64 KByte.
- ③ Zusammenspiel mit Routing (Wegvermittlung)
- ④ Hilfsprotokoll: ARP (unterstützt die Interaktion)

Netzwerk Host

für physikalische Netz für Rechner

> Klasse: A B C D E

2⁴ 2⁸ 2⁸

Subnetz.

Wegwahl: 1. Durch Host 2. Durch Netzwerkadresse 3. Default-Eintrag.

IP-Header. 1. Version 2. IHL (Length) 3. Total Length 4. Source Address

- Time to Live (TTL) max. 255 hops.
zählt wie viele Router um 1 verringert
Bei 0 wird Datagramm verworfen.

- DF: Don't Fragment
MF: More Fragment.
Fragment Offset: Folgenummer.

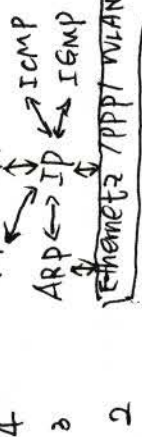
"1": weitere Fragment

"0": letztes Fragment. F.

MTU: Maximum Transfer Unit

IP ↔ MAC

ARP: Umsetz IP-Address → Schicht 2 / MAC Address



z.B. IP Address 137.226.13.40 → Ethernet Address: 00:14:5E:67:99:C9

→ (ARP) RARP: 地址解析, 地址

Zuweisung.

→ DHCP: (Dynamic Host Configuration Protocol). einfache Konfiguration von vernetzten Rechnern.

(Nest) IP-Address zu und liefert Info: DNS-server-Address, Domain-Name, Subnetz-Masken, Router etc...

→ automatische Integration eines Rechners in das Internet bzw. Intranet.

→ ICMP (Internet Control Message Protocol): für Fehlerbehebung oder Testzwecke.

IPv6: - 128 Bit. { Reduktion des Umfangs von Routing-Tabelle.
Multi-Homing
Automatische Konfiguration von Adressen durch einen Rechner (obst auch durch DHCP)

- Vereinfachungsprotokoll.

- Markieren von Paketen für speziellen Verkehr.

NAT: Network Address Translation: 解决 IP 不足问题.

将内部地址和端口号转换成合法的外部地址和端口号.

UDP: Angabe von Sender- und Empfänger-Port auf dieser Ebene notwendig.

Kommunikation zwischen Prozessen: TCP zuverlässige Datenübertragung durch Sendungsmechanismus und Flusskontrolle.

UDP: schnelle Übertragung, da es keinen Kontrollmechanismus hat; füge einem IP-Paket lediglich Portnummern.

7.1.7: TCP: zuverlässig durch ARQ

Flusskontrolle durch Sliding Window mit dynamischer Fenstergröße.
Staukontrolle zur Vermeidung der Netzüberlastung.

UDP: keine Kontrollmechanismen, gleich ~~wie~~ Problem wie IP. (unzuverlässig).

kein Overhead durch Verbindungsaufbau und Verwaltung.

Geringe Latenz beim Senden kleinerer ~~Paketgrößen~~ Datenmengen.

K5. Transport (TCP, UDP)

Schicht 4: End-zu-Ende-Dienst zwischen Anwendungen.

(Kernstück der gesamten Protokollhierarchie)

> unabhängig von den in der Vermittlungsschicht existierenden Diensten.

> Übertragungsqualität wählbar. (z.B. zuverlässig / unzuverlässig)

→ Verdeckung der unterschiedlichen Vermittlungsschichtsdienste.

Instanz der Transportschicht finden nur in den Endsystemen.

Schicht 4 nicht Rechnersystem adressiert sondern Anwendung.

Protokollmechanismen der Transportschicht.

Anwendungscharakteristika:

Remote Work (SSH):

Zuverlässig, geringe Latenz

Protokoll:

Namensauflösung (DNS):

Logische Rechnernamen in IP-Adressen auflösen.

(Transmission Control Protocol)

→ TCP: zuverlässig

(z.B. SSH, HTTP, FTP)

UDP: Einfachheit und geringe Latenz. (z.B. DNS, SNMP)

UDP: Verbindungsloses Transportsprotokoll,

(User Datagram Protocol) fügt Kopfzeile

ein Anwendungschnittstelle

zu IP hinzu.

在IP上添加一个应用接口

Verbindungslos

Latenz.

- keine Kontrollmechanismen (Vermeidung von

- Stauvermeidung sinnvoll. Overhead)

Problem von IP:

- unzuverlässigkeit

- nicht garantieren eine bestimmte Latenz.

→ Paketverlust, in falscher Reihenfolge ankommen, dupliziert

(Fehlerrückmeldung, Stauvermeidung)

④ keine Flusskontrolle vorhanden.

(Flusskontrolle Stauvermeidung)

- Reihenüberlastung

- Belastung eines Empfängers.

⑤ Verzögerung an Paket (Stauvermeidung)

(Reihenfolge- und Duplikaterkennung)

⑥ oft größere Menge an Daten (komplexe Webseiten)

- strombasiert

- Kontext zwischen den Segmenten notwendig (Verbindungsorientiert)

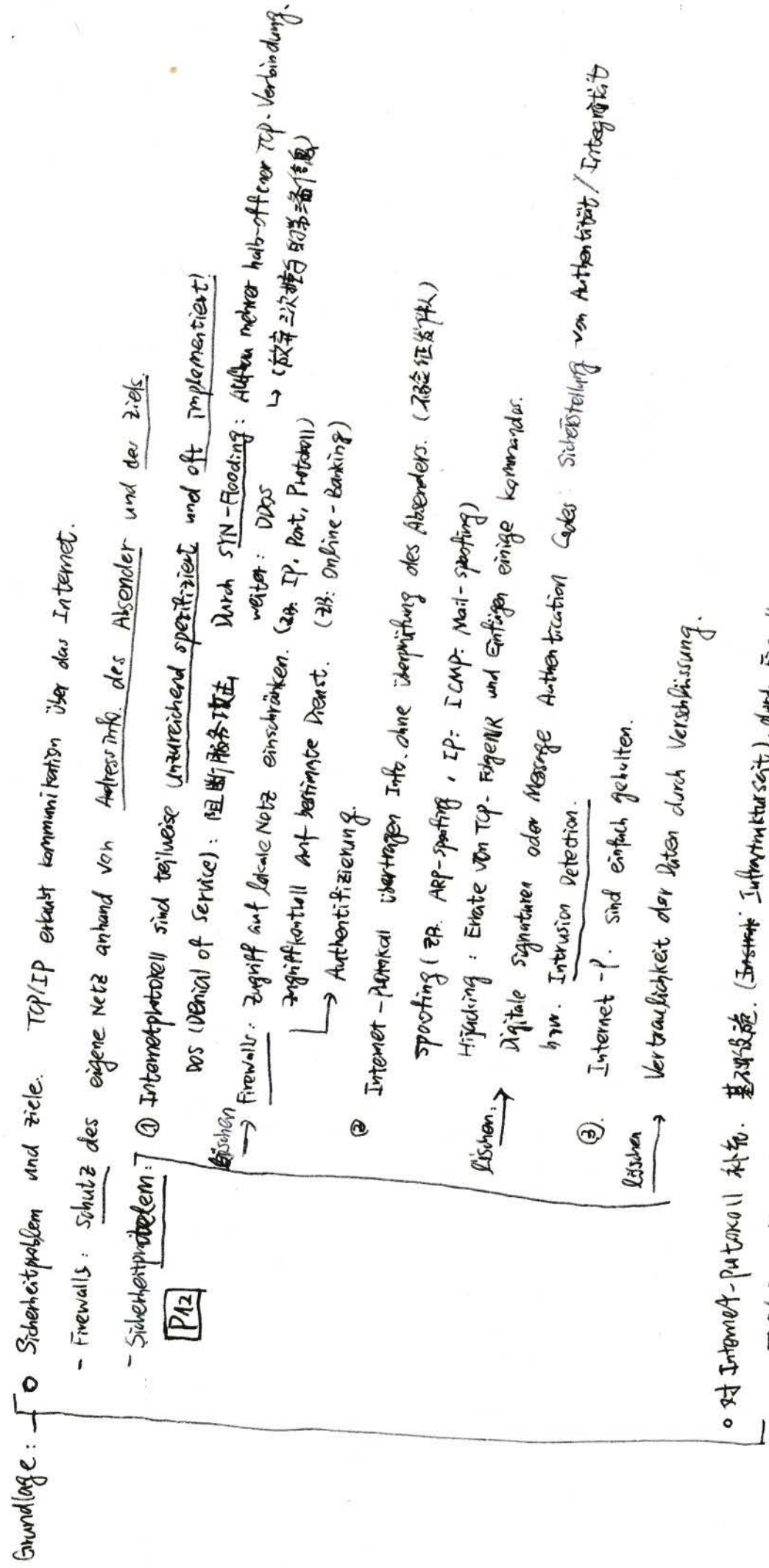
> oft geringe Menge (ein Paket) oder zeitkritische Daten ohne hohe Zuverlässigkeitsanforderung.

- Paketbasiert

- Verbindungslos.

Kb. Internet-Protokoll und Sicherheit.

- Grundlagen: Verschlüsselung, Authentifizierung, Integrität. ^{完整}
- sichere Internet-Protokoll
- Firewalls.



• 对 Internet-Protokoll 补充. 基础设施. (Internet: Infrastruktur). durch Firewall und Intrusion-Detection-Systeme nötig.

TOP/IP 扩展: IPSec (Internet Protocol Security) IKE TLS

Transport: IPSec (Internet key exchange v2) TLS (Transport Layer Security)

Integrität: IPsec TLS

Symmetrische und asymmetrische Verschlüsselung.

- Vertraulichkeit (Geheimhaltung) durch Verschlüsselung.

- Symmetrische: Einigung auf einen gemeinsamen Schlüssel.

Verfahren: DES, AES, RC4... - schneller Übertragung großer Datenmengen.

① Shift Cipher: - Sicherer Datenkommunikationskanal notwendig. (z.B. über ein gemeinsames Geheimnis)

$X = Y - \text{Schlüssel}$ Verschlüsselungsfkt. mit $Y = \text{verschlüsselter Text}$

$X = Y + \text{Schlüssel}$ Entschlüsselungsfkt.

Problem: verschlüsselter Text einfach analysiert werden können.

Block-chiffen

② One-Time Pad. Bitweise XOR-Verknüpfung → Blockchiffen (z.B. DES, IDEA, AES).

- AES: (Advanced Encryption Standard) - Rundstruktur zur mehrfachen Verschlüsselung.

1. 128 Bit - 128 Bit - 128 Bit - 128 Bit - 128 Bit - 128 Bit - 128 Bit - 128 Bit

2. 128 Bit - 128 Bit - 128 Bit - 128 Bit - 128 Bit - 128 Bit - 128 Bit - 128 Bit

3. 128 Bit - 128 Bit - 128 Bit - 128 Bit - 128 Bit - 128 Bit - 128 Bit - 128 Bit

4. 128 Bit - 128 Bit - 128 Bit - 128 Bit - 128 Bit - 128 Bit - 128 Bit - 128 Bit

5. 128 Bit - 128 Bit - 128 Bit - 128 Bit - 128 Bit - 128 Bit - 128 Bit - 128 Bit

6. 128 Bit - 128 Bit - 128 Bit - 128 Bit - 128 Bit - 128 Bit - 128 Bit - 128 Bit

7. 128 Bit - 128 Bit - 128 Bit - 128 Bit - 128 Bit - 128 Bit - 128 Bit - 128 Bit

③ CBC (Cipher Block Chaining): "langer" Nachschlüssel. (z.B. nicht mehr verwendet)

Jeder Block wird vor der Verschlüsselung mit dem Ciphertext des vorherigen Blocks XOR verschlüsselt.

④ MAC (Message Authentication Code): Integritätsprüfung mittels AES und CBC.

⑤ CTR (Counter Mode)

Diffie-Hellman Algo. zum Schlüsselaustausch.

$$T_A = g^a \text{ mod } P$$

$$T_B = g^b \text{ mod } P$$



- Asymmetrische Verschlüsselung: unterschiedliche Schlüssel zur Ver- und Entschlüsselung. (private key / public key).
 langsamer als symmetrische...

① Bsp: RSA (Rivest, Shamir und Adleman): - variable Schlüssellänge

- v. Klartextlänge

Euler's Theorem: $\phi(n) = n-1$ n prim:

$a^{\phi(n)} = 1 \mod n$ a relativ prim zu n.

$q \rightarrow \phi(n) = (p-1) \cdot (q-1)$ (teilerfremd)

n prim oder Produkt zweier Primzahlen \rightarrow n Produkt p, q Primzahlen

$x^y \mod n = x^{y \mod \phi(n)} \mod n$

Fermat's Theorem: n prim und $0 < a < n \rightarrow a^{n-1} = 1 \mod n$.

② HMAC: MAC aufrechterk.

③ PKCS und DSS.

④ ECC (Elliptic Curve Cryptography). Effizient.

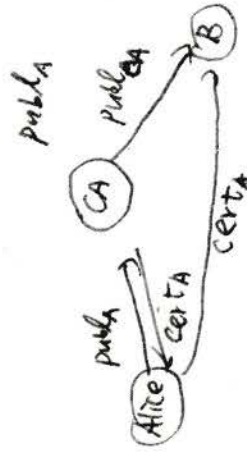
~~PKCS~~ (Konzept)

⑤ Authentifizierung. Problems: ① symmetrisch ~~PKCS~~ KDC (Key Distribution Center)

② Asymmetrisch.

CAs (Certification Authorities)

Lösung:



$\begin{cases} s = m^d \mod n. & \text{Entschlüsselung} \\ v_1 = s^e \mod n & \text{Verschlüsselung} \end{cases}$

Verschlüsselung: $C = m^e \mod n$.

Entschlüsselung: $m = C^d \mod n$.

öffentlich

privat

Sicherung / Transport

Gemeinsam: 1. Strukturierung des Datenstroms: Ethernet teilt die zu übertragenden Daten in Rahmen. In Rahmen: TCP in Segment.

2. Flusskontrolle zur Vermeidung der Überlast des Empfängers. ~~Sliding~~ sliding-window bei beiden Protokoll.

3. Fehlererkennung in beiden Fällen durch Prüfsumme.
 CRC Ethernet.
 TCP Errorkomplement.