

Vertiefung Rechnertechnik und -netzwerke

2 Schichtenmodelle

2.1 Das DoD-Schichtenmodell

Department of Defense

Nr.	Name	Beispiele
4	Anwendung	HTTP, SMTP, SSH, OpenVPN, FTP, LDAP, NCP, AppleTalk AFP
3	Transport	UDP, TCP, SPX, AppleTalk ATP
2	Internet	IP, IPX, NetBEUI, AppleTalk DDP
1	Netzzugang	Ethernet, FDDI, Profibus, ARCNET, Token Ring, LocalTalk

2 Schichtenmodelle

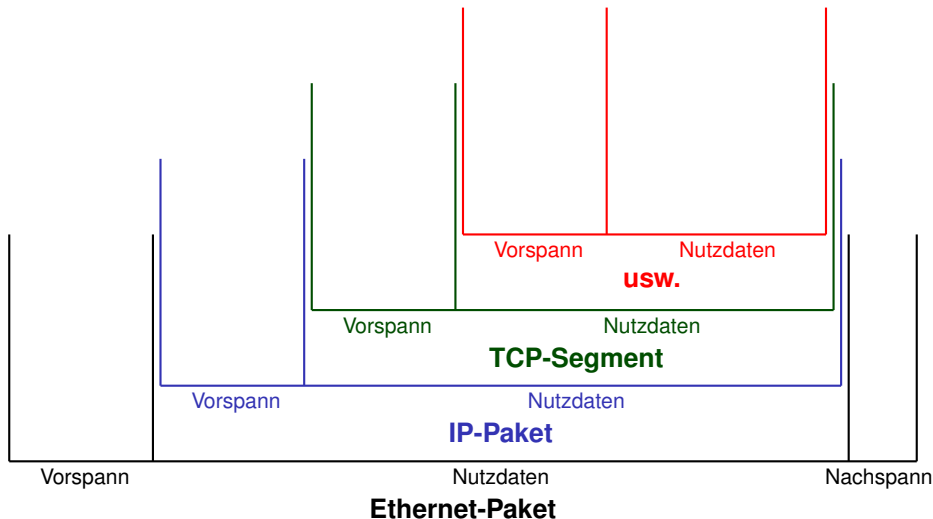
2.2 Das OSI-Schichtenmodell

Open Systems Interconnection

Nr.	Name	Beispiele
7	Anwendung	OpenPGP, S/MIME
		HTTP, SMTP, SSH, OpenVPN, FTP, LDAP, NCP, AppleTalk AFP
6	Darstellung	ASCII, EBCDIC, Kompression, SSL/TLS (Verschlüsselung)
5	Sitzung	RPC, SOCKS, AppleTalk ASP
4	Transport	UDP, TCP, SPX, AppleTalk ATP
3	Vermittlung	IP, IPsec, ICMP, IPX, NetBEUI, AppleTalk DDP
2	Sicherung	ARP
		Ethernet, FDDI, Profibus, ARCNET, Token Ring, LocalTalk, Briefftauben
1	Bitübertragung	Telefon-, Koaxial-, TP-, Glasfaser- oder sonstige Kabel, Funk, Papier

2 Schichtenmodelle

2.3 Protokollstapel



2 Schichtenmodelle

2.4 Netzwerkanalyse in Schicht 2

- Hub: leitet alle Ethernet-Pakete überallhin
Switch: merkt sich Hardware-Adressen

- `tcpdump`: Pakete beobachten
- `wireshark`: Pakete analysieren

—> Konfiguration untersuchen, Fehler und Angriffe erkennen

- `ettercap`: Man-in-the-Middle-Angriffe

Warnung: Unerlaubte Anwendung ist eine Straftat!
(—> mehrjährige Freiheitsstrafe)

2.4 Netzwerkanalyse in Schicht 2

- ARP-Spoofing:
Man-in-the-Middle-Angriffe

2.4 Netzwerkanalyse in Schicht 2

- ARP-Spoofing:
Man-in-the-Middle-Angriffe
Hochverfügbarkeit: verzögerungsfrei übernehmen

2.4 Netzwerkanalyse in Schicht 2

- ARP-Spoofing:
Man-in-the-Middle-Angriffe
Hochverfügbarkeit: verzögerungsfrei übernehmen
- ARP-Ping:
Manipulation der eigenen ARP-Tabelle
IP-Adresse eines anderen Teilnehmers „künstlich“ setzen
oft nötig, um Komponenten einzurichten

2.4 Netzwerkanalyse in Schicht 2

- ARP-Spoofing:
Man-in-the-Middle-Angriffe
Hochverfügbarkeit: verzögerungsfrei übernehmen
- ARP-Ping:
Manipulation der eigenen ARP-Tabelle
IP-Adresse eines anderen Teilnehmers „künstlich“ setzen
oft nötig, um Komponenten einzurichten
- MAC-Spoofing:
Manipulation der eigenen MAC-Adresse (`ifconfig`)
Identität eines anderen Rechners annehmen

2.5 Schicht 1: Störungs- und Kollisionsvermeidung

- Draht: elektrisches Signal übertragen

2.5 Schicht 1: Störungs- und Kollisionsvermeidung

- Draht: elektrisches Signal übertragen
- Problem: elektromagnetische Störungen von/nach außen

2.5 Schicht 1: Störungs- und Kollisionsvermeidung

- Draht: elektrisches Signal übertragen
- Problem: elektromagnetische Störungen von/nach außen
- Lösungen:

2.5 Schicht 1: Störungs- und Kollisionsvermeidung

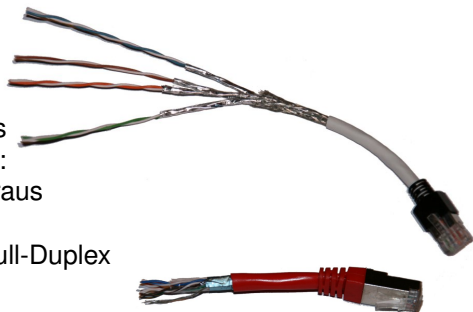
- Draht: elektrisches Signal übertragen
- Problem: elektromagnetische Störungen von/nach außen
- Lösungen:
 - Abschirmung
 - (pseudo-) differentielle Signalübertragung

2.5 Schicht 1: Störungs- und Kollisionsvermeidung

- Draht: elektrisches Signal übertragen
- Problem: elektromagnetische Störungen von/nach außen
- Lösungen:
 - Abschirmung
 - (pseudo-) differentielle Signalübertragung
- Koaxialkabel:
 - Wellenleiter
 - Terminatoren
 - T-Stücke

2.5 Schicht 1: Störungs- und Kollisionsvermeidung

- Draht: elektrisches Signal übertragen
- Problem: elektromagnetische Störungen von/nach außen
- Lösungen:
 - Abschirmung
 - (pseudo-) differentielle Signalübertragung
- Koaxialkabel:
 - Wellenleiter
 - Terminatoren
 - T-Stücke
- Twisted-Pair-Kabel:
 - Störungen mitteln sich heraus
 - Unterschiedliche Schlaghöhe: Übersprechen mittelt sich heraus
 - in der Karte terminiert
 - 2 von 4 Paaren verwendet: Full-Duplex
 - verschiedene Qualitäten



„Koaxialkabel für Arme“

2.5 Schicht 1: Störungs- und Kollisionsvermeidung

- Draht: elektrisches Signal übertragen
- Problem: Kollisionen

2.5 Schicht 1: Störungs- und Kollisionsvermeidung

- Draht: elektrisches Signal übertragen
- Problem: Kollisionen
- Lösungen:

2.5 Schicht 1: Störungs- und Kollisionsvermeidung

- Draht: elektrisches Signal übertragen
- Problem: Kollisionen
- Lösungen:
 - Token Ring: Signal („Token“) kreist zwischen den Teilnehmern
Jeder „spricht“, wenn er an der Reihe ist.
→ Echtzeit-Anwendungen möglich,
Bandbreite voll ausnutzbar

2.5 Schicht 1: Störungs- und Kollisionsvermeidung

- Draht: elektrisches Signal übertragen
- Problem: Kollisionen
- Lösungen:
 - Token Ring: Signal („Token“) kreist zwischen den Teilnehmern
Jeder „spricht“, wenn er an der Reihe ist.
→ Echtzeit-Anwendungen möglich,
Bandbreite voll ausnutzbar
 - Ethernet: CSMA/CD: Kollision erkennen,
ggf. zufällige Zeit abwarten,
dann neuer Versuch
→ keine Echtzeit-Anwendungen möglich,
Bandbreite nur teilweise ausnutzbar

CSMA/CD = Carrier Sense Multiple Access / Collision Detection

2.5 Schicht 1: Störungs- und Kollisionsvermeidung

- Glasfaser: optisches Signal übertragen
- Problem: Kollisionen

2.5 Schicht 1: Störungs- und Kollisionsvermeidung

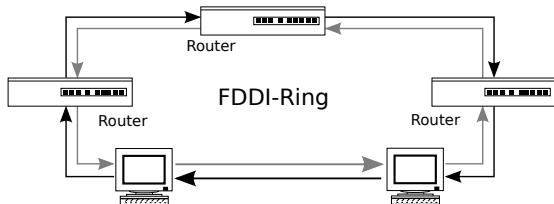
- Glasfaser: optisches Signal übertragen
- Problem: Kollisionen
- Lösung:

2.5 Schicht 1: Störungs- und Kollisionsvermeidung

- Glasfaser: optisches Signal übertragen
- Problem: Kollisionen
- Lösung:
 - FDDI: Signal („Token“) kreist zwischen den Teilnehmern
Jeder „spricht“, wenn er an der Reihe ist.
→ Echtzeit-Anwendungen möglich, Bandbreite voll ausnutzbar

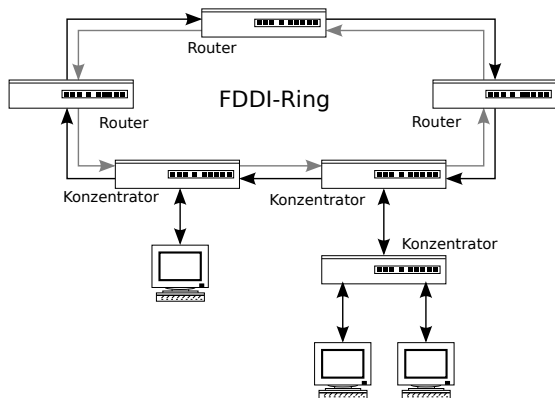
2.5 Schicht 1: Störungs- und Kollisionsvermeidung

- Glasfaser: optisches Signal übertragen
- Problem: Kollisionen
- Lösung:
 - FDDI: Signal („Token“) kreist zwischen den Teilnehmern
Jeder „spricht“, wenn er an der Reihe ist.
→ Echtzeit-Anwendungen möglich, Bandbreite voll ausnutzbar
- FDDI Klasse A:
Zusätzlich: Reserve-Ring



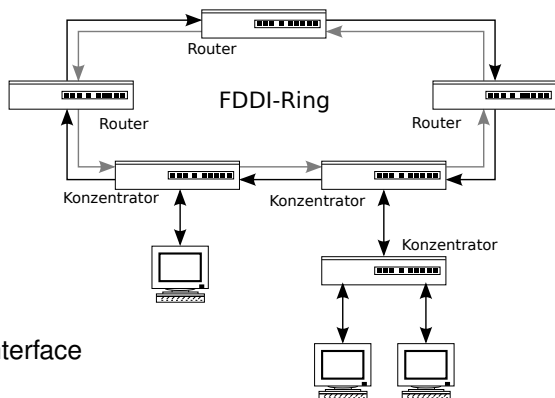
2.5 Schicht 1: Störungs- und Kollisionsvermeidung

- Glasfaser: optisches Signal übertragen
- Problem: Kollisionen
- Lösung:
 - FDDI: Signal („Token“) kreist zwischen den Teilnehmern
Jeder „spricht“, wenn er an der Reihe ist.
→ Echtzeit-Anwendungen möglich, Bandbreite voll ausnutzbar
- FDDI Klasse A:
Zusätzlich: Reserve-Ring
- FDDI Klasse B:
Anschluß an Konzentrator



2.5 Schicht 1: Störungs- und Kollisionsvermeidung

- Glasfaser: optisches Signal übertragen
- Problem: Kollisionen
- Lösung:
 - FDDI: Signal („Token“) kreist zwischen den Teilnehmern
Jeder „spricht“, wenn er an der Reihe ist.
→ Echtzeit-Anwendungen möglich, Bandbreite voll ausnutzbar
- FDDI Klasse A:
Zusätzlich: Reserve-Ring
- FDDI Klasse B:
Anschluß an Konzentrator
- Dual Homing:
Klasse A an zwei Konzentratoren



FDDI = Fiber Distributed Data Interface

2.5 Schicht 1: Störungs- und Kollisionsvermeidung

- Funk: elektromagnetisches Signal übertragen
- Problem: Kollisionen

2.5 Schicht 1: Störungs- und Kollisionsvermeidung

- Funk: elektromagnetisches Signal übertragen
- Problem: Kollisionen
- Lösung:

2.5 Schicht 1: Störungs- und Kollisionsvermeidung

- Funk: elektromagnetisches Signal übertragen
- Problem: Kollisionen
- Lösung:
 - CSMA/CD: Kollision erkennen,
ggf. zufällige Zeit abwarten,
dann neuer Versuch

2.5 Schicht 1: Störungs- und Kollisionsvermeidung

- Funk: elektromagnetisches Signal übertragen
 - Problem: Kollisionen
 - Lösung:
 - ~~CSMA/CD: Kollision erkennen,
ggf. zufällige Zeit abwarten,
dann neuer Versuch~~
- Während des Senden kein Abhören möglich!

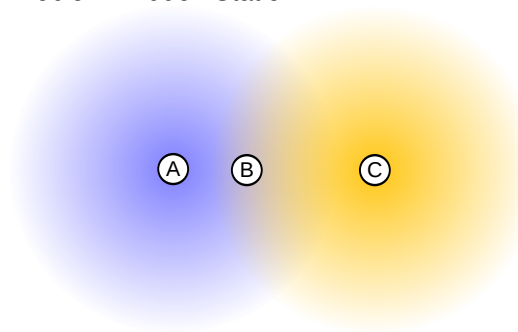
2.5 Schicht 1: Störungs- und Kollisionsvermeidung

- Funk: elektromagnetisches Signal übertragen
- Problem: Kollisionen
- Lösung:
 - ~~CSMA/CD: Kollision erkennen,
ggf. zufällige Zeit abwarten,
dann neuer Versuch~~
Während des Senden kein Abhören möglich!
 - WLAN: CSMA/CA: Kollision möglichst vermeiden
horchen, ob Leitung eine bestimmte Zeit lang frei ist
(„inter-frame spacing“)
zusätzlich zufällige Zeit abwarten
wenn immer noch frei, dann senden

CSMA/CA = Carrier Sense Multiple Access / Collision Avoidance

2.5 Schicht 1: Störungs- und Kollisionsvermeidung

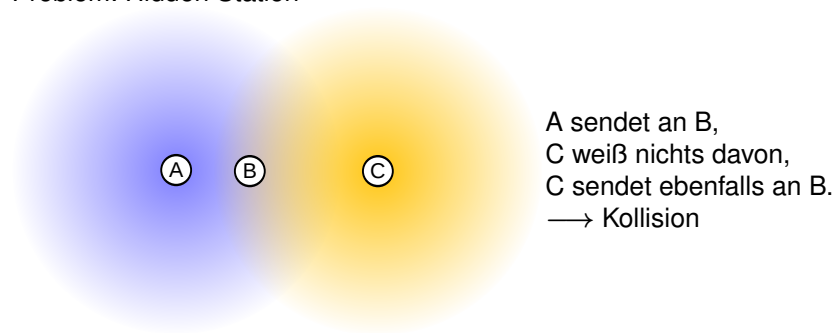
- Funk: elektromagnetisches Signal übertragen
- Problem: Hidden Station



A sendet an B,
C weiß nichts davon,
C sendet ebenfalls an B.
→ Kollision

2.5 Schicht 1: Störungs- und Kollisionsvermeidung

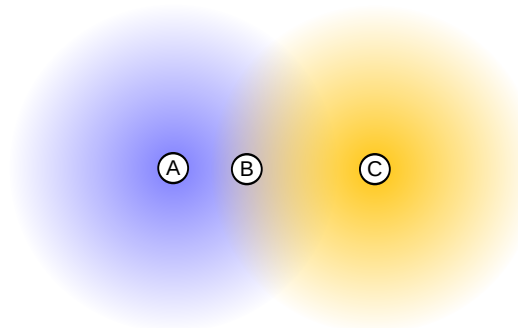
- Funk: elektromagnetisches Signal übertragen
- Problem: Hidden Station



- Lösung: B sendet gelegentlich „Clear to Send“ an A, C merkt es.
—> weniger Kollisionen

2.5 Schicht 1: Störungs- und Kollisionsvermeidung

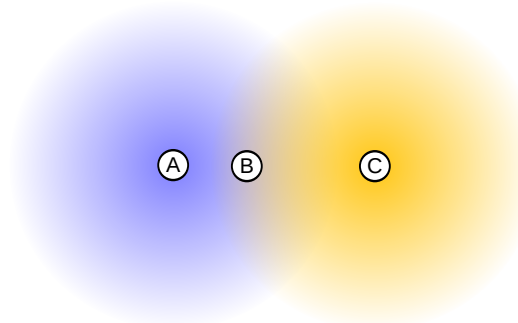
- Funk: elektromagnetisches Signal übertragen
- Problem: Exposed Station



B sendet an A,
C will an jemand
ganz anderen senden,
C wartet, bis B fertig ist.

2.5 Schicht 1: Störungs- und Kollisionsvermeidung

- Funk: elektromagnetisches Signal übertragen
- Problem: Exposed Station



B sendet an A,
C will an jemand
ganz anderen senden,
C wartet, bis B fertig ist.

- Lösung: B sendet gelegentlich „Ready to Send“ an A.
C merkt, daß das zugehörige „Clear to Send“ ausbleibt.

Verschlüsselung

Einführung

- Permutationen: über Buchstabenhäufigkeit knackbar
- periodisch wechselnde Permutationen:
über Autokorrelationen und Buchstabenhäufigkeit knackbar
- Pseudozufallszahlen, Schlüssel = Startwert:
durch Durchprobieren aller Schlüssel knackbar („Brute Force“)
- Echte Zufallszahlen, Schlüssel = alle Zufallszahlen:
unknackbar, aber Schlüssel genauso lang wie Botschaft

- **Spezielle** Pseudozufallszahlen,
Schlüssel = Startwert:

Ab ca. 80 Bit Schlüssellänge:
zu viele Schlüssel,
um alle durchzuprobieren

→ Symmetrische
Verschlüsselungsalgorithmen

Verfahren	Schlüssellänge
DES	56 Bit
3DES	112 Bit
IDEA	128 Bit
Blowfish	32–448 Bit
Twofish	128–256 Bit
Rijndael/AES	128–256 Bit
...	...

Verschlüsselung

Einführung

- Symmetrische Verschlüsselung:
derselbe Schlüssel zum Ver- und Entschlüsseln
3DES, IDEA, Blowfish, Twofish, Rijndael/AES, ...

Verschlüsselung

Einführung

- Symmetrische Verschlüsselung:
derselbe Schlüssel zum Ver- und Entschlüsseln
3DES, IDEA, Blowfish, Twofish, Rijndael/AES, ...
Problem: Schlüsselaustausch

Verschlüsselung

Einführung

- Symmetrische Verschlüsselung:
derselbe Schlüssel zum Ver- und Entschlüsseln
3DES, IDEA, Blowfish, Twofish, Rijndael/AES, ...
Problem: Schlüsselaustausch
- Asymmetrische Verschlüsselung:
öffentlicher Schlüssel zum Verschlüsseln
geheimer Schlüssel zum Entschlüsseln

Verschlüsselung

Einführung

- Symmetrische Verschlüsselung:
derselbe Schlüssel zum Ver- und Entschlüsseln
3DES, IDEA, Blowfish, Twofish, Rijndael/AES, ...
Problem: Schlüsselaustausch
- Asymmetrische Verschlüsselung:
öffentlicher Schlüssel zum Verschlüsseln
geheimer Schlüssel zum Entschlüsseln
RSA, ElGamal, ...

Verschlüsselung

Einführung

- Symmetrische Verschlüsselung:
derselbe Schlüssel zum Ver- und Entschlüsseln
3DES, IDEA, Blowfish, Twofish, Rijndael/AES, ...
Problem: Schlüsselaustausch
- Asymmetrische Verschlüsselung:
öffentlicher Schlüssel zum Verschlüsseln
geheimer Schlüssel zum Entschlüsseln
RSA, ElGamal, ...
Problem: langsam

Verschlüsselung

Einführung

- Symmetrische Verschlüsselung:
derselbe Schlüssel zum Ver- und Entschlüsseln
3DES, IDEA, Blowfish, Twofish, Rijndael/AES, ...
Problem: Schlüsselaustausch
- Asymmetrische Verschlüsselung:
öffentlicher Schlüssel zum Verschlüsseln
geheimer Schlüssel zum Entschlüsseln
RSA, ElGamal, ...
Problem: langsam
- Hybride Verschlüsselung:
verwende Asymmetrische Verschlüsselung
für den Austausch eines symmetrischen Schlüssels


Noch mehr Sicherheit:
Verfahren geheimhalten

~~Noch mehr Sicherheit:
Verfahren geheimhalten~~

„Security by Obscurity“
funktioniert nicht.



**Ist echte Sicherheit möglich,
wenn jeder die Funktionsweise
des Systems untersuchen kann?**

A photograph of the front of a silver car with its hood open, revealing the engine and various fluid reservoirs. The car is parked outdoors on a paved surface with green foliage in the background. A semi-transparent text box is overlaid on the right side of the engine compartment.

**Echte Sicherheit ist nur dann möglich,
wenn jeder die Funktionsweise
des Systems untersuchen kann!**



**Echte Sicherheit ist nur dann möglich,
wenn jeder die Funktionsweise
des Systems untersuchen kann!**

Beispiel 1: Diffie-Hellman-Schlüsselaustausch

- 1976 entdeckt
- Die Formel: $y = b^x$ ist leichter zu berechnen als $x = \log_b y$.
- Bis heute nicht geknackt

Beispiel 2: CSS-DRM-System

- 1996 eingeführt
- Die Formel: *streng geheim*
- 1999 geknackt (von einem 16jährigen Schüler)