



Zusammenfassende Aufgaben zu den OSI-Schichten 1 und 2

WLAN

Da drahtlose lokale Netze immer weitere Verbreitung finden, soll hier auf ein paar wichtige Sicherheitsmerkmale dieser Übertragungstechnik hingewiesen werden:

Passwörter

Ein Passwort für den Zugang zu einem WLAN-Router sollte Buchstaben in Groß- und Kleinschreibung, Zahlen und Sonderzeichen enthalten. Die Geräte werden häufig mit einer Kombination für den Benutzernamen und das Passwort wie beispielsweise „admin“ – „admin“ ausgeliefert.

- Das Passwort sollte unbedingt geändert werden!

Verschlüsselung

Ursprünglich war WEP (Wired Equivalent Privacy) Teil des WLAN-Standards IEEE 802.11.

Die darin enthaltene Verschlüsselung reicht jedoch nicht aus, das WLAN zu sichern. Es gibt frei erhältliche Programme, die den Schlüssel knacken können.

Deshalb wurde mit **WPA2** ein neuer Sicherheitsstandard entwickelt.



Beispiel für die Konfigurationsseite der Sicherheitseinstellungen eines WLAN-Routers

Sicherheit / SSID & Verschlüsselung 1

SSID

SSID: (Bezeichnung des Netzwerks)

SSID unsichtbar: ☐

Verschlüsselung

Betriebsart: WPA2 mit Pre-shared key

Einstellungen zum Pre-shared key

Pre-shared key (PSK): A01!B02?CCxyz

- Ein privates WLAN muss mit dem aktuell besten Verschlüsselungsverfahren (derzeit **WPA2**; Stand: Juli 2018) und einem starken Schlüssel abgesichert werden. Voraussichtlich im Jahr 2019 wird der Sicherheitsstandard **WPA3** eingeführt. Der Schlüssel (häufig auch als Kennwort oder Passwort bezeichnet) sollte mindestens 12 Zeichen lang sein und möglichst viele Sonderzeichen und Zahlen enthalten. Er kann auch notiert und sicher verwahrt werden, denn im Unterschied zu einem Kennwort im Internet hat ein Einbrecher, der an diese Notiz herankommt, auch direkten Zugriff auf den Router.
- Die Betriebssysteme codieren manche Sonderzeichen unterschiedlich. Sollte der Zugriff auf das WLAN mit manchen Geräten nicht möglich sein, ist dies eine mögliche Ursache.

Authentifizierung

Die meisten Router bieten die Möglichkeit, den Zugriff nur für bestimmte MAC-Adressen zu ermöglichen.

Diese Maßnahme ist aber nur als zusätzlicher Schutz sinnvoll, weil sich MAC-Adressen vor-täuschen lassen.



Beispiel für die Einstellungen zur MAC-Filterung bei einem WLAN-Router

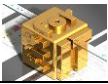
Sicherheit / MAC-Filterung / PCs übernehmen & freigeben

PCs übernehmen & freigeben

MAC-Adresse	IP-Adresse	PC-Name	
00-12-BF-C5-3B-A3	192.168.2.147	(PC1-Name)	Übern.
00-13-CE-6A-64-11	192.168.2.138	(PC1-Name)	Übern.

1. Nenne wichtige Sicherheitsmaßnahmen beim Betrieb eines WLAN-Routers.

- Aktivierung der Verschlüsselung mindestens mit WPA2
- Vergabe eines sicheren Netzwerkschlüssels
- Eingabe eines Passwortes für den Zugang zum Router
- Änderung des SSID-Namens (Bezeichnung des Netzwerks)



2.5.1 Datennetze I

2. Dein Onkel hat gerade eine neue Wohnung gekauft. Um sich besser vorstellen zu können, was er noch anschaffen muss, hat er mit einem Wohnungsplaner ein 3D-Modell erstellt.

Er bittet er dich, ihm ein paar Tipps zu möglichen Vernetzungstechniken zu geben. Dazu hat er eine 3D-Ansicht ausgedruckt und mitgebracht. Außerdem hat er auch ein Video zur virtuellen Begehung der Wohnung erstellt*.

(vgl. .\251-materialien\wohnung\wohnung.mpg)

Die Begehung startet im Wohnzimmer, geht durch das Esszimmer und dann Zimmer für Zimmer nach Norden (in der 3D-Ansicht von oben nach unten).

* Erstellt mit Sweet Home 3D.

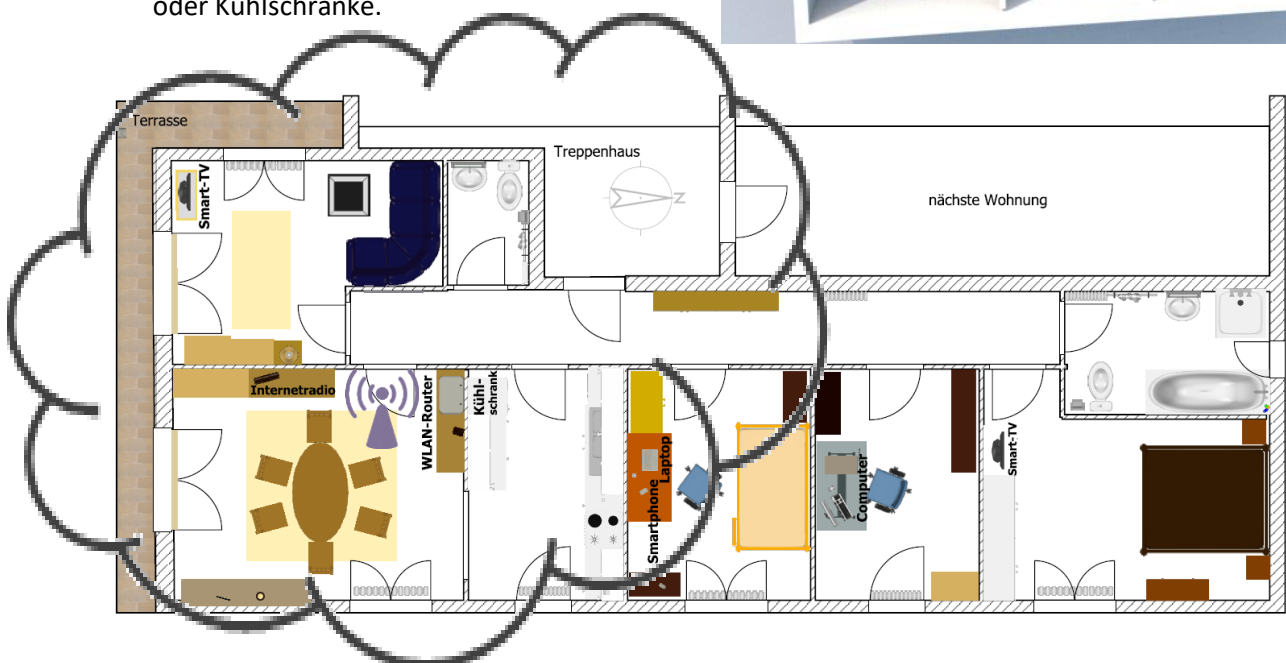
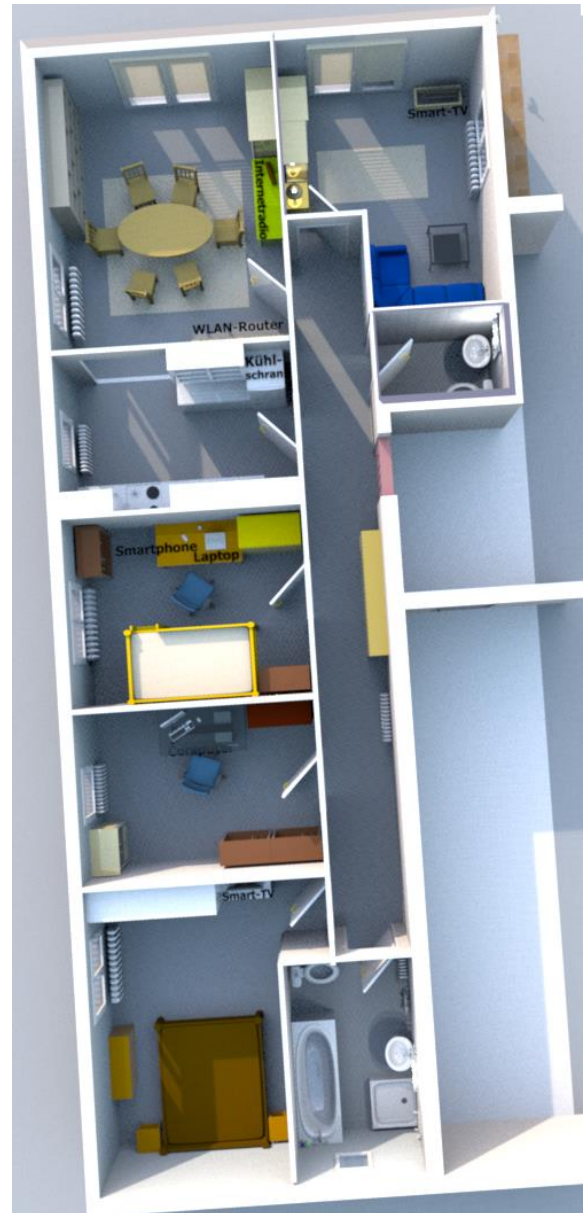
Das Programm ist veröffentlicht unter der GNU General Public License.

Weitere Informationen und Download:
<http://www.sweethome3d.com/>

- a) Besprich mit einem Partner oder in der Gruppe mögliche Vernetzungstechniken für den Grundriss der Wohnung unten.

Hinweise:

- Da der WLAN-Router der Ausgangspunkt möglicher Maßnahmen ist, wird dieser stark vergrößert dargestellt.
- Durch Hindernisse wird das Funksignal gedämpft. Eine Mauer reduziert die Signalstärke je nach Dicke der Wand etwa um ein Viertel. Feuchtigkeit und Metall dämpfen besonders stark. Das gilt z. B. für mit Metallträgern gebaute Rigipswände, Fußbodenheizungen, Waschmaschinen oder Kühlschränke.





2.5.1 Datennetze I

- b) Erläutere, was man bei der Verwendung der jeweiligen Techniken beachten muss. Nenne Vor- und Nachteile der verschiedenen Möglichkeiten.

Hinweise:

- Die Signalstärke ist im Bereich von 2-3 Wänden normalerweise hinreichend, wobei die Datenübertragungsrate mit jeder Wand immer weiter abnimmt.
- Der WLAN-Router steht auf der anderen Seite der Wand direkt hinter dem Kühlschrank. Allgemein gilt: Je höher der Router steht, desto besser. In diesem Fall sollte er auf jeden Fall über dem Kühlschrank montiert werden, wofür man ein Wandregal anbringen könnte.

Mögliche Maßnahmen:

- Ein doppelt geschirmtes Kabel (z. B. S/FTP bzw. Cat 5-Kabel) in das Arbeitszimmer verlegen und *dort einen WLAN Access Point anschließen.*

Vorteil(e): *Schnell, stabil*

Nachteil(e): *Aufwand, Kosten*

- Einen DLAN (Powerline) Adapter mit WLAN Access Point im Arbeitszimmer *über das Stromnetz mit dem WLAN-Router verbinden.*

Vorteil(e): *Geringer Aufwand*

Nachteil(e): *Langsamer als Gigabit-Ethernet*

Störungen durch schlecht entstörte Haushaltsgeräte möglich

- Man könnte auch einen WLAN-Repeater *im Kinderzimmer aufstellen.*

Vorteil(e): *Kann einfach und flexibel positioniert werden*

Nachteil(e): *Niedrigere Datenübertragungsrate*

Höherer Verwaltungsaufwand – insbesondere wenn man

Wert auf Sicherheit legt (siehe Aufgabe c)

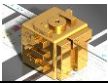
- Für WLAN-Router gibt es auch externe Antennen mit höherer Sendeleistung zu kaufen.
- Beim WLAN muss man letztlich aber ausprobieren. Um die Empfangsqualität festzustellen muss man nicht gleich ein Messgerät kaufen, sondern kann sich für eine grobe Orientierung auch mit der Anzeige der Empfangsqualität auf einem Smartphone behelfen.

- c) In der Erdgeschosswohnung möchte dein Onkel eine Rollladensteuerung installieren, damit er mit Hilfe einer App alle Rolläden zentral herunterlassen und wieder hochziehen kann. Er überlegt auch, die Heizkörperthermostate über eine Smart-Home-Anwendung zu steuern. Außerdem sollen im Flur und im Esszimmer zwei Rauchmelder installiert werden, die über WLAN miteinander vernetzt sind.

- Dein Onkel sollte beachten, dass solche Geräte angreifbar sind und ein Sicherheitsrisiko darstellen. Es ist sinnvoll, dafür zwei getrennte Netze bzw. Zonen zu installieren.

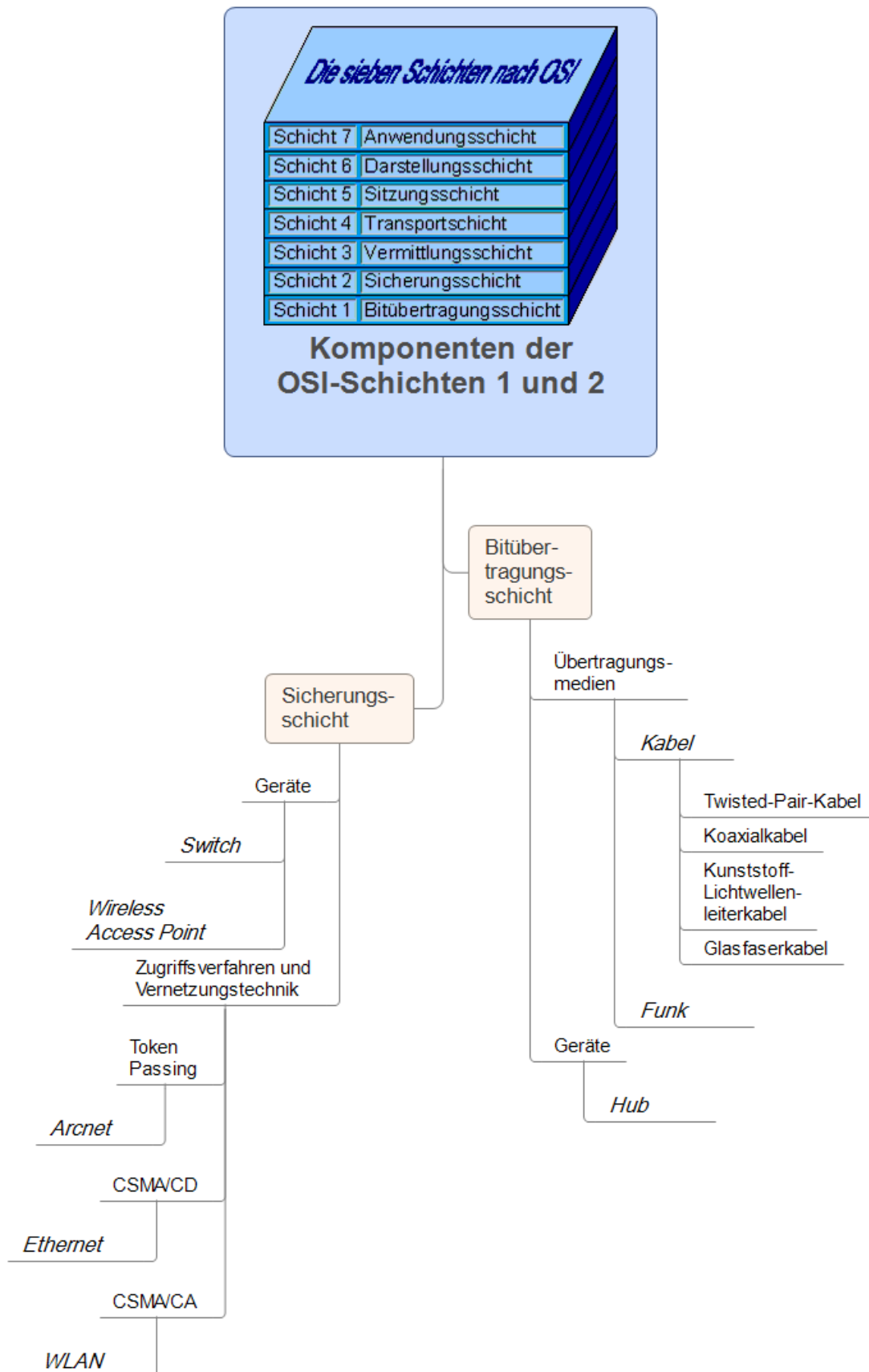
Abhilfe:

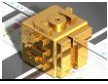
- Manche Router verfügen über die Option, *ein Gastnetz zu aktivieren.*
- Wenn das nicht möglich ist, kann mit einem zweiten Router eine *Routerkaskade gebildet und ein zweites WLAN aufgespannt werden.*
- Es gibt Router, die mehrere Zonen im Netzwerk unterstützen. Um diese zu konfigurieren, muss man sich aber intensiv mit IP-Adressierung beschäftigen (vgl. z. B. c't 2017, Heft 14, S. 114-120)



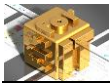
2.5.1 Datennetze I

3. Ergänze die Mindmap zu den Schichten 1 und 2 des OSI-Modells.





4. Kann das CSMA/CD-Verfahren bei einspurigen Verbindungen im Schienennetz verwendet werden?
Das CSMA/CD-Verfahren ist im Schienennetz bei einspurigen Verbindungen wegen möglicher Kollisionen nicht anwendbar.
5. Was ist der wesentliche Unterschied zwischen den Zugriffsverfahren Token-Passing und CSMA/CD in Bezug auf die Sicherung der Übertragung?
- Bei Token-Passing wird die Übertragung eines Datenframes gesichert, indem der Empfänger nach einer erfolgreichen Übertragung eine Bestätigung an den Sender zurücksendet.
 - Bei CSMA/CD ist die Übertragung eines Datenframes mit großer Wahrscheinlichkeit erfolgreich. Der Erfolg wird aber auf der OSI-Schicht 2 nicht garantiert, es können also durchaus Frames während der Bitübertragung verlorengehen.
6. Nenne Kommunikationsarten und gib Beispiele für deren Verwendung an.
- Verbindungsorientiert: Die Kommunikationspartner nutzen eine Leitung exklusiv.
Beispiele: Telegrafie, Telefonie
 - Verbindungslos: Es besteht keine direkte Verbindung zwischen zwei Endpunkten.
*Der Kommunikationskanal wird von mehreren Teilnehmern genutzt.
Beispiel: Computernetze*
7. Beschreibe die Kommunikationsrichtungen, die du kennen gelernt hast.
Nenne Beispiele für technische Lösungen zu den Kommunikationsrichtungen und überlege dir jeweils ein Beispiel dazu im Bereich von Verkehrsnetzen.
- Simplex: Die Datenübertragung erfolgt nur in eine Richtung.
*Fernseh- oder Rundfunkempfang, GPS-Navigation;
zum Beispiel auch bei Motorsport-Rennstrecken.*
 - Halbduplex: Hier kann man nur entweder senden oder empfangen.
Funkgeräte; zum Beispiel bei einspurigen Schienenverbindungen kann ebenfalls nur entweder die eine oder die andere Richtung befahren werden.
 - Vollduplex: Die Teilnehmer können gleichzeitig senden und empfangen.
Telefon, Computernetz; zum Beispiel bei zweisepurigen Schienenverbindungen können gleichzeitig beide Richtungen befahren werden.



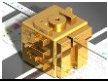
2.5.1 Datennetze I

8. Ergänze die Tabelle zu den OSI-Schichten 1 und 2.

#	Bezeichnung	Erläuterung	Geräte / Techniken
2	Sicherungsschicht (data link layer) - Zugriffsverfahren	Mehrere Bits (meist einige hundert Byte) werden zu Rahmen (<i>frames</i>) zusammengefügt und in eine geordnete Reihe gebracht. Übertragungsfehler werden nach Möglichkeit korrigiert.	Switches verbinden Geräte bzw. Netzsegmente. Wireless Access Points verbinden kabellose Geräte und leitungsgebundene Netze. Ethernet: Zugriffsverfahren <i>CSMA/CD</i> - Netzwerkadapter werden über die <i>MAC-Adresse</i> identifiziert (Media Access Control). WLAN und DLAN: Zugriffsverfahren <i>CSMA/CA</i> WLAN und DLAN (Powerline) verwenden dieselbe Adressierung wie Ethernet, es sind auch alle Daten für jeden Teilnehmer sichtbar. Die Signale können auch außerhalb der Wohnung bzw. des Gebäudes empfangen werden. Zur Datensicherheit ist deshalb die Verwendung von Verschlüsselungsverfahren erforderlich: - Im WLAN derzeit <i>WPA2</i> - Im DLAN derzeit AES (Stand: Mai 2017)
1	Bitübertragungsschicht (physical layer) - Übertragungsmedium	Die Datenübertragung in der Leitung in Form der Bits (1 und 0) als Elektrizität oder mit Hilfe optischer Signale wird geregelt.	z. B. <i>Kabel oder Funk</i> Hubs leiten Daten weiter.

9. Beschreibe die Faktoren zur Leistungsfähigkeit eines Datennetzes:

- **Datenübertragungsrate** (Brutto-Datenrate): *Die Anzahl der Binärzeichen, die pro Sekunde **maximal** in **bit/s** übertragen werden können.*
- **Datendurchsatz** (Netto-Datenrate): Hier werden die reinen Nutzdaten in **bit/s** angegeben.
- **Auslastung:**
 - CSMA/CD im Bus bzw. CSMA/CA im WLAN oder DLAN: *Bei hoher Auslastung nimmt die Datenübertragungsrate auf Grund häufiger werdender Kollisionen ab.*
 - CSMA/CD im Baum: *Die Datenübertragungsrate bleibt auch bei hoher Belastung gleich groß. Allerdings kann es bei hoher Auslastung zu Engpässen kommen.*



2.5.1 Datennetze I

12. In den bisherigen Arbeitsblättern wurden bereits verschiedene Merkmale von Datennetzen genannt - zum Beispiel Kosten, Erweiterbarkeit, Ausfallsicherheit.

Stelle Vorteile und Nachteile der einzelnen Topologien zusammen:

Topologie

Bus

Vorteile

Leichte Erweiterbarkeit

Einfache Handhabung

Preisgünstige Verkabelung

Der Ausfall eines Rechners hat keine Auswirkung auf den Rest des Netzes

Nachteile

Eine Störung in einem Kabel/Stecker blockiert den gesamten Netzverkehr

Immer nur eine Station kann Daten senden

Bei hoher Auslastung „Datenstau“

Im gemeinsamen Übertragungsmedium können Daten abgehört werden

Stern

Vorteile

Hohe Übertragungsraten

Einfache Handhabung und Fehlersuche

Technisch leichte Erweiterbarkeit, sofern die Verkabelung kein Problem ist

Der Ausfall eines Gerätes hat keine Auswirkung auf den Rest des Netzes

Nachteile

Hohe Kosten für die Verkabelung

Der Ausfall des Verteilers blockiert den gesamten Netzverkehr

Baum

Vorteile

Hohe Übertragungsraten

Einfache Handhabung und Fehlersuche

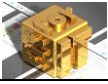
Leichte Erweiterbarkeit, die Verkabelung wird gegenüber dem Stern einfacher

Der Ausfall eines Gerätes hat keine Auswirkung auf den Rest des Netzes

Nachteile

Bei hoher Auslastung sind Engpässe möglich („Datenstau“)

Der Ausfall des Verteilers blockiert den Netzverkehr im ganzen Ast



13. Stelle Anwendungsbereiche, Vorteile und Nachteile der Zugriffsverfahren aus den bisherigen Arbeitsblättern zusammen. Ergänze evtl. weitere Informationen aus dem Internet.

Zugriffsverfahren

Token-Passing

Anwendungsbereiche

Überwachungs- und Steuerungssysteme (z. B. Kraftwerken, in der Medizin, Steuerung

von Automaten in Produktionsanlagen)

Übermittlung von Medien in garantierter Qualität (Telefonvermittlung, Video)

Kommunikation in Transportsystemen (z. B. Schiffe, Raketen)

Vorteile

Echtzeitfähigkeit

Auf den OSI-Schichten 1 und 2 gesicherte Übertragung der Frames

Bus-, Baum-, Stern- und Ringtopologien sind möglich

Hohe Effizienz bei starker Auslastung des Netzes

Nachteile

Maximale Datenübertragungsrate niedriger als bei Ethernet

Etwas höherer Organisationsaufwand bei der Installation und Erweiterung

CSMA/CD

Anwendungsbereiche

Zeitunkritische Computernetze, zum Beispiel Büroanwendungen,

Internetanbindung im lokalen Netz, Anbindung von Druckern

Vorteile

Hohe theoretisch mögliche maximale Datenübertragungsrate

Geringer Organisationsaufwand bei der Installation und Erweiterung

Bus-, Baum- und Sterntopologien sind möglich

Nachteile

Nachlassende Effizienz bei starker Auslastung des Netzes

Keine Echtzeitfähigkeit

Auf den OSI-Schichten 1 und 2 keine gesicherte Übertragung der Frames