

# ITS

Zusammenfassungen für das Fach ITS vorbereitend für die Abschlussprüfung Teil 1.

- Strukturierte Verkabelung
- DHCP / DNS / FTP / TCP / UDP
- ISO / OSI Modell
- IPv4
- IPv6
- Netzwerkkabelarten
- Sicherheitsaspekte
- Berechnungshilfe
- Übungsaufgabe 1
- Übungsaufgabe 2
- Dual-Stack

# Strukturierte Verkabelung

Eine strukturierte Verkabelung oder universelle Gebäudeverkabelung (UGV) ist ein einheitlicher Aufbauplan für eine zukunftsorientierte und anwendungsunabhängige Netzwerkinfrastruktur, auf der unterschiedliche Dienste (Sprache oder Daten) übertragen werden. Damit sollen teure Fehlinstallationen und Erweiterungen vermieden und die Installation neuer Netzwerkkomponenten erleichtert werden.

## Bestandteile einer strukturierten Verkabelung

- standardisierte Komponenten, wie Leitungen und Steckverbindungen
- hierarchische Netzwerk-Topologie (Stern, Baum, ...)
- Empfehlungen für Verlegung und Installation
- standardisierte Mess-, Prüf- und Dokumentationsverfahren

## Ziele einer strukturierten Verkabelung

- Unterstützung aller aktuellen und zukünftigen Kommunikationssysteme, **strukturierte anwendungsneutrale Verkabelung**
- Kapazitätsreserve hinsichtlich der Grenzfrequenz
- das Netz muss sich gegenüber dem Übertragungsprotokoll und den Endgeräten neutral verhalten. Es ist egal, wie wir das Gerät verbinden, das Netzwerk sollte am Ende einfach funktionieren
- flexible Erweiterbarkeit
- Ausfallsicherheit durch vermaschte und/oder eine baumstrukturierte Verkabelung
- Datenschutz und Datensicherheit müssen realisierbar sein
- Einhaltung existierender Standards

## Primärverkabelung - Geländeverkabelung

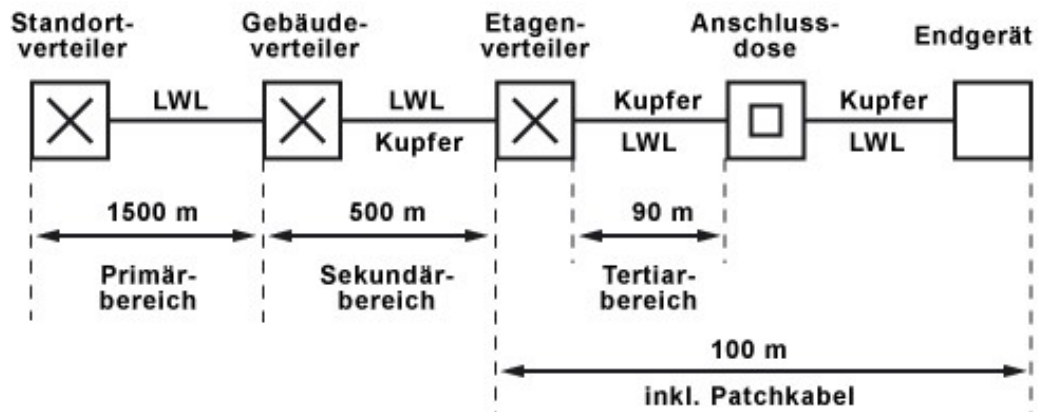
Der Primärbereich wird als Campusverkabelung oder Geländeverkabelung bezeichnet. Er sieht die Verkabelung von einzelnen Gebäuden untereinander vor. Der Primärbereich umfasst meist große Entfernungen, hohe Datenübertragungsraten, sowie eine geringe Anzahl von Stationen.

## Sekundärverkabelung - Gebäudeverkabelung

Der Sekundärbereich wird als Gebäudeverkabelung oder Steigbereichsverkabelung bezeichnet. Er sieht die Verkabelung von einzelnen Etagen und Stockwerken untereinander innerhalb eines Gebäudes vor.

## Tertiärverkabelung - Etagenverkabelung

Der Tertiärbereich wird als Etagenverkabelung bezeichnet. Er sieht die Verkabelung von Etagen- oder Stockwerksverteilern zu den Anschlussdosen vor. Während sich im Stockwerksverteiler ein Netzwerkschrank mit Patchfeld befindet, mündet das Kabel am Arbeitsplatz des Anwenders in einer Anschlussdose in der Wand, in einem Kabelkanal oder in einem Bodentank mit Auslass.



# DHCP / DNS / FTP / TCP / UDP

## DHCP

**Dynamic Host Configuration Protocol** - mit diesem Protokoll werden die IP-Adressen an Endgeräte (das könnte ein PC, Smartphone oder Drucker sein) innerhalb eines Netzwerks zugewiesen. Die Hosts werden dynamisch (automatisch) konfiguriert.

Das Ziel von diesem Protokoll ist es, dass jedem Host im Netzwerk eine IP-Adresse sowohl auch ein Gateway, Subnetzmaske und DNS automatisch zuzuordnen.

Port **67** - UDP (**Server**)

Port **68** - UDP (**Client**)

**Layer 7 (Application Layer)** - OSI Modell

## Ablauf DHCP

- |   |
|---|
| 1. DHCP <b>REQUEST</b> : Der Client fordert eine der angebotenen IP-Adressen, weitere Daten sowie Verlängerung der Lease-Zeit von einem der antwortenden DHCP-Server.                             |
| 2. DHCP <b>OFFER</b> : Die DHCP-Server antworten mit entsprechenden Werten auf eine DHCPDISCOVER-Anfrage.   |
| 3. DHCP <b>ACK</b> : Bestätigung des DHCP-Servers zu einer DHCPREQUEST-Anforderung oder die Übermittlung von Konfigurationsparametern, die vorher durch DHCPINFORM vom Client angefordert wurden. |
| 4. DHCP <b>NAK</b> : Ablehnung einer DHCPREQUEST-Anforderung durch den DHCP-Server.   |
| 5. DHCP <b>DECLINE</b> : Ablehnung durch den Client, da die IP-Adresse schon verwendet wird.  |
| 6. DHCP <b>RELEASE</b> : Der Client gibt die eigene Konfiguration frei, damit die Parameter wieder für andere Clients zur Verfügung stehen.   |
| 7. DHCP <b>INFORM</b> : Anfrage eines Clients nach weiteren Konfigurationsparametern, z. B. weil der Client eine statische IP-Adresse besitzt.  |

## Wichtige Headereinträge DHCP

Client-/Transaction-ID	Zufallszahl, die der Client bestimmt und dem Server der Zuordnung hilft
Flags	Discover Offer Request Acknowledge
Server-Address	Hilft dem DHCP-Server zu erkennen, an wen der Request gerichtet ist
Client-Address	Die IP-Adresse, die dem Client dann zugeordnet wird
Client hardware address	MAC-Adresse welcher der Client Broadcastet

---

## DNS

**Domain Name System** - funktioniert ähnlich wie ein Telefonbuch: Es verwaltet die Zuweisung zwischen Namen und Nummern. DNS-Server übersetzen Namensanforderungen in IP-Adressen und steuern dabei, welchen Server ein Endbenutzer erreicht, wenn er in seinen Webbrowser einen Domänen-Namen eingibt.

Port **53** - UDP

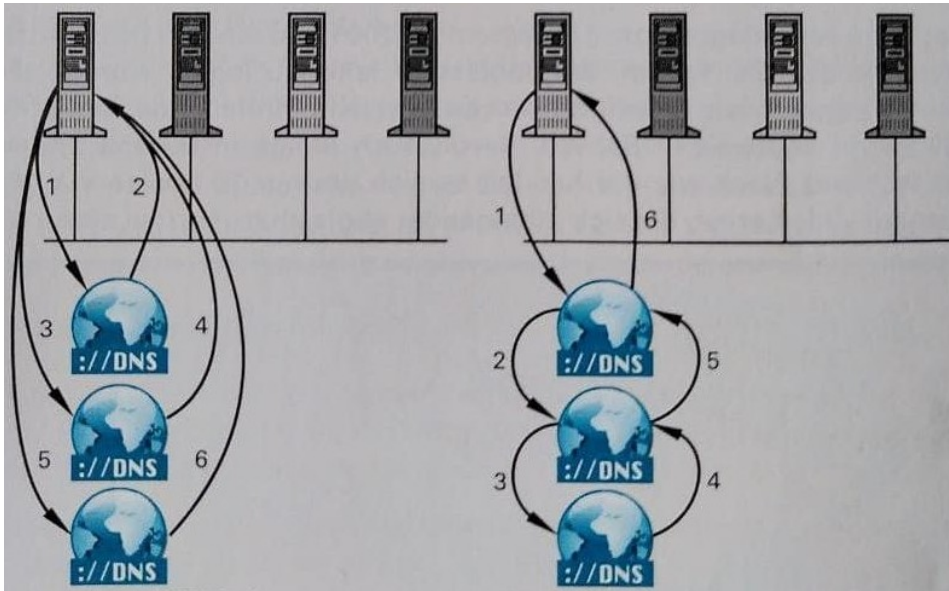
### **Layer 7 (Application Layer)** - OSI Modell

Auf jedem Client ist ein Stück Software installiert, dass sich Resolver nennt. Sollte man eine IP-Adresse auf Basis einer URL benötigen, dann kümmert sich der Resolver um die Anfrage beim DNS-Server.

Eine Anfrage bei einem DNS-Server kann zwei unterschiedliche Antworten zur Folge haben. Beim iterativen Verfahren (links im Bild) bekommt man entweder die gewünschte Antwort oder einen Verweis zu einem anderen DNS-Server. Dieser wird dann vom Resolver auf dem Client angefragt.

Beim rekursiven Verfahren (rechts im Bild) fragt der Resolver ebenfalls bei einem DNS-Server an, sollte der die Antwort nicht kennen, dann leitet dieser sie selbst an den nächsten DNS-Server weiter.

---



## TCP

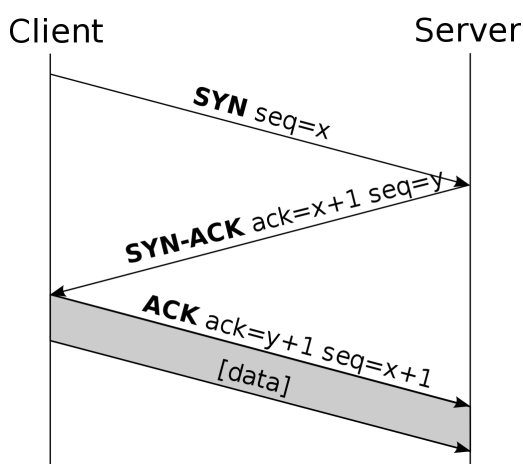
**Transmission Control Protocol** - ist ein verbindungsorientiertes und paketvermittelltes Transportprotokoll. Kommunikation über TCP lässt sich in drei Schritte einteilen, dem Verbindungsaufbau, der Datenübertragung und dem Verbindungsabbau.

**Layer 7 (Application Layer)** - OSI Modell

**Verbindungsaufbau** - Drei-Wege-Handshake

Client (Rechner der Verbindung aufbauen will) schickt ein **SYN** mit einer zufälligen 32-Bit langen Sequenznummer(seq). Ist der Server (Rechner zu dem die Verbindung aufgebaut wird) bereit die Verbindung zu zulassen, dann antwortet er mit einem **SYN-ACK**. Dabei wird die erhaltene seq um eins weitergezählt und als Acknowledgenummer(ack) zurück geschickt. Zusätzlich erstellt der Server selbst eine 32-Bit lange Sequenznummer und schickt diese mit.

Das **SYN-ACK** wird vom Client mit einem **ACK** bestätigt. Hier wird die seq des Servers als ack verwendet und um eins hochgezählt.



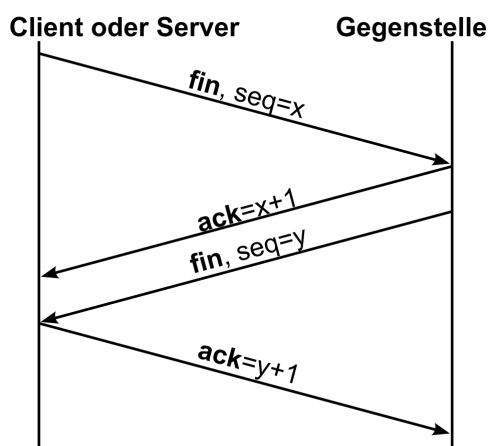
## Datenübertragung

Hier werden die eigentlichen Informationen übertragen. Früher wurde jedes Paket das

ausgetauscht wurde von der Gegenseite mit Hilfe einer Sequenznummer bestätigt. Das führt allerdings zu einer hohen Netzbelastung. Aus diesem Grund hat man die Möglichkeit geschaffen auch mehrere Pakete auf einmal schicken und bestätigen zu können. Dabei wird immer das letzte Paket, das passt bestätigt. Damit ist dem Sender bekannt, was er nochmal nachschicken muss bzw. ab welchem Punkt er weitere Pakete schicken kann.

### Verbindungsabbau - Vier-Wege-Handshake

Ähnlich wie beim Verbindungsaufbau, wird auch hier gegenseitig bestätigt, dass man die Verbindung abbaut. Dabei schickt die eine Seite ein **FIN** mit zufälliger Sequenznummer(seq). Diese wird um eins hoch gezählt und als **ACK** zurückgeschickt. Zusätzlich wird ein zweites, eignes **FIN** Paket verschickt, welches ebenfalls mit einem **ACK** bestätigt wird. Erst ab diesem Moment ist die Verbindung geschlossen.



## UDP

**User Datagram Protocol** - minimales und verbindungsloses Netzwerkprotokoll. Im Gegensatz zu TCP wird hier keine Verbindung aufgebaut, sondern die Daten einfach losgeschickt. Es gibt keine Bestätigung ob die Pakete angekommen sind oder nicht. Es kann also zu unbemerktem Datenverlust kommen. Jedoch gibt es eine Checksumme, die überprüft ob die Pakete fehlerfrei angekommen sind.

Streaming und Telefonie läuft über UDP, da der Verlust von einzelnen Paketen nicht wahrgenommen wird. Und sollte man doch etwas nicht verstanden haben kann man nachfragen.

### Layer 7 (Application Layer) - OSI Modell

---

## FTP

**File Transfer Protocol** - Protokoll wird genutzt um Daten von einem Client zum Server hochzuladen oder von einem Server zum Client herunterzuladen. Zusätzlich können über FTP auch Verzeichnisse angelegt und ausgelesen werden. Zudem können Verzeichnisse und Dateien umbenannt und gelöscht werden.

**Aktives FTP** - Der Client öffnet einen zufälligen Port und teilt diesen zusammen mit der eigenen IP-Adresse mit.

**Passives FTP** - Der Client bittet den Server eine Verbindung aufzubauen, daraufhin öffnet der Server einen Port und schickt diesen zusammen mit der Server-IP an den Client.

Der Verbindungsaufbau dient u.a. der Datenintegrität, damit nicht zwei User gleichzeitig eine Datei umbenennen, löschen usw. können bzw. klar geregelt ist, wer Vorrang hat.

Port **21** - TCP

**Layer 7 (Application Layer)** - OSI Modell



# ISO / OSI Modell

## Unterschiede der beiden Modelle

Das TCP/IP-Modell wurde vor dem OSI-Modell entwickelt, daher unterscheiden sich die Schichten. In Bezug auf das Diagramm ist deutlich zu sehen, dass das TCP/IP-Modell vier Schichten wohingegen das OSI-Modell mit sieben arbeitet. Einer der Hauptunterschiede ist, dass es sich bei OSI um ein konzeptionelles Modell handelt, das praktisch nicht für die Kommunikation verwendet wird, während TCP/IP für den Verbindungsaufbau und die Kommunikation über das Netzwerk verwendet wird.

Vergleichsgrundlage	TCP/IP-Modell	OSI-Modell
Erweitert zu	TCP/IP-Übertragungssteuerungsprotokoll/Internetprotokoll	OSI - Open System Interconnect
Bedeutung	Es ist ein Client-Server-Modell, das zur Übertragung von Daten über das Internet verwendet wird.	Es ist ein theoretisches Modell, das für ein Computersystem verwendet wird.
Anzahl der Schichten	4 Schichten	7 Schichten
Entwickelt von	Verteidigungsministerium (DoD)	ISO (Internationale Standardorganisation)
Verwendungszweck	Meistens benutzt	Nie benutzt

„Please **Do Not Throw Salami Pizza Away**“ (Physical Layer, Data Link Layer usw.)

## Hintergrund und Vor-/Nachteile des ISO/OSI-Modells

Vor der Einführung gab es für die Netzwerkkommunikation verschiedene Standards. Mit der Einführung wollte man ein einheitliches Modell erschaffen, mit dem alle arbeiten, um eine höhere Kompatibilität zwischen Systemen zu gewährleisten.

Vorteile	Nachteile
Anpassungsfähiger und sicherer als die Bündelung aller Dienste in einer Schicht	Es definiert kein bestimmtes Protokoll.
Es unterteilt die Netzkommunikation in kleinere Teile, um sie leichter verständlich zu gestalten	Die Sitzungsschicht und die Darstellungsschicht sind nicht so nützlich wie andere Schichten im OSI-Modell.
Es verfügt über die Flexibilität, sich an viele Protokolle anzupassen	Einige Dienste sind auf verschiedenen Schichten dupliziert, wie die Transport- und Sicherungsschicht

## Protokolle im TCP/IP - Stack

Schicht	Protokoll
Anwendungsschicht (Application Layer)	DHCP, DNS, FTP, IMAP, LDAP, POP3, SMTP, SSH, NTP, SNMP
Transportschicht (Transport Layer)	TCP, UDP
Netzwerkschicht (Network Layer)	IPv4, IPv6
Physische Schicht (Link Layer)	MAC

# IPv4

## Subnetting a subnet --sunny way

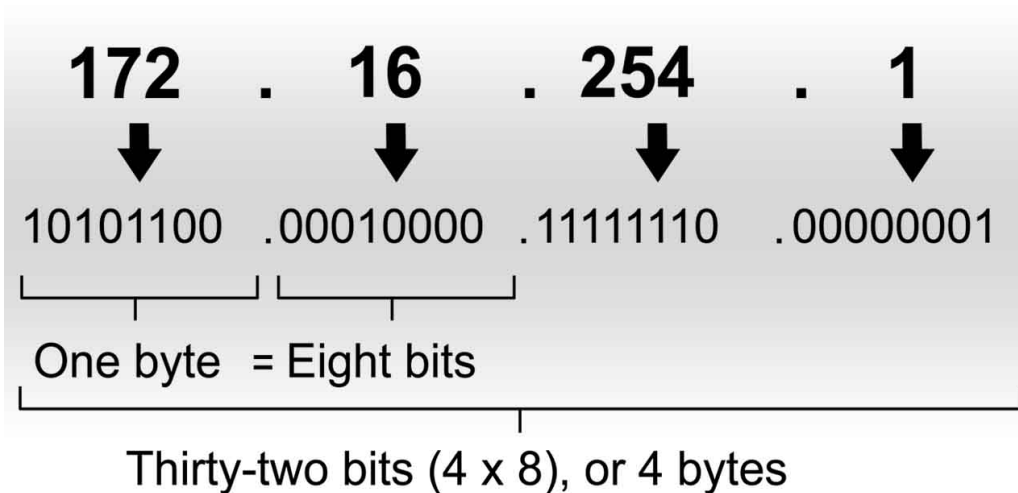
<https://www.youtube-nocookie.com/embed/aVTEZHC2wdA>

## Class B ID - Subnetting

<https://www.youtube-nocookie.com/embed/wuldYxaV46Y>

## Aufbau IPv4 - Adresse

An IPv4 address (dotted-decimal notation)



- geschrieben in dotted Dezimal, also Dezimalzahlen durch Punkte getrennt
- jeder Block besteht aus 8 Bit, also einem Byte auch ein Octet genannt
- gesamte Adresse besteht aus vier Byte
- um mit der Adresse arbeiten zu können muss von Dezimal in Binär umgerechnet werden dabei hilft das Rechnen mit Rest (Modulo)  
Umrechnung am Beispiel von 199

Dividend		Divisor		Quotient	Rest
199	/	2	=	99	1
99	/	2	=	49	1
49	/	2	=	24	1
24	/	2	=	12	0
12	/	2	=	6	0
6	/	2	=	3	0
3	/	2	=	1	1
1	/	2	=	0	1

Reste werden von unten nach oben aufgeschrieben, somit ergibt sich aus dem Beispiel die binäre Zahl:

11000111

# IPv6

## Was ist IPv6 und warum brauchen wir es?

IPv6 (Internet Protocol Version 6) ist ein auf Layer 3 stattfindendes Protokoll für die Übertragung und Vermittlung von Datenpaketen in einem paketorientiert arbeitenden Netzwerk wie dem Internet. Es soll das bisher verwendete IP-Protokoll Version 4 (IPv4) ablösen.

Das Internetprotokoll der Version 4 ist in vielen Bereichen veraltet und kann die Anforderungen moderner Netzwerke und netzwerkfähiger Applikationen nicht mehr im gewünschten Maß erfüllen. Es vereinfacht die Einrichtung und den Betrieb und ist direkt nach dem Start eines netzwerktauglichen Gerätes verfügbar. Zustands behaftete Verfahren zur Adressvergabe wie DHCP, die bei IP der Version 4 zum Einsatz kommen, werden überflüssig.

Im Vergleich zu den IP-Adressen der Version 4 mit 32 Bit Länge sind IPv6-Adressen 128 Bit lang. Sie bieten damit einen wesentlich größeren Adressraum und eine Lösung für die Adressknappheit von IPv4-Adressen im Internet.

## Beispiel einer IPv6 Adresse

**2001:0000:0000:0000:0080:ACDE:02CE:1234**

- **Acht Gruppen** mit je **16 Bit**, separiert mit Doppelpunkten
- Jede Gruppe hat **vier Hexadezimalzeichen** zu je **4 Bit**

Jede in einer Gruppe vorausführende Null kann weggelassen werden

Somit würde die IPv6 Adresse wie folgt aussehen:

**2001:0:0:0:80:ACDE:2CE:1234**

Gruppen aus Nullen können wiederum durch zwei Doppelpunkte dargestellt werden. Dies darf aber nur ein mal angewendet werden. Es können also keine doppelten Paare aus Doppelpunkten verwendet werden!

Schlussendlich sieht unsere IPv6 Adresse dann wie folgt aus:

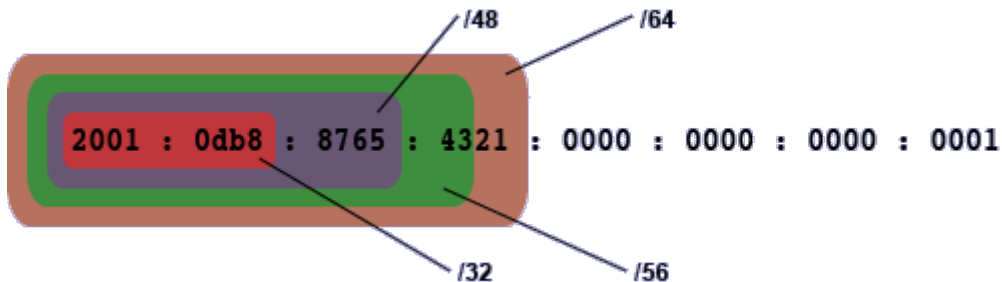
**2001::80:ACDE:2CE:1234**

## Unterteilung der Gruppen

2001:0000:0000:0000:0080:ACDE:02CE:1234

2001:0000:0000:0000	Network Prefix (Präfix oder Netz-ID) – Wobei dieses Modell weiter unterteilt werden kann. So können die letzten 8 Bits der Network Prefix die Subnet Prefix angeben.
0080:ACDE:02CE:1234	Interface Identifier (Suffix, IID oder EUI)

## Segmentierung: Präfix und Präfixlänge



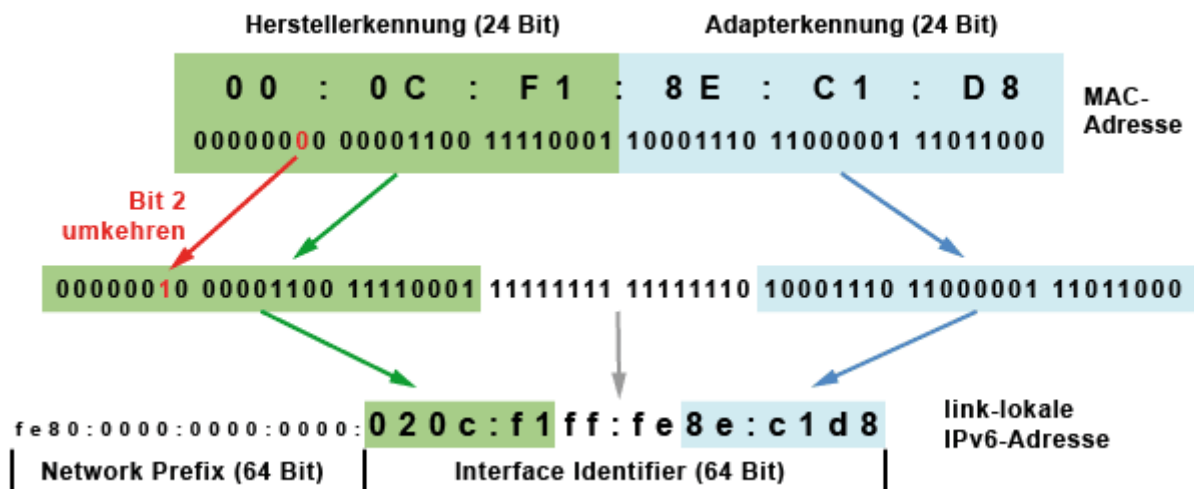
Die von IPv4 bekannte Netzmaske bzw. Subnetzmaske fällt bei IPv6 ersatzlos weg. Um trotzdem eine Segmentierung und Aufteilung von Adressbereichen bzw. Subnetzen vornehmen zu können, wird die Präfixlänge definiert und mit einem / an die eigentliche IPv6-Adresse angehängt. Der hierarchische Aufbau des Präfixes soll das Routing mit IPv6 vereinfachen. Standardmäßig ist /64 die Präfixlänge. Es gibt jedoch weitere typische Präfixe, die 32, 48 und 56 Bit lang sind.

## IPv6-Address-Scopes (Gültigkeitsbereiche)

<b>Unicast</b>	Link-Local-Adressen (Verbindungslokale Unicast-Adressen) sind nur innerhalb von geschlossenen Netzsegmenten gültig. Router dürfen Datenpakete mit Link-Local Adressen als Quelle oder Ziel nicht an andere Links weiterleiten.  Präfix: <b>fe80::/10</b>
<b>Multicast-Adressen</b>	Eine Multicast-Adresse ist ein Identifier für eine Gruppe von Geräten. Jedes Gerät kann zu beliebig vielen Multicast-Gruppen gehören.  Präfix: <b>ff00::/8</b>
<b>Anycast-Adressen</b>	Im IPv6 wurde ein neuer Adresstyp "Anycast" definiert. Dieser Adresstyp erlaubt es, dass Datenpakete zu einem oder mehreren Geräten mit gleicher Adresse geroutet werden. Anycast-Adressen können einem oder mehreren, typischerweise an unterschiedlichen Geräten befindlichen, Netzwerk-Interfaces zugewiesen werden. Die Routing-Protokolle liefern jedes Paket zum nächsten Interface.

## SLAAC und DAD

**Stateless Address Autoconfiguration (SLAAC)** ist ein Verfahren zur zustandslosen und automatischen Konfiguration von IPv6-Adressen an einem Netzwerk-Interface. Mit „stateless“ bzw. „zustandslos“ ist gemeint, dass die jeweilige IPv6-Adresse nicht zentral vergeben und gespeichert wird. Demnach erzeugt sich der Host seine IPv6-Adresse unter Zuhilfenahme zusätzlicher Informationen selbst.



Eine link-lokale IPv6-Adresse wird aus einem Präfix (64 Bit) und einem Suffix (64 Bit) gebildet. Der Präfix für alle link-lokalen IPv6-Adressen ist immer "fe80:0000:0000:0000". Das Suffix (Interface Identifier) ist der EUI-64-Identifizierer oder IEEE-Identifizierer, der aus der MAC-Adresse (Hardware-Adresse des Netzwerkadapters) gebildet wird.

In der Mitte der 48-Bit-MAC-Adresse (zwischen dem dritten und dem vierten Byte) werden mit "ff:fe" zwei feste Bytes eingefügt, damit es 64 Bit werden. **Zusätzlich wird noch das zweite Bit im ersten Byte der MAC-Adresse invertiert.** Das heißt, aus "1" wird "0" und aus "0" wird "1".

Auf diese Weise wird zum Beispiel die MAC-Adresse "00:0C:F1:8E:C1:D8" zum Interface Identifier "020c:f1ff:fe8e:c1d8". Und der Host bildet sich so die link-lokale Adresse "fe80:0000:0000:0000:020c:f1ff:fe8e:c1d8".

Um Adresskollisionen zu vermeiden sollte der Host bei einer neu generierten IPv6-Adresse eine **Duplicate Address Detection (DAD)** durchführen.

1. **Neighbor Solicitation:** Dazu schickt der Host eine Anfrage an die generierte Adresse ins lokale Netz. Als Antwort-Adresse dient eine Multicast-Adresse.
2. **Neighbor Advertisement:** Falls eine andere Station die IPv6-Adresse bereits nutzt, kommt eine Antwort zurück.

Erst wenn keine Antwort von dieser Adresse zurückkommt bindet sich das Interface an diese Adresse und kann sie für die Kommunikation nutzen.

Weil es keine Pflicht gibt eine DAD durchzuführen, sind Adresskollisionen durchaus möglich. Aufgrund des sehr großzügigen Adressraums und der weltweit eindeutigen MAC-Adressen aber eher unwahrscheinlich.

Sollte es doch einmal zu einer Kollision kommen und die IPv6-Adresse tatsächlich schon existieren,

dann muss die IPv6-Adresse vom Anwender manuell geändert werden.

Dann sollte man gleich das ganze Netzwerk überprüfen. Es könnte dann sein, dass jemand eine MAC-Adresse gekapert hat und per MAC-Spoofing ins Netzwerk eingedrungen ist.



# Netzwerkkabelarten

Um die Netzwerkkabel und ihre Übertragungseigenschaften eindeutig zu beschreiben, existieren die Kategorien eins bis acht (Cat.1 bis Cat.8).

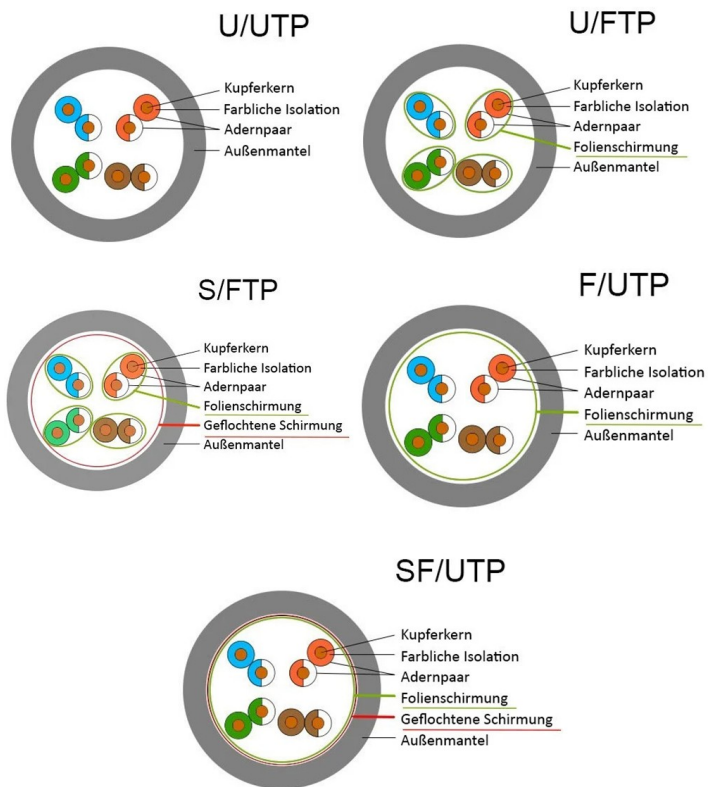
Im praktischen Einsatz spielen Kabel der Kategorien eins bis vier heute kaum noch eine Rolle. Sie wurden zum Teil für die reine Sprachübertragung oder für Netzwerke mit niedrigen Bandbreiten verwendet. Im Unterschied zu diesen Kabeln eignen sich **Cat.5 bis Cat.8 Patchkabel** für aktuelle Netzwerk- und Telekommunikationsstandards.

## Was ist ein UTP-Kabel

Ein UTP-Kabel ist ein beliebtes Kabel für Telefon- und Computernetzwerke und besteht aus gedrehten Aderpaaren mit einer Standard-Farbcodierung. Der Name „UTP-Kabel“ wird übrigens zu Unrecht für alle sog. Twisted-Pair-Netzwerkkabel verwendet. Twisted-Pair-Netzwerkkabel gibt es in geschirmter und nicht-geschirmter Form, wobei es sich bei UTP (also die Unshielded-Twisted-Pair) um die nicht abgeschirmte Kabelvariante handelt. Dieser Typ Kabel verfügt somit über keinen elektromagnetischen Schutz gegen Interferenzen bzw. elektromagnetische Störungen. Zu diesem Zweck gibt es verschiedene geschirmte UTP-Kabel wie FTP (Foiled-Twisted-Pair), STP (Shielded-Twisted-Pair) und S/FTP-Kabel.

## Geschirmte Kabel

Alter Name	Neuer Name	Schirmung Kabel	Schirmung Aderpaare
UTP	U/UTP	keine	keine
STP	U/FTP	keine	Folie
FTP	F/UTP	Folie	keine
S-STP	S/FTP	Geflecht	Folie
S-FTP	SF/UTP	Folie und Geflecht	keine



Welche Geschwindigkeiten kann ein UTP-Kabel erreichen?

Bezeichnung	Geschwindigkeit	Durchsatzgeschwindigkeit
Cat.5	100 Mbit/s	100 MHz
Cat.5e	1000 Mbit/s	100 MHz
Cat.6	1000 Mbit/s	250 MHz
Cat.6a	10.000 Mbit/s	500 MHz
Cat.7	10.000 Mbit/s	600 - 1.000 MHz
Cat.8	40.000 Mbit/s - 100.000 Mbit/s	1.600 - 2.000 MHz

Ein flexibles Kabel (stranded) oder einen Starrleiter (solid)?

Der UTP-Kabeltyp ist vom Aufbau der einzelnen Adernpaare abhängig.

Wenn Sie das UTP Kabel entmanteln, sehen Sie 8 kleine Adern. Wenn Sie diese kleinen Adern wiederum stripfen, wird der Unterschied zwischen flexibel und Starrleiter sichtbar. Bei flexiblen Kabeln besteht jede einzelne Ader aus vielen kleinen Kupferdrähten. Beim Starrleiter besteht jede kleine Ader aus einem festen Kern.

# Sicherheitsaspekte

## Allgemeine Schutzziele

- **Vertraulichkeit:** Daten dürfen lediglich von autorisierten Benutzern gelesen bzw. modifiziert werden, dies gilt sowohl beim Zugriff auf gespeicherte Daten wie auch während der Datenübertragung.
- **Integrität:** Daten dürfen nicht unbemerkt verändert werden. Alle Änderungen müssen nachvollziehbar sein.
- **Verfügbarkeit:** Verhinderung von Systemausfällen; der Zugriff auf Daten muss innerhalb eines vereinbarten Zeitrahmens gewährleistet sein.

## Weitere Schutzziele

- **Authentizität** bezeichnet die Eigenschaften der Echtheit, Überprüfbarkeit und Vertrauenswürdigkeit eines Objekts.
- **Verbindlichkeit/Nichtabstreitbarkeit:** Sie erfordert, dass „kein unzulässiges Abstreiten durchgeführter Handlungen“ möglich ist. Sie ist unter anderem wichtig beim elektronischen Abschluss von Verträgen. Erreichbar ist sie beispielsweise durch elektronische Signaturen.
- **Zurechenbarkeit:** „Eine durchgeführte Handlung kann einem Kommunikationspartner eindeutig zugeordnet werden.“
- in bestimmtem Kontext (zum Beispiel im Internet) auch **Anonymität**

## Besonderes Schutzziel im Zuge der DSGVO

- **Resilienz:** Widerstandsfähigkeit/Belastbarkeit gegenüber Ausspähungen, irrtümlichen oder mutwilligen Störungen oder absichtlichen Schädigungen (Sabotagen)

## Was ist die DSGVO?

Die Datenschutz-Grundverordnung (DSGVO oder DS-GVO) ist eine Verordnung der Europäischen Union, mit der die Regeln zur Verarbeitung personenbezogener Daten durch die meisten Verantwortlichen, sowohl private wie öffentliche, EU-weit vereinheitlicht werden. Dadurch soll einerseits der Schutz personenbezogener Daten innerhalb der Europäischen Union sichergestellt, und auch andererseits der freie Datenverkehr innerhalb des europäischen Binnenmarktes gewährleistet werden.

- Die DSGVO harmonisiert seit dem 25. Mai 2018 die rechtlichen Vorgaben zur Verarbeitung personenbezogener Daten durch private Unternehmen und öffentliche Stellen in Europa.

- Die DSGVO erlegt Unternehmen umfangreiche Pflichten auf, wie Meldepflichten, Rechenschaftspflichten, Sicherstellung der Datensicherheit und Umsetzung von Betroffenenrechten. Gleichzeitig stärkt die DSGVO die Verbraucherrechte.
- Zusätzlich gewährt die DSGVO Schadensersatzansprüche für materielle und immaterielle Schäden, die Personen aufgrund einer Verletzung von Regelungen aus der DSGVO entstehen.

## Weitere für die Prüfung interessante Punkte

- Aktuelle Software/Firmware
- Kennwortvergabe und -sicherheit (Es soll mindestens zehn Zeichen lang sein, Groß- und Kleinschreibung, Sonderzeichen und mindesten eine Zahl enthalten. Es soll keine Wörter aus Wörterbüchern enthalten.)
- Verschlüsselungsmethode und Kennwortvergabe bei WLAN und anderen Diensten
- ~~Abschaltung Systeme außerhalb der Arbeitszeiten~~ Bitte in der Prüfung diskutieren! :D

# Berechnungshilfe

Binär				Dezimal	Hexadezimal
0	0	0	0	0	0
0	0	0	1	1	1
0	0	1	0	2	2
0	0	1	1	3	3
0	1	0	0	4	4
0	1	0	1	5	5
0	1	1	0	6	6
0	1	1	1	7	7
1	0	0	0	8	8
1	0	0	1	9	9
1	0	1	0	10	a
1	0	1	1	11	b
1	1	0	0	12	c
1	1	0	1	13	d
1	1	1	0	14	e
1	1	1	1	15	f

Mit Hilfe dieser Tabelle kann man sehr leicht jede dezimal Zahl in eine hexadezimale Zahl umrechnen. Dabei geht man den Umweg über die binären Zahlen. Der Rückweg ist ebenfalls möglich.

Umrechnung am Beispiel von 999

Dividend		Divisor		Quotient	Rest
999	/	2	=	499	1
499	/	2	=	249	1
249	/	2	=	124	1
124	/	2	=	62	0
62	/	2	=	31	0
31	/	2	=	15	1
15	/	2	=	7	1
7	/	2	=	3	1
3	/	2	=	1	1
1	/	2	=	0	1

- Es ergibt sich die binäre Zahl (von unten nach oben gelesen):  
1111100111
- Diese wird von rechts nach links in vierer Blöcke unterteilt:  
11 | 1110 | 0111
- sollte der Block ganz links nicht aus vier Bit bestehen wird mit Null aufgefüllt:  
0011 | 1110 | 0111
- jeder Block kann mit Hilfe der Tabelle in eine hexadezimale Zahl umgewandelt werden:  
3 | e | 7 -> 0x 3e7

# Übungsaufgabe 1

## Netzkonfiguration

Die Firma DarSys GmbH ist dabei, die bisherige IPv4-Netzkonfiguration in eine IPv6-Netzkonfiguration umzustellen. Zum aktuellen Zeitpunkt wird im Dual-Stack gearbeitet, um den laufenden Betrieb nicht zu gefährden. Den logischen Netzwerkplan der Firma DarSys können Sie der Anlage 3.pdf entnehmen.

1. Alle Netzwerk- und Hostanteile der IPv4-Adressen und IPv6-Adressen sind fortlaufend zu nummerieren. Der binäre Wert des dezimalen Host-Teils der IPv4-Adresse soll mit dem binären Wert des hexadezimalen Host-Teils der IPv6-Adresse im letzten Byte identisch sein.
  - Stellen Sie die IPv6-Adresse in gekürzter und ungekürzter Version dar.
  - Vervollständigen Sie die grau hinterlegten Felder der Adresstabelle auf dem Vorgabeblatt Anlage 9.pdf.
2. Erläutern Sie, warum einem Switch eine IP-Adresse gegeben wurde.
3. Ein Mitarbeiter der DarSys GmbH berichtet, dass er an seinem neuen Arbeitsplatz immer die gleiche Fehlermeldung bekommt (siehe Abbildung), wenn er eine Webseite in seinem Internetbrowser aufrufen möchte.



- Nennen Sie drei Ursachen am Computer oder im Netzwerk für die abgebildete Fehlermeldung, die sich auf unterschiedliche Layer eines Schichtenmodells

beziehen.

- Beschreiben Sie mögliche Verfahren, mit denen die drei genannten Fehler erkannt werden können.

4. Einige Beschäftigte beklagen sich, dass immer beim Betrieb der Klimaanlage das Netzwerk in einigen Büros „langsam“ wird. Es wird festgestellt, dass in diesen Büros vor wenigen Jahren Netzwerkleitungen (Anlage 4.pdf) verlegt wurden.

Informieren Sie Ihre Kundin, Frau Schreiber von der DarSys GmbH, durch eine E-Mail warum dieses Problem auftritt und wie dieses behoben werden kann.

Verwenden Sie für Ihre Lösung das Vorgabeblatt Anlage 10.pdf.



# Übungsaufgabe 2

Die Datenerfassung und Datenübertragung im Lager soll mithilfe von Handheld-Terminals und Notebooks in Echtzeit erfolgen.

1. Zur Errichtung der Netzwerkinfrastruktur sollen unter anderem bis zu acht Accesspoints angeschafft werden. An der Decke der Lagerhalle wurden an mehreren Stellen Netzwerkdosen, jedoch keine 230 V-Steckdosen, installiert. Es stehen mehrere Accesspoints zur Auswahl ([Anlage 5.pdf](#)).

- Schlagen Sie anhand von fünf Kriterien den passenden WLAN-Accesspoint-Typ vor.

2. Ihnen liegt der Grundriss des Lagers und das Antennendiagramm des von Ihnen gewählten

WLAN-Accesspoints bei Deckenmontage vor ([Anlage 6.pdf](#)).

- Bestimmen Sie im Grundriss bis zu acht Positionen der Accesspoints, mit denen das Lager optimal mit WLAN ausgeleuchtet ist.

3. Die WLAN-Accesspoints wurden geliefert und in der Lagerhalle montiert. Vor der Inbetriebnahme und Abnahme durch den Fahrradhersteller sollen diese zeitgemäß abgesichert werden.

- Beschreiben Sie drei zu bearbeitenden Sicherheitsaspekte.

4. Ihnen liegt in der Eingabeaufforderung die IP-Konfiguration eines WLAN-Devices vor ([Anlage 7.pdf](#)). Ein Zugriff auf das Internet von diesem Gerät ist nicht möglich.

- Begründen Sie, ob ein Zugriff über die IP-Adresse auf den Dateiserver möglich ist.
- Entwerfen Sie eine IP-Konfiguration, mit der ein Zugriff auf das Internet möglich ist.

# Dual-Stack