3. Schriftliche Wiederholung
Konsolidierte Folien

NETZWERKTECHNIK / SEMESTER 1 UND 2

1

Physical Layer

NETZWERKTECHNIK / SEMESTER 1 UND 2

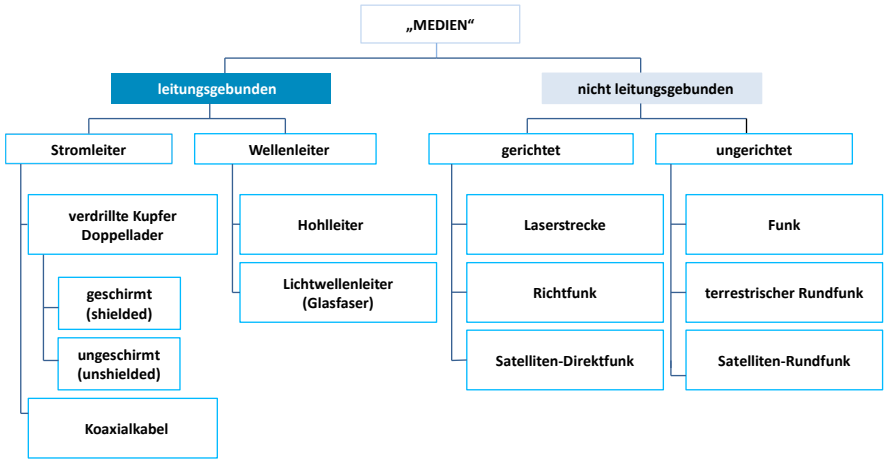
2

01

Allgemeines

3

Klassifikation der Medien



[Quelle: Vernetzte IT-Systeme 2. Übertragungstechnische Grundlagen, Hochschule Weserbergland, V. Langer, F. Schimanke]

4

NETZWERKTECHNIK / SEMESTER 1 und 2

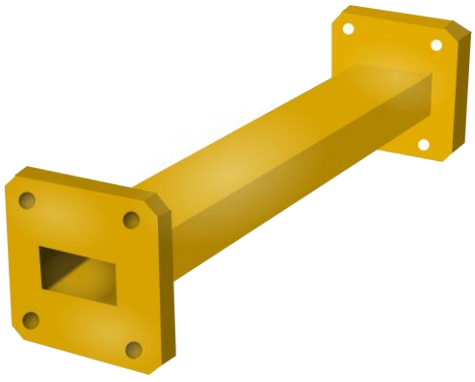
Richtfunk

tgm [Quelle: https://www.pandacomdirekt.de/fachwissen-netzwerktechnologien/detail/grundlagen-richtfunk.html - letzter Abruf 28.11.2025]

5

NETZWERKTECHNIK / SEMESTER 1 und 2

Hohlleiter

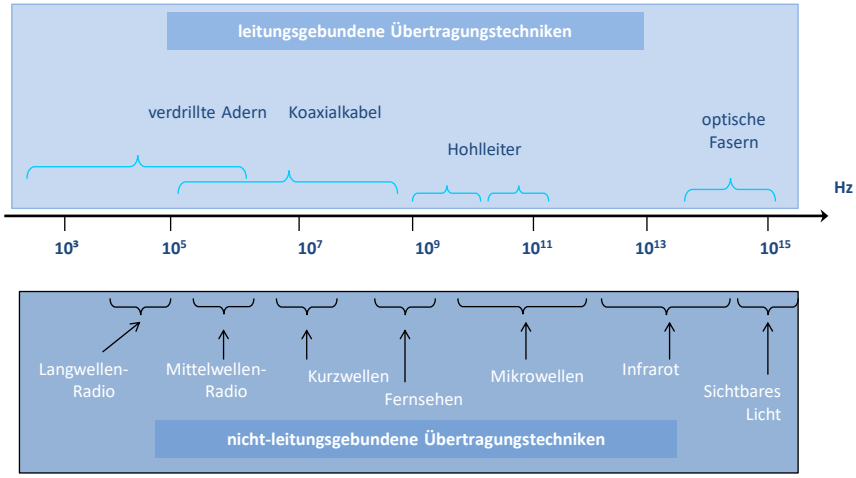


tgm [Quelle: https://de.wikipedia.org/wiki/Hohlleiter - letzter Abruf 28.11.2025]

6

NETZWERKTECHNIK / SEMESTER 1 und 2

Medien im elektromagnetischem Spektrum



[Quelle: Vernetzte IT-Systeme 2. Übertragungstechnische Grundlagen, Hochschule Weserbergland, V. Langer, F. Schimanke]

02

Kupferverkabelung

Eigenschaften der Kupferverkabelung

- Kupferverkabelung ist die **gebräuchlichste Art der Verkabelung**, die heute in Netzwerken verwendet wird. Es ist kostengünstig, einfach zu installieren und hat einen geringen Widerstand gegen den elektrischen Stromfluss.

Einschränkungen:

- **Dämpfung** – je länger die elektrischen Signale unterwegs sind, desto schwächer werden sie.
- Das elektrische Signal ist **anfällig für Störungen** aus zwei Quellen, die die Datensignale verzerren und verfälschen können: Elektromagnetische Interferenz (EMI), Radio Frequency Interference (RFI) und Übersprechen.

Maßnahmen:

- Die strikte Einhaltung der **Kabellängenbeschränkungen** verringert die Dämpfung.
- Einige Arten von Kupferkabeln mildern EMI und RFI durch **metallische Abschirmung und Erdung**.
- Einige Arten von Kupferkabeln schwächen das Übersprechen, indem sie gegensätzliche Schaltungspaardrähte miteinander **verdrillen**.

Kabeltypen

Unshielded Twisted-Pair (UTP) Cable

Shielded Twisted-Pair (STP) Cable

Coaxial Cable

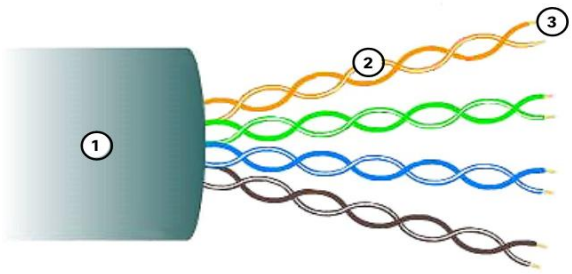
NETZWERKTECHNIK / SEMESTER 1 und 2

Unshielded Twisted Pair (UTP)

- UTP ist das **gebräuchlichste Netzwerkmedium**.
- Abschluss mit **RJ-45**-Anschlüssen
- Verbindet Hosts mit **zwischengeschalteten Netzwerkgerät**

Hauptmerkmale von UTP

1. Der **Außenmantel** schützt die Kupferdrähte vor physischer Beschädigungen.
2. **Twisted Pairs** schützen das Signal vor Störungen.
3. Eine **farbcodierte Kunststoffisolierung** isoliert die Drähte elektrisch voneinander und identifiziert jedes Paar.

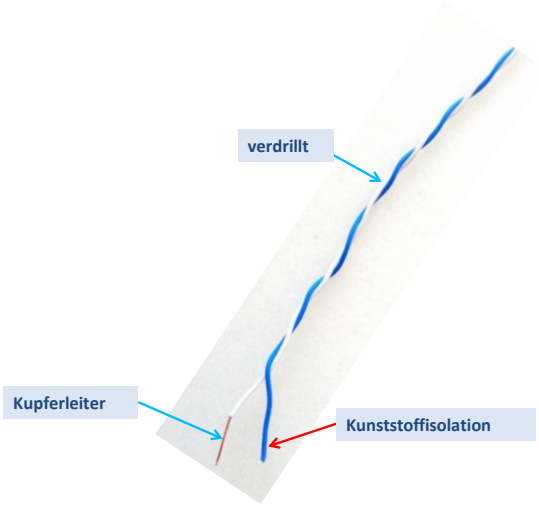


tgm [Quelle: CCNAv7: Introduction to Networks (ITN) Companion Guide, Cisco Press]

NETZWERKTECHNIK / SEMESTER 1 und 2

Kupfer Doppelader

- vielfältiger Einsatz in Telefon- und Datennetzen
- Leiterdurchmesser: 0,4 - 0,9 mm
- Bandbreite: einige 100 kHz bis ca. 600 MHz
- Fachbezeichnung: Unshielded Twisted Pair (UTP)
- verschiedene Qualitätsklassen, z. B. UTP 3, 4, 5, 6 bis zu 2,5 Gbit/s
- vollduplex (z.B. CAT 5)
- unterschiedliche Bauformen
- **Warum verdrillt => Kompensation der Induktion**

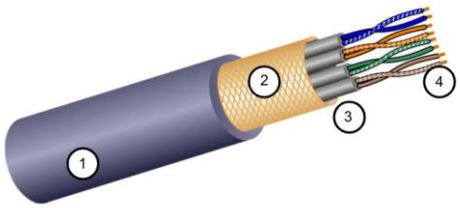


tgm [Quelle: Vernetzte IT-Systeme 2. Übertragungstechnische Grundlagen, Hochschule Weserbergland, V. Langer, F. Schimanke]

NETZWERKTECHNIK / SEMESTER 1 und 2

Shielded Twisted Pair (STP)

- Besserer Schutz gegen **Rauschen** als UTP
- **Teurer** als UTP
- **Schwieriger zu installieren** als UTP
- Abschluss mit **RJ-45-Anschlüssen**
- Verbindet Hosts mit **zwischengeschalteten Netzwerkgeräten**



Hauptmerkmale von STP

1. Der **Außenmantel** schützt die Kupferdrähte vor physischen Beschädigungen
2. **Geflochtene oder Folienabschirmung** bietet EMI/RFI-Schutz
3. **Folienabschirmung** für jedes Adernpaar bietet EMI/RFI-Schutz
4. Eine **farbcodierte Kunststoffisolierung** isoliert die Drähte elektrisch voneinander und identifiziert jedes Paar

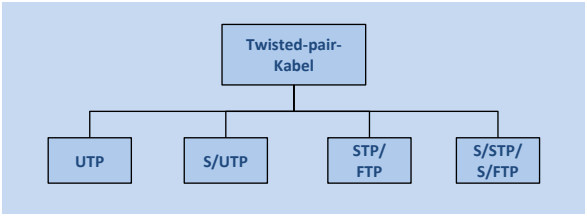
tgm [Quelle: CCNAv7: Introduction to Networks (ITN) Companion Guide, Cisco Press]

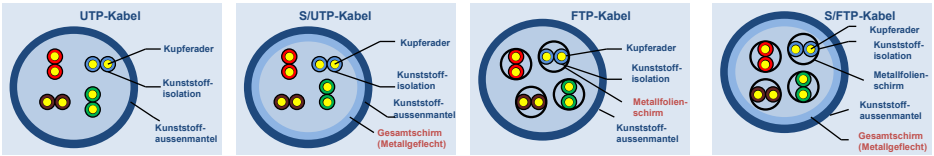
13

NETZWERKTECHNIK / SEMESTER 1 und 2

Twisted Pair Im Querschnitt

Warum Abschirmung => Kompensation elektromagnetischer Einflüsse von außen

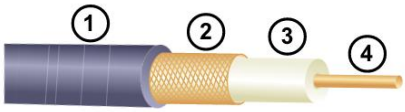




tgm [Quelle: Vernetzte IT-Systeme 2. Übertragungstechnische Grundlagen, Hochschule Weserbergland, V. Langer, F. Schimanke]

14

Koaxialkabel



Besteht aus folgenden Komponenten:

1. **Äußerer Kabelmantel**, um kleinere physische Schäden zu vermeiden
2. Ein **gewebtes Kupfergeflecht** oder eine Metallfolie fungiert als zweiter Draht in der Schaltung und als Abschirmung für den Innenleiter.
3. Eine Schicht aus **flexibler Kunststoffisolierung (Dielektrikum)**
4. Für die Übertragung der elektronischen Signale wird ein Kupferleiter verwendet.

- Es gibt **verschiedene Arten von Steckverbindern**, die mit Koaxialkabeln verwendet werden.
- Wird häufig in den folgenden Situationen verwendet:
- Drahtlose Installationen - Befestigen Sie **Antennen** an drahtlosen Geräten
- **Kabel-Internet**-Installationen - Verkabelung beim Kunden

tgm [Quelle: CCNAv7: Introduction to Networks (ITN) Companion Guide, Cisco Press]

15

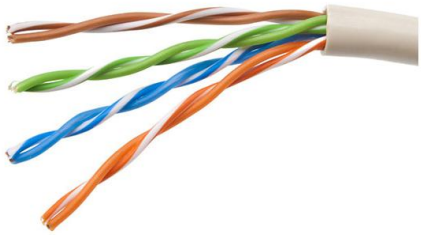
03

UTP

16

Eigenschaften von UTP Kabeln

- UTP besteht aus **vier Paaren farbcodierter Kupferdrähte**, die miteinander verdrillt und von einem flexiblen Kunststoffmantel ummantelt sind. Es wird keine Abschirmung verwendet. UTP stützt sich auf die folgenden Eigenschaften, um das Übersprechen zu begrenzen:
- **Cancellation** - Jeder Draht in einem Adernpaar verwendet eine entgegengesetzte Polarität. Ein Draht ist negativ, der andere ist positiv. Sie sind miteinander **verdreht und die Magnetfelder heben sich gegenseitig** und außerhalb von EMI/RFI effektiv auf.
- Variation der Verdrillungen pro cm in jedem Draht - **Jeder Draht wird unterschiedlich stark verdrillt**, was dazu beiträgt, ein Übersprechen zwischen den Drähten im Kabel zu verhindern.



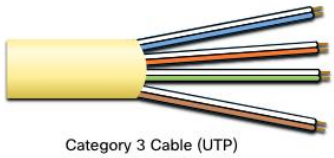
tgm [Quelle: CCNAv7: Introduction to Networks (ITN) Companion Guide, Cisco Press]

UTP Kategorien

Kategorie	Klasse laut ISO	Frequenzbereich	Anwendung/Dienst
Kategorie 2	Klasse A	100 kHz	Telefonie, Modem, DFÜ
Kategorie 3	Klasse B	1 MHz	ISDN, IBM-Verkabelung Typ 3
Kategorie 4	Klasse C	16 MHz	Token Ring, Ethernet
Kategorie 5	Klasse D	100 MHz	Fast Ethernet, Gigabit Ethernet
Kategorie 6	Klasse E	200 MHz	Fast Ethernet, Gigabit Ethernet
Kategorie 7	Klasse F	600 MHz	ATM, Gigabit Ethernet

tgm [Quelle: http://d.pcnews.at/ins/pcn/095/001800/main.htm (letzter Abruf 18.07.2025)]

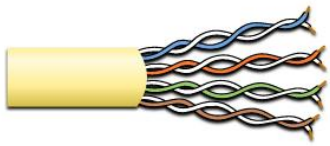
Standardisierungen und Stecker



Category 3 Cable (UTP)

Die Standards für UTP werden von der **TIA/EIA** festgelegt. TIA/EIA-568 standardisiert Elemente wie:

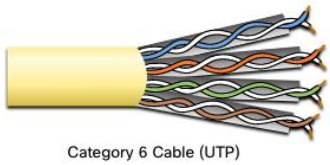
- Kabeltypen
- Kabellängen
- Verbinder
- Kabelabschluss
- Prüfmethoden



Category 5 and 5e Cable (UTP)

Elektrische Standards für Kupferkabel werden von der **IEEE** festgelegt, die Kabel nach ihrer Leistung bewertet. Beispiele hierfür sind:

- Kategorie 3(Cat 3)
- Kategorie 5 und 5e (Cat 5, 5e)
- Kategorie 6 (Cat 6)



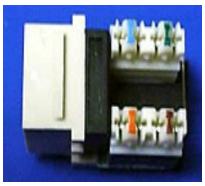
Category 6 Cable (UTP)

tgm [Quelle: CCNAv7: Introduction to Networks (ITN) Companion Guide, Cisco Press]

Standardisierungen und Stecker

RJ-45 Stecker

Schlecht abgeschlossenes UTP-Kabel



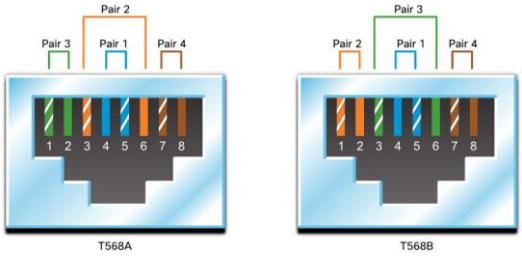
RJ-45 Socket

Ordnungsgemäß
abgeschlossenes UTP-Kabel

tgm [Quelle: CCNAv7: Introduction to Networks (ITN) Companion Guide, Cisco Press]

NETZWERKTECHNIK / SEMESTER 1 und 2

Straight-through und Crossover UTP Kabel



Typ	Standard	Anwendung
Ethernet Straight-through	Both ends T568A or T568B	Host zu Netzwerkgerät
Ethernet Crossover *	One end T568A, other end T568B	Host-zu-Host, Switch-zu-Switch, Router-zu-Router
* Gilt als Legacy, da die meisten Netzwerkkarten Auto-MDIX verwenden, um den Kabeltyp und die vollständige Verbindung zu erkennen		
Rollover	Cisco Proprietär	Serieller Anschluss des Host zum Router/Switch (meist mit Adapter)

tgm [Quelle: CCNAv7: Introduction to Networks (ITN) Companion Guide, Cisco Press]

04

Glasfaser

Eigenschaften der Glasfaserverkabelung

- **Nicht so häufig wie UTP** wegen der damit verbundenen Kosten
- Ideal für **bestimmte Netzwerkszenarien**
- Überträgt Daten über **größere Entfernungen** mit höherer Bandbreite als jedes andere Netzwerkmedium
- Weniger anfällig für **Dämpfung** und **völlig immun gegen EMI/RFI**
- Hergestellt aus flexiblen, **extrem dünnen Strängen aus sehr reinem Glas**
- Verwendet einen **Laser oder eine LED**, um Bits als **Lichtimpulse** zu kodieren
- Das Glasfaserkabel fungiert als **Wellenleiter**, um Licht mit minimalem Signalverlust zwischen den beiden Enden zu übertragen

tgm [Quelle: CCNAv7: Introduction to Networks (ITN) Companion Guide, Cisco Press]

Prinzip der LWL

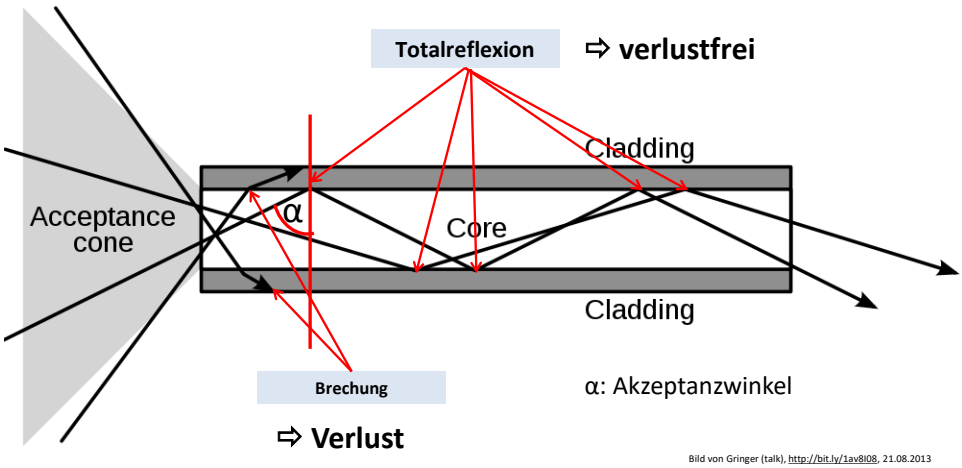


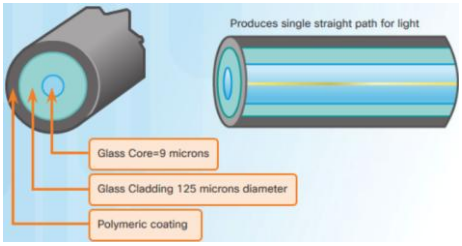
Bild von Gringer (talk), http://bit.ly/1av8l08, 21.08.2013

tgm [Quelle: Vernetzte IT-Systeme 2. Übertragungstechnische Grundlagen, Hochschule Weserbergland, V. Langer, F. Schimanke]

Typen von Glasfaser

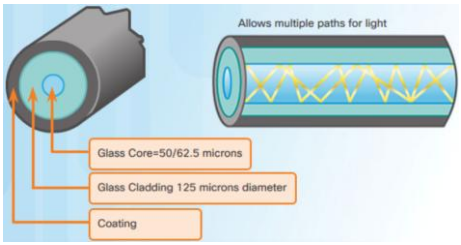
Unter **Dispersion** versteht man die **Ausbreitung eines Lichtimpulses über die Zeit**. Eine erhöhte Dispersion bedeutet einen erhöhten Verlust der Signalstärke. MMF hat eine größere Dispersion als SMF, wobei die maximale Kabelentfernung für MMF 550 Meter beträgt.

Single-Mode Fiber



- Sehr kleiner Kern
- Verwendet teure Laser
- Anwendungen über große Entfernungen

Multimode Fiber



- Größerer Kern
- Verwendet weniger teure LEDs
- LEDs senden in verschiedenen Winkeln
- Bis zu 10 Gbit/s über 550 Meter

tgm [Quelle: CCNAv7: Introduction to Networks (ITN) Companion Guide, Cisco Press]

Was bedeutet mehrere Moden?

- **Mehrere Moden in einer Glasfaser bedeuten, dass ein Lichtsignal nicht nur auf einem einzigen Weg, sondern auf verschiedenen Ausbreitungswegen durch die Faser läuft.**

Bei einem einfachen digitalen Signal (z. B. eine Folge von 1 und 0) passiert Folgendes:

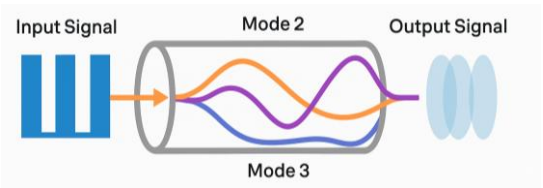
Beispiel: Digitales Signal in Multimode-Faser

- Du sendest ein Rechtecksignal (z. B. 101010).
- Dieses Signal wird als Lichtimpulse in die Faser eingespeist.
- In einer Multimode-Faser breitet sich jeder Impuls gleichzeitig in mehreren Moden aus:
  - Mode 1: kürzester Weg (fast gerade durch den Kern).
  - Mode 2: etwas schräger, längerer Weg.
  - Mode 3: noch schräger, noch längerer Weg.

Ergebnis: Die Lichtimpulse kommen zeitlich versetzt am Ende der Faser an, weil die Wege unterschiedlich lang sind.

Folge: Modendispersion

- Die ursprünglich scharfen Impulse „verschmieren".
- Aus einem klaren Signal wie 101010 wird am Ende etwas wie 1__0_1_0__10 (Überlappung).
- Je länger die Faser und je mehr Moden, desto stärker die Verzerrung → begrenzte Bandbreite.



tgm [Quelle: CCNAv7: Introduction to Networks (ITN) Companion Guide, Cisco Press]

Nein, Mode bedeutet nicht die Übertragung mehrerer digitaler Signale gleichzeitig.

Es geht nicht um parallele Datenströme, sondern um verschiedene Ausbreitungswege desselben Signals innerhalb der Glasfaser.

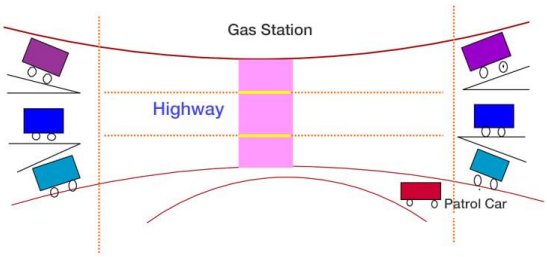
- Die Moden sind physikalische Eigenschaften der Faser, keine separaten Kanäle für unabhängige Daten.
- Für mehrere unabhängige Signale würde man Multiplexing-Techniken verwenden (z. B. WDM – Wavelength Division Multiplexing), nicht die Moden.

Wichtige Punkte:

- Du sendest ein einziges digitales Signal (z. B. eine Bitfolge).
- In einer Multimode-Faser wird dieses Signal in mehreren Lichtmoden übertragen:
  - Jede Mode ist ein anderer Weg, den das Licht durch die Faser nimmt.
  - Alle Moden transportieren denselben Inhalt, aber sie kommen zu unterschiedlichen Zeiten an.
- **Das führt zu Modendispersion, nicht zu paralleler Datenübertragung.**
- **Multimode-Faser:** Ein Signal wird in mehreren Moden übertragen → gleiche Daten, aber unterschiedliche Wege → Verzerrung durch Modendispersion.
- **WDM:** Mehrere unabhängige Signale werden auf unterschiedlichen Wellenlängen gleichzeitig übertragen → parallele Datenübertragung ohne gegenseitige Verzerrung.

tgm [https://www.fibermall.com/de/blog/types-of-wavelength-division-multiplexing-wdm.htm?srsltid=AfmBOoqAjS9sqEM0Tr8vrxo2YdtxO_HdoA_Sz4lWVT3vzb5FVAzhePy3# - letzter Abruf 15.1.2026]

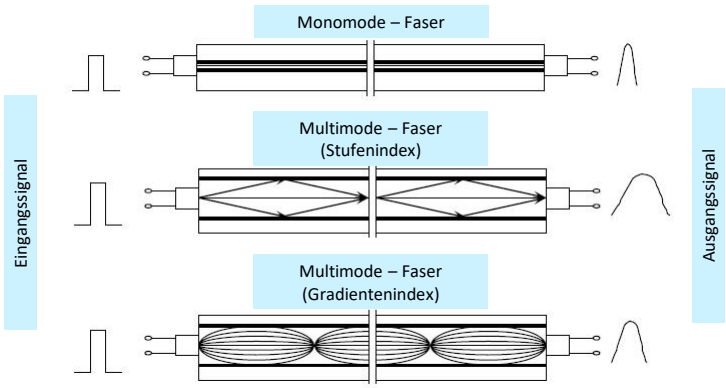
Funktionsprinzip von WDM



tgm [https://www.fibermall.com/de/blog/types-of-wavelength-division-multiplexing-wdm.htm?srsltid=AfmBOoqAjS9sqEM0Tr8vrxo2YdtxO_HdoA_Sz4lWVT3vzb5FVAzhePy3# - letzter Abruf 15.1.2026]

NETZWERKTECHNIK / SEMESTER 1 und 2

Pulsfervormung durch Dispersion



optische Dispersion

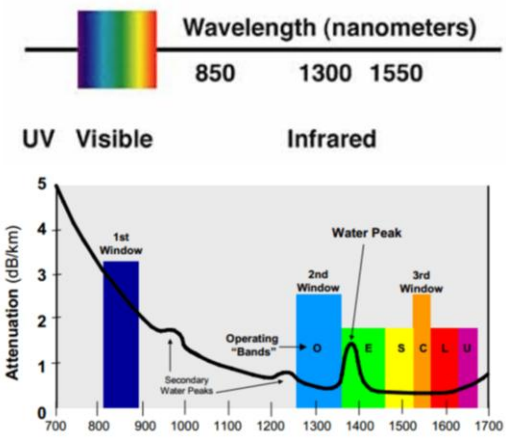
[Quelle: Vernetzte IT-Systeme 2. Übertragungstechnische Grundlagen, Hochschule Weserbergland, V. Langer, F. Schimanke]

29

NETZWERKTECHNIK / SEMESTER 1 und 2

Grundlagen der Wellenlänge

- Licht wird durch seine **Wellenlänge** definiert.
- Die Wellenlänge ist eine Zahl, die das **Spektrum des Lichts** darstellt. Jeder Frequenz oder Farbe des Lichts ist eine Wellenlänge zugeordnet.
- Die am häufigsten verwendeten Wellenlängen in Glasfasern sind: **850 nm, 1300 nm und 1550 nm.**
  - 850 nm und 1300 nm eignen sich für Multimode-Fasern,
  - 1310 nm und 1550 nm am besten für Singlemode-Fasern geeignet
- Zur Lichtausbreitung in optischen Fasern zählen auch **Laser und Leuchtdioden:**
  - **Laser** werden in Singlemode-Geräten mit Wellenlängen von **1310 nm oder 1550 nm** verwendet
  - **LEDs** in Multimode-Geräten mit Wellenlängen von **850 nm oder 1300 nm**



[https://ftthfiberoptic.com/de/what-is-the-wavelength-of-the-optical-fiber/ - letzter Abruf 15.1.2026]

30

Einsatzbereiche

Glasfaserkabel werden heute in vier Industriezweigen eingesetzt:

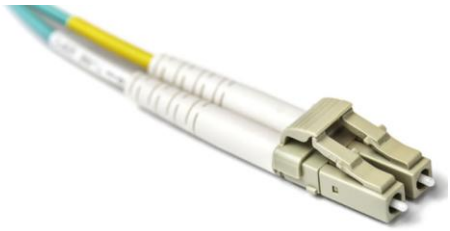
- **Unternehmensnetzwerke** – Wird für **Backbone** Verkabelung und die Verbindung von Infrastrukturgeräten verwendet
- **Fiber-to-the-Home (FTTH)** - Wird verwendet, um ständig verfügbare **Breitbanddienste** für Haushalte und kleine Unternehmen bereitzustellen
- **Langstreckennetze** - Werden von Dienstanbietern verwendet, um **Länder und Städte** zu verbinden
- **Unterseekabel** - Werden verwendet, um zuverlässige Hochgeschwindigkeitslösungen mit hoher Kapazität bereitzustellen, die in rauen Unterwasserumgebungen bis zu **transozeanischen Entfernungen** überleben können.

Stecker

Straight-Tip (ST) Connectors

Lucent Connector (LC) Simplex Connectors

Subscriber Connector (SC) Connectors



Duplex Multimode LC Connectors

Patchkabel

SC-SC MM Patch Cord

LC-LC SM Patch Cord

ST-LC MM Patch Cord

ST-SC SM Patch Cord

Eine gelber Mantel steht für **Singlemode-Glasfaserkabel** und Orange (oder Aqua) für **Multimode-Glasfaserkabel**.

tgm [Quelle: CCNAv7: Introduction to Networks (ITN) Companion Guide, Cisco Press]

Vergleich Glasfaser und Kupfer

- Glasfasern werden in erster Linie als Backbone-Verkabelung für stark frequentierte Punkt-zu-Punkt-Verbindungen verwendet
- Verbindungen zwischen Datenverteilungseinrichtungen und für die Vernetzung von Gebäuden
- In Campusumgebungen mit mehreren Gebäuden.

Eigenschaft	UTP Cabling	Fiber-Optic Cabling
Unterstützte Bandbreite	10 Mb/s - 10 Gb/s	10 Mb/s - 100 Gb/s
Entfernung	Relativ kurz(1 - 100 meters)	Relativ lang(1 - 100,000 meters)
Immunität gegen EMI und RFI	Niedrig	Hoch (Vollständig immun)
Immunität gegen elektrische Gefahren	Niedrig	Hoch (Vollständig immun)
Medien- und Konnektorkosten	Sehr Niedrig	Sehr Hoch
Erforderliche Installationskenntnisse	Sehr Niedrig	Sehr Hoch
Sicherheitsvorkehrungen	Sehr Niedrig	Sehr Hoch

tgm [Quelle: CCNAv7: Introduction to Networks (ITN) Companion Guide, Cisco Press]

05

Drahtlos

Eigenschaften von Drahtlosverbindungen

Er überträgt **elektromagnetische Signale**, die Binärziffern unter Verwendung von **Radio- oder Mikrowellenfrequenzen** darstellen. Dies bietet die größte Mobilitätsoption. Die Zahl der drahtlosen Verbindungen nimmt weiter zu.

Einige der Einschränkungen von Wireless:

- **Abdeckungsbereich** - Die effektive Abdeckung kann erheblich von den physischen Eigenschaften des Einsatzortes beeinflusst werden.
- **Interferenzen** - Wireless ist anfällig für Interferenzen und kann durch viele gängige Geräte gestört werden.
- **Sicherheit** - Die drahtlose Kommunikationsabdeckung erfordert keinen Zugriff auf einen physischen Medienstrang, sodass jeder Zugriff auf die Übertragung erhalten kann.
- **Shared Medium** – WLANs arbeiten im Halbduplex-Modus, was bedeutet, dass jeweils nur ein Gerät senden oder empfangen kann. Viele Benutzer, die gleichzeitig auf das WLAN zugreifen, führen zu einer reduzierten Bandbreite für jeden Benutzer.

tgm [Quelle: CCNAv7: Introduction to Networks (ITN) Companion Guide, Cisco Press]

Arten von Drahtlosverbindungen

Die IEEE- und Telekommunikationsindustriestandards für die drahtlose Datenkommunikation decken sowohl die Datenverbindungs- als auch die physikalische Schicht ab. In jeder dieser Normen wird für die physikalische Schicht vorgeschrieben:

- Methoden zur Codierung von Daten in Funksignale
- Frequenz und Leistung der Übertragung
- Anforderungen an den Signalempfang und die Dekodierung
- Antennendesign und –bau

Wireless-Standards:

- **Wi-Fi (IEEE 802.11)** - Wireless LAN (WLAN)-Technologie
- **Bluetooth (IEEE 802.15)** - Standard für Wireless Personal Area Network (WPAN)
- **WiMAX (IEEE 802.16)** – Verwendet eine Punkt-zu-Mehrpunkt-Topologie, zum drahtlosen Breitbandzugriff
- **Zigbee (IEEE 802.15.4)** - Kommunikation mit niedriger Datenrate und geringem Stromverbrauch, hauptsächlich für Anwendungen beim Internet der Dinge (IoT)

Erforderliche Komponenten

Generell werden für ein Wireless LAN (WLAN) folgende Geräte benötigt:

- **Wireless Access Point (AP)** - Bündeln die drahtlosen Signale von Benutzern und verbinden mit der vorhandenen kupferbasierten Netzwerkinfrastruktur
- **Wireless-NIC** – Wireless-Kommunikationsfunktionen beim Host
- Netzwerkadministratoren müssen **strenge Sicherheitsrichtlinien und -prozesse** entwickeln und anwenden, um WLANs vor unbefugtem Zugriff und Beschädigung zu schützen.

06

Strukturierte Verkabelung

39

Universelle Gebäudeverkabelung

- **„Strukturierte diensteneutrale Verkabelung“** – Betrieb des Netzwerkes professionell und kostengünstig
- Diensteneutral bedeutet das die Verkabelung unabhängig vom Dienst ist, der die Leitungswege benutzt.
- Unterstützung von: Computernetzwerk, Video, Telefon
- Gesamtkostensicht (TCO Total Cost of Ownership) – deutlich billiger als getrennte Verkabelungen
- Normen EN 50173-1 bzw. ISO/IEC 11801
  - **Primärbereich = Standortverkabelung**
    - Von einem Standortverteiler werden einzelne Gebäude angeschlossen (Backbone)
  - **Sekundärbereich = Gebäudeverkabelung**
    - Von einem Gebäudeverteiler werden einzelne Stockwerke angeschlossen
  - **Tertiärbereich = Etagenverteilung**
    - Von einem Etagenverteiler werden Steckdosen (TA = Technischer Anschluss) in den Büros angeschlossen
- **Übliche Topologie = Stern**

tgm [Quelle: CCNAv7: Introduction to Networks (ITN) Companion Guide, Cisco Press]

40

NETZWERKTECHNIK / SEMESTER 1 und 2

Universelle Gebäudeverkabelung

Motivation:

- die wachsende Anzahl vernetzter Computer in Unternehmen
- die zunehmende Mobilität der Anwender, z.B. durch Umstrukturierung des Unternehmens, Umzüge etc.
- die immer kürzer werdenden Innovationszyklen von Hard- und Software

Vorteile:

- **Nur einmal investieren** - alle weiteren Kosten für Änderungen und Services sind sehr gering.
- **Ohne Probleme umziehen** - universelle Anschlussdose RJ45 und vorausschauende, flächendeckende Verkabelung mit einheitlicher Anschlusstechnik
- **Flexibel reagieren auf Markterforderungen** - z.B. Umstrukturierungen im Unternehmen
- **Investitionsschutz** - alle Komponenten entsprechen den international genormten Standards.
- **Geringe Kosten für Wartung und Verwaltung** – nur ein sehr übersichtliches Netz verwaltet und gepflegt

tgm [Quelle: https://www.fischer-engstingen.de/strukturierte-verkabelung-nach-din-en-50173/ (letzter Abruf 18.07.2025)]

41

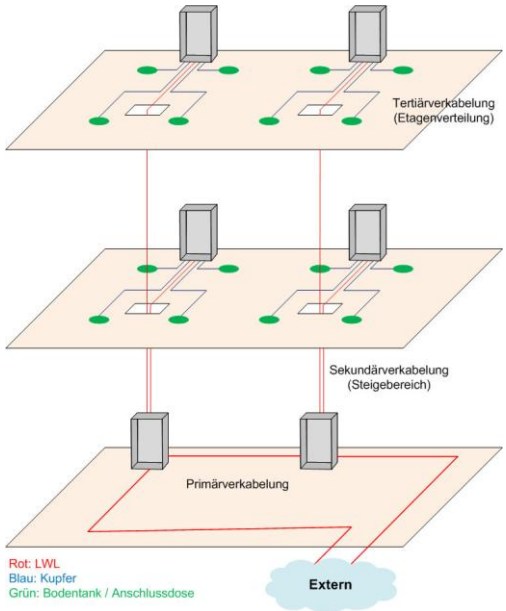
NETZWERKTECHNIK / SEMESTER 1 und 2

Standortverkabelung

Drei Bereiche:

- **Primär** = Gebäude zu Gebäude 900 – 1500 m
- **Sekundär** = Etagen zu Etagen <= 500 m
- **Tertiär** = Verteiler zu Endgeräten ~100 m

- Um im Fehlerfall Ausfälle zu minimieren müssen Reserveleitungen vorgesehen werden. Die Umschaltung erfolgt dann über aktive Komponenten im Netzwerk wie Switches und Router



tgm [Quelle: https://www.fischer-engstingen.de/strukturierte-verkabelung-nach-din-en-50173/ (letzter Abruf 18.07.2025)]

42

NETZWERKTECHNIK / SEMESTER 1 und 2

Primär, Sekundär und Tertiärverkabelung

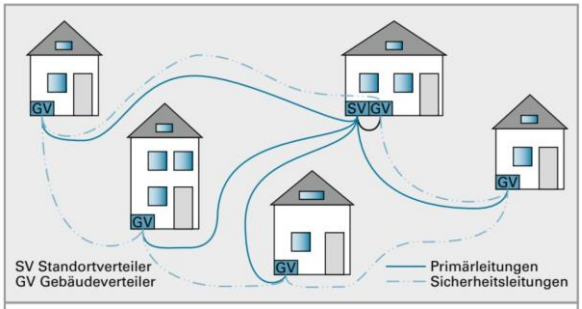


Bild 2.11: Primärverkabelung, Standortverkabelung

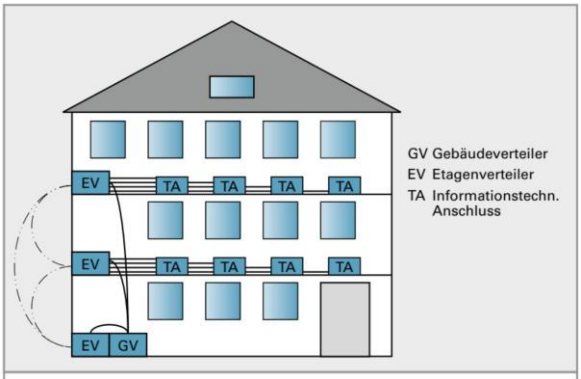


Bild 2.12: Sekundär- und Tertiärverkabelung im Gebäude und auf der Etage

tgm [Quelle: Fachwissen Netzwerktechnik, 4. Auflage, Kapitel 1, Europathek]

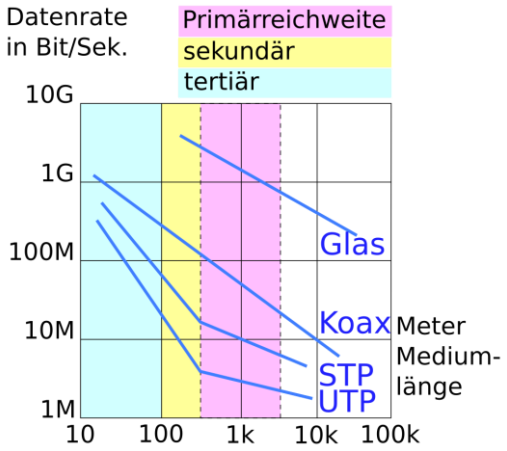
43

NETZWERKTECHNIK / SEMESTER 1 und 2

Medien in der strukturierten Verkabelung

Drei Bereiche:

- **Primär** = Gebäude zu Gebäude
  - Glasfaserkabel: 2.000 m
  - Twisted-Pair-Kabel mit VDSL-Modems: 900 m (bei 26 MB/s)
- **Sekundär** = Etagen zu Etagen
  - Glasfaserkabel: 2.000 m
  - Twisted-Pair-Kabel: 100 m
- **Tertiär** = Verteiler zu Endgeräten
  - Glasfaserkabel: 2.000 m
  - Twisted-Pair-Kabel: 100 m (davon 90 m Installationskabel und 10 m Patchkabel vorgesehen)



tgm [Quelle: https://de.wikipedia.org/wiki/Strukturierte_Verkabelung (letzter Abruf 18.07.2025)]

44

Strukturierte Verkabelung – Erweiterter Stern

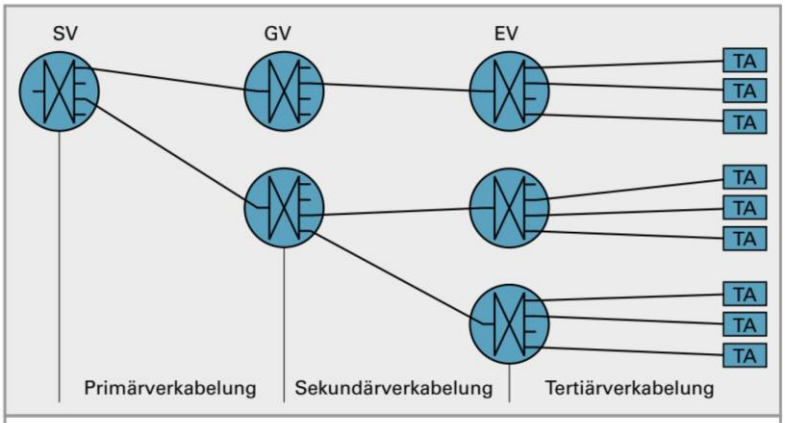


Bild 2.13: Strukturierte Verkabelung – Erweiterter Stern

[Quelle: Fachwissen Netzwerktechnik, 4. Auflage, Kapitel 1, Europathek]

Strukturierte Verkabelung – Netzanwendungsklassen und Leitungskategorien

Tabelle 2.1: Netzanwendungsklassen

Klasse	Frequenzbereich	Anwendungen
A	≤ 100 kHz	niederfrequente Anwendungen (z. B. Telefon, Fax)
B	≤ 1 MHz	Anwendungen mit niedriger Bitrate (z. B. ISDN)
C	≤ 16 MHz	Anwendungen mit hoher Bitrate (z. B. Ethernet)
D	≤ 100 MHz	Anwendungen mit sehr hoher Bitrate (z. B. Fast-Ethernet oder Gigabit-Ethernet)
E	≤ 250 MHz	Anwendungen mit sehr hoher Bitrate (z. B. Fast-Ethernet, Gigabit-Ethernet oder 10-Gigabit-Ethernet, Kabelfernsehen)
E_A	≤ 500 MHz	Anwendungen mit sehr hoher Bitrate (z. B. Fast-Ethernet, Gigabit-Ethernet oder 10-Gigabit-Ethernet, Kabelfernsehen)
F	≤ 600 MHz	reserviert für künftige Anwendungen
F_A	≤ 1000 MHz	reserviert für künftige Anwendungen

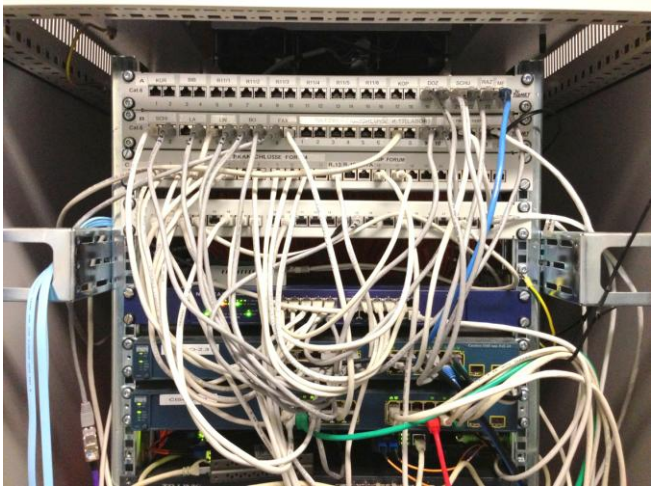
Tabelle 2.3: Leitungs-Kategorien

Kategorie	Frequenzbereich	Anwendung	geeignet für Klasse
3	≦ 16 MHz	Telefon, Token-Ring, Ethernet	C
5	≦ 100 MHz	Fast Ethernet, Gigabit-Ethernet	D
6	≦ 250 MHz	Gigabit-Ethernet, 10-Gigabit-Ethernet	D, E
6_A	≦ 625 MHz	Gigabit-Ethernet, 10-Gigabit-Ethernet	D, E, E_A
6_E	≦ 500 MHz	Gigabit-Ethernet, 10-Gigabit-Ethernet	D, E, E_A
7	≦ 600 MHz	10-Gigabit-Ethernet, Kabelfernsehanlagen	D, E, E_A, F
7_A	≦ 1000 MHz	10-Gigabit-Ethernet, Kabelfernsehanlagen	D, E, E_A, F, F_A

[Quelle: Fachwissen Netzwerktechnik, 4. Auflage, Kapitel 1, Europathek]

NETZWERKTECHNIK / SEMESTER 1 und 2

Beispiel Verteilerschrank



[Quelle: Vernetzte IT-Systeme 2. Übertragungstechnische Grundlagen, Hochschule Weserbergland, V. Langer, F. Schimanke]

NETZWERKTECHNIK / SEMESTER 1 und 2

Beispiel Anforderung Verteilerschrank

19" DV-Schrank

- 80cm x 100cm
- 42 HE
- mit Käfigmuttern
- M5-Kreuzschlitzschrauben
- von vorn und hinten zugänglich
- Platzreserve vorsehen

LWL-Anbindung

- grün - monomode APC / 8° (E2000)
- grau oder blau - multimode PC
- DWDM, passiv, 10G monomode

Schrankkontrolle

- Nur nach Anforderung

DV-Schrank mit Access-Technik

- 25% Platzreserve

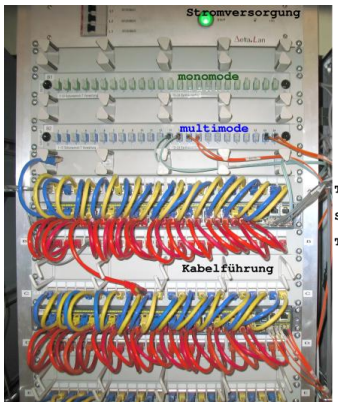
Eltschrank als DV-Verteiler

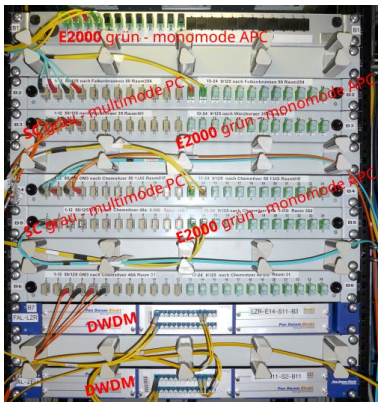
- Unterputz Eltverteiler mit Schließzylinder und Lüftermodul. Patch-Panel und Switch sind vertikal verbaut aufgrund der geringen Tiefe.

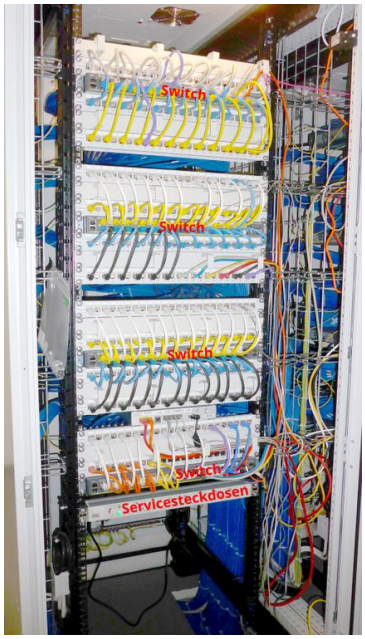
[Quelle: https://tu-dresden.de/zih/dienste/info-netz/richtlinien/dv-schrank (letzter Abruf 18.07.2025)]

NETZWERKTECHNIK / SEMESTER 1 und 2

Beispiel Verteilerschrank







tgm [Quelle: https://tu-dresden.de/zih/dienste/info-netz/richtlinien/dv-schrank (letzter Abruf 18.07.2025)]

49

Sicherungsschicht

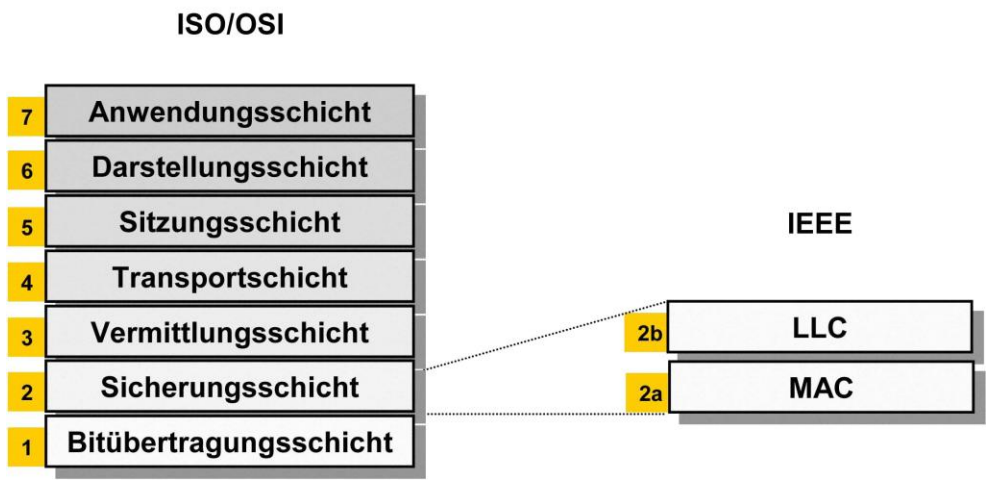
NETZWERKTECHNIK / SEMESTER 1 UND 2

50

01

Zweck der Sicherungsschicht

Einordnung im ISO/OSI Modell

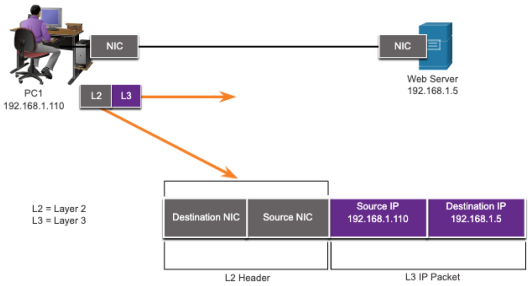


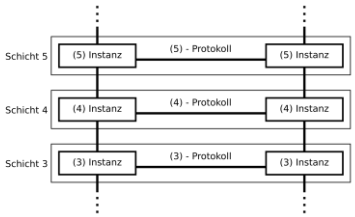
[Quelle: https://www.airnet.de/cr1-gfe/de/html/TrFddiIEEE802_learningObject6.xml - letzter Abruf 21.07.2025]

NETZWERKTECHNIK / SEMESTER 1 und 2

Die Sicherungsschicht

- Die Datenverbindungsschicht ist für die **Kommunikation zwischen den Netzwerkkarten der Endgeräte** verantwortlich.
- Es ermöglicht Protokollen der oberen Schicht den Zugriff auf die Medien der Bitübertragungsschicht und **kapselt Layer-3-Pakete (IPv4 und IPv6) in Layer-2-Frames**.
- Es führt auch eine **Fehlererkennung** durch und lehnt beschädigte Frames ab.





tgm [Quelle: Introduction to Networks v7.0 (ITN), Cisco Systems]

53

NETZWERKTECHNIK / SEMESTER 1 und 2

Standardisierung der Sicherungsschicht

Protokolle der Sicherungsschicht werden von technischen Organisationen definiert:

- Institut für Elektro- und Elektronikingenieure (IEEE) z.B. Ethernet
- Internationale Fernmeldeunion (ITU) z.B. ISDN
- Internationale Organisationen für Normung (ISO) z.B. HDLC
- Amerikanisches Nationales Normungsinstitut (ANSI) z.B. BacNet

tgm [Quelle: Introduction to Networks v7.0 (ITN), Cisco Systems]

54

Medienzugriff

Pakete, die zwischen Knoten ausgetauscht werden, können zahlreiche Sicherungsschichten und Medienübergänge erfahren.

Bei jedem Hop entlang des Pfads führt ein Router vier grundlegende Layer-2-Funktionen aus:

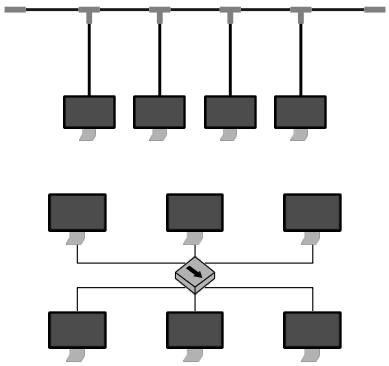
1. Akzeptiert einen Frame vom Netzwerkmedium.
2. Entkapselt den Frame, um das gekapselte Paket verfügbar zu machen.
3. Kapselt das Paket erneut in einen neuen Frame.
4. Leitet den neuen Frame auf dem Medium des nächsten Netzwerksegments weiter.

Direktverbindungsnetze

- d. h. **alle angeschlossenen Knoten sind direkt erreichbar und werden mittels einfacher Adressen der Schicht 2 identifiziert**
- es findet **keine Vermittlung** statt,
- eine **einfache Weiterleitung** (in Form von „Bridging“ oder „Switching“) ist aber möglich.

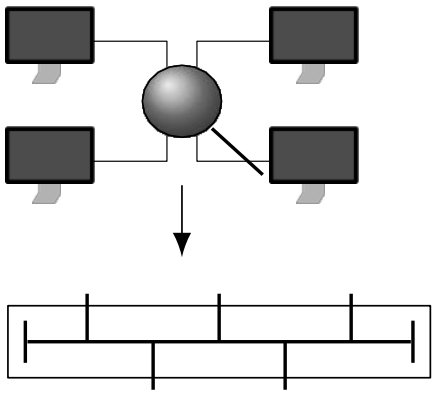
<u>Beispiele:</u>

- einzelne lokale Netzwerke (hier Verbindung mittels Bus / Hub, aber auch mittels Switch möglich)
- Verbindung zwischen Basisstation und Mobiltelefon
- Bus-Systeme innerhalb eines Computers, z. B. USB, PCIe etc.



Medienzugriff

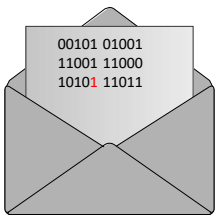
- Hubs z. B. erzeugen nur auf den ersten Blick eine Sterntopologie
- Intern werden alle angeschlossenen Computer zu einem Bus verbunden
- **Gleichzeitiges Senden von zwei Stationen führt zu Kollisionen und daher zum Verlust von Nachrichten**



tgm [Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), TU München, Prof. Dr.-Ing. Georg Carle]

Prüfung

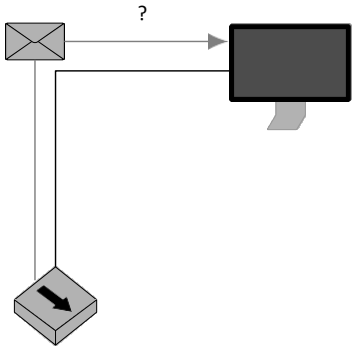
- Trotz Kanalkodierung treten **Übertragungsfehler** auf
- Diese müssen erkannt werden
- **Defekte Nachrichten werden nicht an höhere Schichten weitergegeben**
- **Die Wiederholung einer Übertragung ist häufig Aufgabe höherer Schichten**



tgm [Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), TU München, Prof. Dr.-Ing. Georg Carle]

Addressierung

- Eine Nachricht kann von vielen Knoten empfangen werden, z. B. bei Bus-Verbindungen oder Funknetzwerken
- Der jeweilige Empfänger muss entscheiden können, ob eine Nachricht für ihn bestimmt ist



tgm [Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), TU München, Prof. Dr.-Ing. Georg Carle]

59

02

Topologien

60

60

Physikalische und logische Topologien

- Die Topologie eines Netzwerks ist die Anordnung und Beziehung der Netzwerkgeräte und die Verbindungen zwischen ihnen.
- Es gibt zwei Arten von Topologien, die beim Beschreiben von Netzwerken verwendet werden:
  - **Physische Topologie** – zeigt physische Verbindungen und wie Geräte miteinander verbunden sind.
  - **Logische Topologie** – identifiziert die virtuellen Verbindungen zwischen Geräten mithilfe von Geräteschnittstellen und IP-Adressierungsschemata.

WAN Topologien

Es gibt drei gängige physische WAN-Topologien:

- **Punkt-zu-Punkt** – die einfachste und gebräuchlichste WAN-Topologie. Besteht aus einer permanenten Verknüpfung zwischen zwei Endpunkten.
- **Hub and Spoke** – ähnlich einer Sterntopologie, bei der ein zentraler Standort Zweigstellen über Punkt-zu-Punkt-Verbindungen miteinander verbindet.
- **Mesh** – bietet hohe Verfügbarkeit, erfordert jedoch, dass jedes Endsystem mit jedem anderen Endsystem verbunden ist.

NETZWERKTECHNIK / SEMESTER 1 und 2

Point-to-Point WAN Topologie

- Physische **Punkt-zu-Punkt**-Topologien verbinden zwei Knoten direkt.
- Die Knoten dürfen die **Medien nicht für andere Hosts freigeben**.
- Da alle Frames auf dem Medium nur zu oder von den beiden Knoten übertragen werden können, können **Punkt-zu-Punkt-WAN-Protokolle sehr einfach** sein.

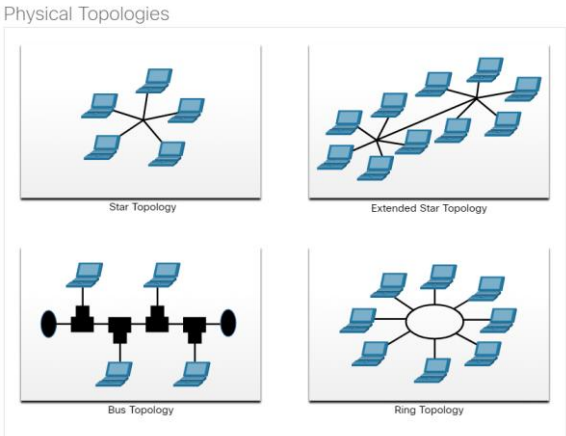
tgm [Quelle: Introduction to Networks v7.0 (ITN), Cisco Systems]

63

NETZWERKTECHNIK / SEMESTER 1 und 2

LAN Topologien

- Endgeräte in LANs werden in der Regel über eine **Stern- oder Extended-Stern-Topologie** miteinander verbunden.
- Stern- und erweiterte Sterntopologien sind einfach zu installieren, sehr skalierbar und leicht zu beheben.
- Frühe Ethernet- und Legacy-Token-Ring-Technologien bieten zwei zusätzliche Topologien:
  - **Bus** – Alle Endsysteme, die miteinander verkettet und an jedem Ende abgeschlossen sind.
  - **Ring** – Jedes Endsystem ist mit seinen jeweiligen Nachbarn verbunden, um einen Ring zu bilden.



tgm [Quelle: Introduction to Networks v7.0 (ITN), Cisco Systems]

64

03

Medienzugriff

65

Übertragungsrichtung

- **Halbduplex-Kommunikation**
  - Es kann jeweils nur ein Gerät auf einem freigegebenen Medium senden oder empfangen.
  - Wird in WLANs und Legacy-Bustopologien mit Ethernet-Hubs verwendet.
- **Vollduplex-Kommunikation**
  - Ermöglicht beiden Geräten das gleichzeitige Senden und Empfangen auf einem gemeinsam genutzten Medium.
  - Ethernet-Switches arbeiten im Vollduplex-Modus.

tgm [Quelle: Introduction to Networks v7.0 (ITN), Cisco Systems]

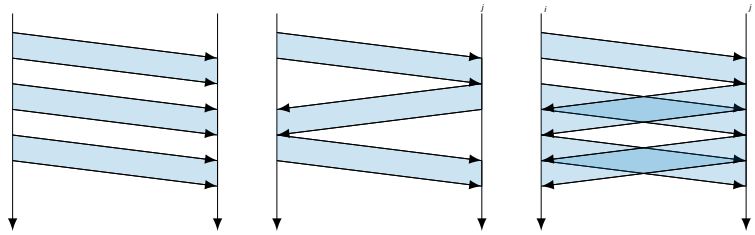
66

NETZWERKTECHNIK / SEMESTER 1 und 2

Halb- und Voll-Duplex Kommunikation

Die Art der Verbindung hängt dabei ab von

- den Fähigkeiten des Übertragungskanals,
- dem Medienzugriffsverfahren und
- den Anforderungen der Kommunikationspartner.



(a) Simplex **(b) Halbduplex** **(c) Vollduplex**

tgm [Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), TU München, Prof. Dr.-Ing. Georg Carle]

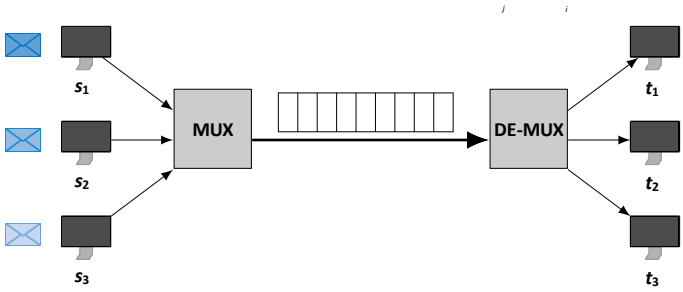
NETZWERKTECHNIK / SEMESTER 1 und 2

Mehrfachzugriff (Multiplexing)

Häufig ist es von Vorteil, **Nachrichten unterschiedlicher Teilnehmer gemeinsam über eine Leitung zu übertragen**:

- **Einfaches Beispiel:** Werden mehrere Computer mittels eines Hubs miteinander verbunden, so bildet der Hub ein gemeinsames geteiltes Medium, auf das die Computer mittels eines nicht-deterministischen Medienzugriffsverfahrens abwechselnd zugreifen.

<u>Deterministisches Zeitmultiplex-Verfahren:</u>



tgm [Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), TU München, Prof. Dr.-Ing. Georg Carle]

NETZWERKTECHNIK / SEMESTER 1 und 2

Übersicht über Multiplex-Verfahren

- **Zeitmultiplex (Time Division Multiplex, TDM)**
  - Deterministische Verfahren z. B. im Telefonnetz, bei ISDN-Verbindungen und im Mobilfunk
  - Nichtdeterministische Verfahren (konkurrierender Zugriff) in paketbasierten Netzwerken (z. B. Ethernet, WLAN)
- **Frequenzmultiplex (Frequency Division Multiplex, FDM)**
  - Aufteilung des Kanals in unterschiedliche Frequenzbänder (spektrale Zerlegung) und Zuweisung der Frequenzbänder an Kommunikationspartner.
  - Omnipräsent bei Funkübertragungen (z. B. unterschiedliche Radiosender)
  - Einsatz bei Glasfaserübertragungen („Modes“ mit unterschiedlicher Farbe)
  - Koexistenz von ISDN und DSL auf derselben Leitung

tgm [Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), TU München, Prof. Dr.-Ing. Georg Carle]

69

NETZWERKTECHNIK / SEMESTER 1 und 2

Übersicht über Multiplex-Verfahren

- **Raummultiplex (Space Division Multiplex, SDM)**
  - Verwendung mehrerer paralleler Übertragungskanäle.
  - „Kanalbündelung“ (Link Aggregation) bei Ethernet
  - MIMO (Multiple-In Multiple-Out) bei kabellosen Übertragungen (Verwendung mehrerer Antennen schafft mehrere Übertragungskanäle)
- **Codemultiplex (Code Division Multiplex, CDM)**
  - Verwendung orthogonaler Alphabete und Zuweisung der Alphabete an Kommunikationspartner.
  - Die Mobilfunktechnologie UMTS repräsentiert eine Variante von CDMA

tgm [Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), TU München, Prof. Dr.-Ing. Georg Carle]

70

NETZWERKTECHNIK / SEMESTER 1 und 2

TDM (Time Division Multiplexing)

- Die zur Verfügung stehende Ressource „Zeit“ wird auf mehrere Aufgaben aufgeteilt
- Die Zeit in der ein einzelner Kanal durchgeschaltet wird die **Kanaldauer t_c** oder auch Zeitschlitz (slot time) genannt.
- Bei n Kanälen ist die **Rahmenzeit $t_f = n * t_c$**
- Stationen die keine Daten zum übertragen haben belegen trotzdem einen Zeitschlitz

=> **Verbesserung durch asynchrones Zeitmultiplex**

- Kanäle nicht nach festem Zeitraster sondern nach Bedarf durchgeschaltet
- Zeitschlitze werden mit einer Kanalkennung versehen => Header

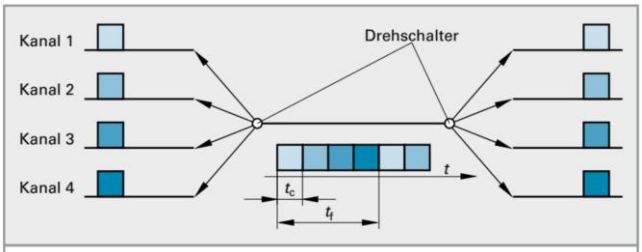


Bild 1.27: Zeitmultiplex mit festem Zeitraster

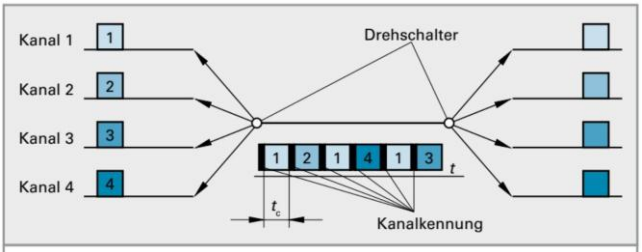


Bild 1.28: Asynchrones Zeitmultiplex

NETZWERKTECHNIK / SEMESTER 1 und 2

FDM (Frequency Division Multiplexing)

- Verfügung stehende Bandbreite des Mediums oder Übertragungskanals wird in mehrere Teilbereiche aufgeteilt
- **Beispiel**: Radio mit verschiedenen Sendefrequenzen der Stationen innerhalb eines Frequenzbandes
- Jedem Kanal zugewiesene Bandbreite wird als **Kanalbandbreite f_{ch}** bezeichnet
- Die Kanäle haben einen „Sicherheitsabstand“ den **Kanalabstand f_s** zueinander.

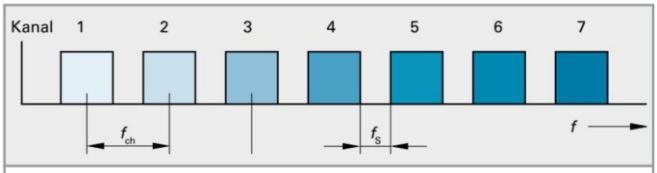


Bild 1.29: Frequenzmultiplex

NETZWERKTECHNIK / SEMESTER 1 und 2

SDM (Space Division Multiplexing)

- Verfügung stehender Raum in verschiedene Bereiche für die verschiedenen Kanäle aufgeteilt
- **Beispiel:** Mobilfunk Basisstation mit mehreren Funkzellen
- Funkzellen benachbarter Basisstationen können bzw. sollen sich überlappen damit keine Funklöcher auftreten

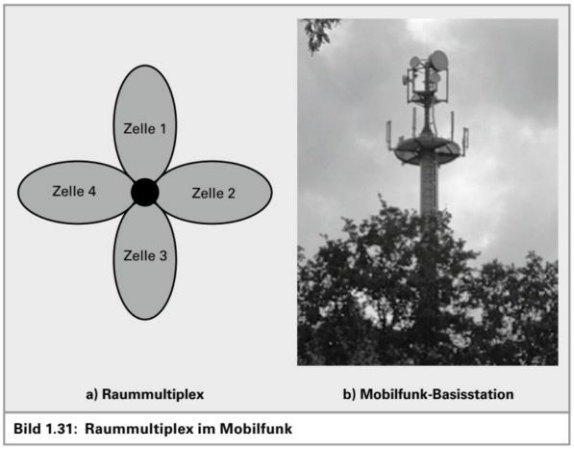


Bild 1.31: Raummultiplex im Mobilfunk

tgm [Quelle: Fachwissen Netzwerktechnik, 4. Auflage, Kapitel 1, Europathek]

NETZWERKTECHNIK / SEMESTER 1 und 2

CDM (Code Division Multiplexing)

- Bei **Funkübertragungen** um mehrere Funkkanäle gleichzeitig auf derselben Frequenz zu übertragen (UMTS, LTE, CDMA, …)
- Die zu sendenden Datenbits werden vor dem Senden mit **Code Sequenzen** verknüpft
- Beim Empfangen wieder mittels gleicher Code-Sequenzen zurückgewonnen
- Der **Chipcode** wird bitweise mit den Datenbits multipliziert
- $z_{i,m} = d_i \cdot c_m$

Beispiel Chipcode: +1 -1 +1 +1 -1 +1 +1 +1

HIGH-Datenbit = +1 -1 +1 +1 -1 +1 +1 +1

LOW-Datenbit = -1 +1 -1 -1 +1 -1 -1 -1 (also invertiert)

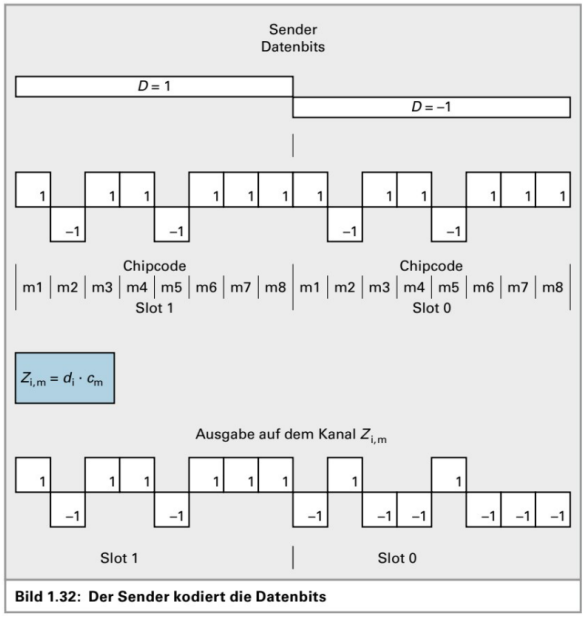


Bild 1.32: Der Sender kodiert die Datenbits

tgm [Quelle: Fachwissen Netzwerktechnik, 4. Auflage, Kapitel 1, Europathek]

CDM (Code Division Multiplexing)

Jedem Kanal wird ein anderer Chipcode zugewiesen. Senden mehrere Kanäle gleichzeitig so überlagern sich die Signale.

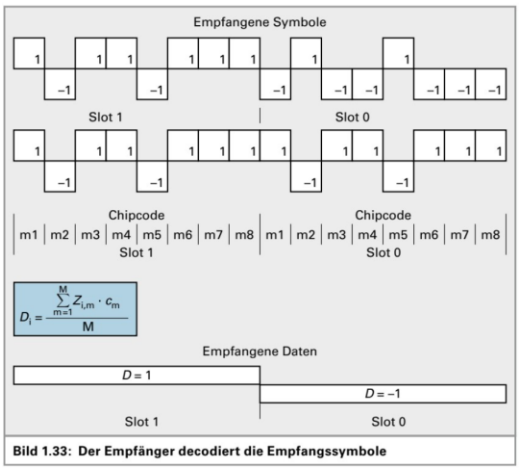


Bild 1.33: Der Empfänger decodiert die Empfangssymbole

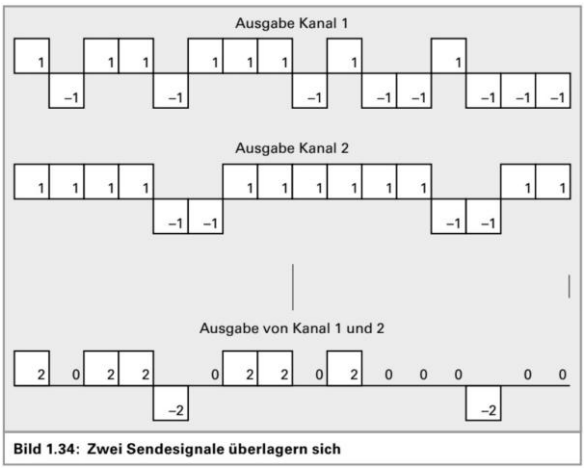
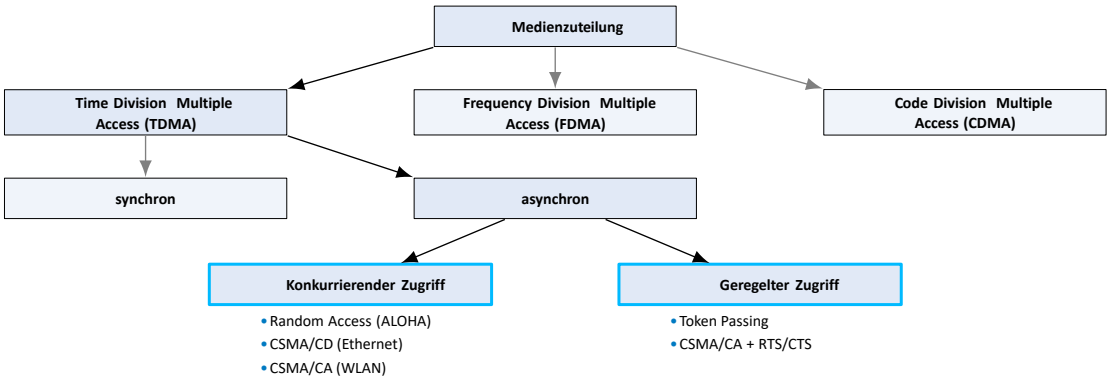


Bild 1.34: Zwei Sendesignale überlagern sich

tgm [Quelle: Fachwissen Netzwerktechnik, 4. Auflage, Kapitel 1, Europathek]

Mehrfachzugriff und Medienzugriffskontrolle

Einige der (statistischen) Multiplexing-Verfahren eignen sich auch als Mehrfachzugriffsverfahren:



tgm [Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), TU München, Prof. Dr.-Ing. Georg Carle]

NETZWERKTECHNIK / SEMESTER 1 und 2

Medienzugriff

- **Konkurrierender Zugriff (Contention-based access)**
  - Alle Knoten, die im Halbduplex-Modus arbeiten und um die Nutzung des Mediums konkurrieren.
    - **Carrier Sense Multiple Access mit Collision Detection (CSMA/CD)**, wie bei Ethernet verwendet
    - **Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)**, wie in Wireless LANs verwendet
- **Geregelter Zugriff (Controlled Access)**
  - Deterministischer Zugriff, bei dem **jeder Knoten seine eigene Zeit auf dem Medium hat**.
  - Wird in älteren Netzwerken wie **Token Ring und ARCNET** verwendet.

NETZWERKTECHNIK / SEMESTER 1 und 2

Contention-Based Access – CSMA/CD

- Wird von älteren **Ethernet-LANs** verwendet.
- Arbeitet im **Halbduplex-Modus**, bei dem jeweils nur ein Gerät sendet oder empfängt.
- Verwendet einen **Kollisionserkennungsprozess, um zu steuern, wann ein Gerät senden kann,** und was passiert, wenn mehrere Geräte gleichzeitig senden.

Prozess der CSMA/CD-Kollisionserkennung:

1. Geräte, die gleichzeitig senden, führen zu einer Signalkollision auf den gemeinsam genutzten Medien.
2. Geräte erkennen die Kollision.
3. Geräte warten eine zufällige Zeit und übertragen Daten erneut.

Contention-Based Access – CSMA/CA

- Wird von **IEEE 802.11 WLANs** verwendet.
- Arbeitet im **Halbduplex-Modus**, bei dem jeweils nur ein Gerät sendet oder empfängt.
- Verwendet einen **Kollisionsvermeidungsprozess, um zu steuern, wann ein Gerät senden kann,** und was passiert, wenn mehrere Geräte gleichzeitig senden.

CSMA/CA-Kollisionsvermeidungsprozess:

1. Bei der Übertragung **beziehen Geräte auch die Zeitdauer mit ein**, die für die Übertragung benötigt wird.
2. Andere Geräte auf dem freigegebenen Medium erhalten die Informationen zur Zeitdauer und **wissen, wie lange das Medium nicht verfügbar sein wird.**

79

Medienzugriff

Bewertungskriterien für Medienzugriffsverfahren sind unter anderem:

- **Durchsatz**, d. h. Gesamtanzahl an Nachrichten pro Zeiteinheit, die übertragen werden können
- **Verzögerung** für einzelne Nachrichten
- **Fairness** zwischen Teilnehmern, die sich dasselbe Medium teilen
- **Implementierungsaufwand** für Sender und Empfänger

Problem bei synchronem TDMA

- Der Kanal **wird statisch zwischen Teilnehmern aufgeteilt**
- **Datenverkehr ist aber stossartig** bzw. **burst-artig**, d. h. ein Teilnehmer überträgt kurz mit hoher Bandbreite und danach längere Zeit nicht mehr
- Bandbreite steht während Ruhepausen anderen Teilnehmern nicht zur Verfügung

Lösungsansatz: Asynchrones (flexibles) TDMA

- **Keine statische Aufteilung** / Zuweisung von Zeitslots
- **Stattdessen: Zufälliger, konkurrierender** oder dynamisch geregelter Medienzugriff

[Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), TU München, Prof. Dr.-Ing. Georg Carle]

80

ALOHA und Slotted ALOHA

Random Access (ALOHA)

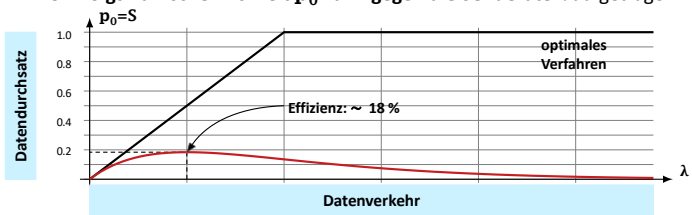
- Entwickelt an der Universität von Hawaii (1971), cf. Prof. Abramson
- Ursprünglich für kabellose Datenübertragungen
- Ziel: Verbindung von Oahu mit den anderen hawaiianischen Inseln

Funktionsweise

- Jede Station sendet an eine zentrale Station (vgl. „Basisstation“ in WLANs), sobald Daten vorliegen
- Senden zwei Stationen gleichzeitig, kommt es zu Kollisionen
- Erfolgreich übertragene Nachrichten werden vom Empfänger auf anderer Frequenz quittiert („out-of-band“ Bestätigungsverfahren auf Link-Layer, keine Kollisionen zwischen Nachrichten und Bestätigungen)

Erreichbarer Durchsatz mit Aloha

- Die **Erfolgswahrscheinlichkeit p_0 kann gegen die Senderate λ** aufgetragen werden:



Dieses Ergebnis ist nicht sehr ermutigend. Wenn aber jeder Daten dann überträgt, wann er will, ist kaum eine Erfolgsrate von 100% zu erwarten.

- Innerhalb eines **beliebigen Intervalls $[t, t + T]$ kann höchstens eine Übertragung** erfolgreich sein kann.
- Dementsprechend entspricht die Anzahl S der erfolgreichen Nachrichten pro Intervall gleichzeitig der Wahrscheinlichkeit für eine erfolgreiche Übertragung.
- Bei einem **optimalen Verfahren** würde die Anzahl. erfolgreicher Nachrichten **S linear mit der Senderate ansteigen, bis die maximale Anzahl von Nachrichten pro Zeitintervall erreicht ist** (1 Nachricht pro Intervall).
- Steigt die Senderate weiter, würde dies ein optimales Verfahren nicht beeinträchtigen.

CSMA, CSMA/CD, CSMA/CA

Carrier Sense Multiple Access (CSMA)

- Eine einfache Verbesserung von Slotted ALOHA: „Listen Before Talk“
- Höre das Medium ab
- Beginne erst dann zu senden, wenn das Medium frei ist

Verschiedene Varianten:

1-persistentes CSMA

1. Wenn Medium frei, beginne Übertragung

2. Wenn Medium belegt, warte bis frei und beginne dann Übertragung

p-persistentes CSMA

1. Wenn Medium frei, übertrage mit Wahrscheinlichkeit p oder verzögere mit Wahrscheinlichkeit $1 - p$ um eine feste Zeit dann 1.

2. Wenn Medium belegt, warte bis frei, dann 1.

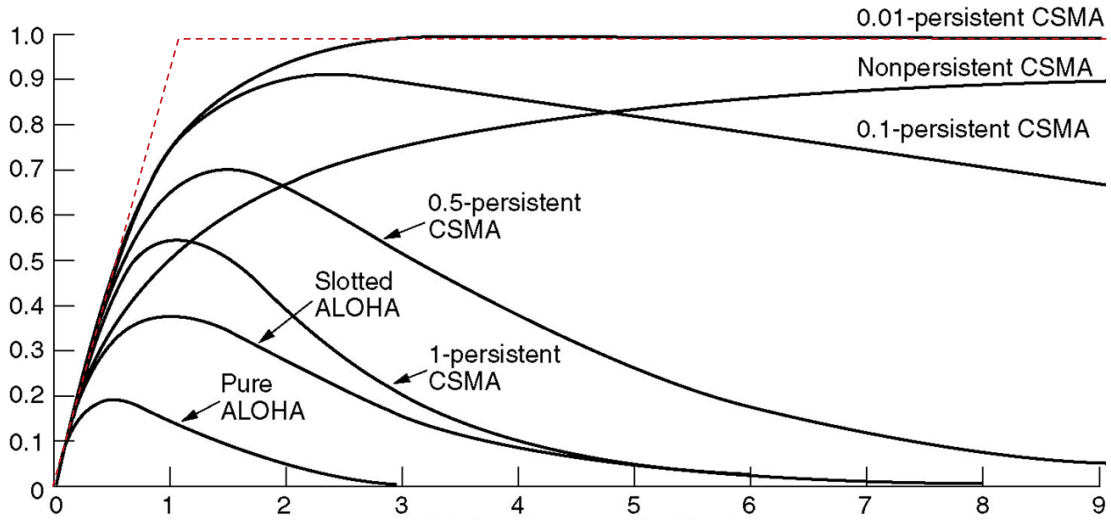
nicht-persistentes CSMA

1. Wenn Medium frei, beginne Übertragung

2. Wenn belegt, warte eine zufällig gewählte Zeitspanne dann 1.

tgm [Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), TU München, Prof. Dr.-Ing. Georg Carle]

Verfahren im Vergleich



tgm [Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), TU München, Prof. Dr.-Ing. Georg Carle]

Warum kein 0,01-persistent?

p-persistent bedeutet:Medium frei?→ Mit Wahrscheinlichkeit p senden→ Mit Wahrscheinlichkeit 1–p warten

Beispiel: p = 0,01 (1 %)

Das bedeutet: Nur jede 100. Chance würde tatsächlich genutzt werden. **Das wäre tödlich für kabelgebundenes Ethernet:**

Grund 1: Ethernet ist ein synchrones, sehr schnelles Medium

- Die Latenz im Kabel ist winzig (Nanosekunden).
- Wenn eine Station 99/100 Chancen verpasst… dann bekommt eine andere Station das Medium längst und sendet los. Das führt zu Nichtausnutzung des Kanals. Das Medium wäre 99% der Zeit ungenutzt, obwohl Daten warten.

Grund 2: Ethernet benutzt Collision Detection (CD)

- CSMA/CD erwartet absichtlich, dass Stationen gleichzeitig senden wollen.
- Warum? Weil Kollisionen schneller gelöst werden können als ewiges Warten und Nicht-Senden.
- Mit 1-persistent: Medium wird frei → ALLE senden sofort → mögliche Kollision
- Kollision erkannt → Backoff + Retry
- Das ist effizient, weil: Minimale Verzögerung, Medium fast nie ungenutzt
- Bei p=0,01 würde Ethernet unbrauchbar langsam.

Grund 3: p-persistent ist nur sinnvoll bei Funk (CSMA/CA)

- Beispiel: WLAN.Warum dort? Funk kann keine Kollisionen erkennen. Deshalb muss man „vorsichtiger“ senden. Daher p-persistent oder Random Backoff.
- Bei Ethernet dagegen: Man kann Kollisionen erkennen,also braucht man kein vorsichtiges Verhalten.

Grund 4: CSMA/CD ist darauf ausgelegt, Kollisionen zu erzeugen und zu lösen

- Das klingt verrückt, ist aber optimal: Schnell senden + Kollisionen schnell erkennen = hohe Effizienz

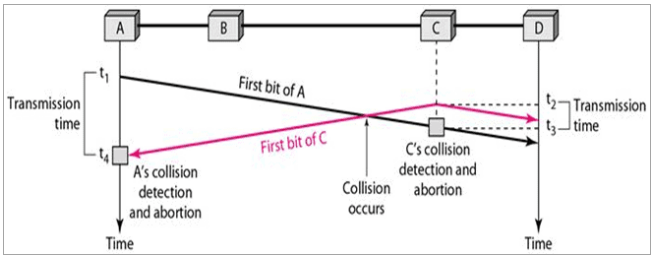
tgm [Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), TU München, Prof. Dr.-Ing. Georg Carle]

85

CSMA mit Kollisionserkennung (CD = Collision Detection)

- **Erkenne Kollisionen und wiederhole die Übertragung**, wenn eine Kollision erkannt wird
- Verzichte auf das Senden von Bestätigungen
- Wird keine Kollision erkannt, gilt die Übertragung als erfolgreich

Problem: Der Sender muss die Kollision erkennen, während er noch überträgt



tgm [Quelle: https://www.softwaretestinghelp.com/what-is-csma-cd/ - letzter Abruf 21.07.2025]

86

Back-Off-Zeit (Binary Exponential Backoff)

Wird 1-persistentes CSMA mit Kollisionserkennung verwendet, ergibt sich folgendes Problem:

- Die **Kollision zerstört die Nachrichten** beider in die Kollision verwickelten Stationen.
- Mind. eine der Stationen sendet ein **JAM-Signal**.
- Nachdem das Medium frei wird, **wiederholen beide Stationen die Übertragung**
  - ➢ **Es kommt sofort wieder zu einer Kollision.**

Lösung: Warte „zufällige" Zeit nach einer Kollision

Durch die Wartezeiten, die

- zufällig gewählt und
- situationsabhängig größer werden,
- wird die Kollisionswahrscheinlichkeit bei Wiederholungen reduziert.

Binary Exponential Backoff
Beim k-ten Sendeversuch einer Nachricht

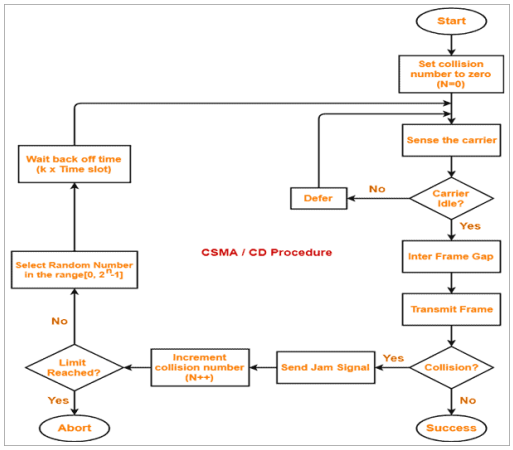
- wählt der Sender zufällig $n \epsilon \{0, \dots, min\{2^{k-1} - 1{,}1023\}\}$aus und
- wartet *n* Slotzeiten vor einem erneuten Sendeversuch.

Die maximale Wartezeit ergibt sich bei $k = 11$ (also bei 10 Wiederholungen) und beträgt 1023 Slotzeiten.

[Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), TU München, Prof. Dr.-Ing. Georg Carle]

CSMA mit Kollisionserkennung (CD = Collision Detection)

1. Zuerst **erkennt** die Station, die die Daten übertragen möchte, den Träger, ob dieser belegt oder inaktiv ist. Wenn ein Träger inaktiv ist, wird die Übertragung durchgeführt.
2. Die Übertragungsstation erkennt eine Kollision, falls vorhanden, unter der folgenden **Bedingung:** $\mathbf{T_t >= 2 * T_p}$, wobei T_t die Übertragungsverzögerung und T_p die Laufzeitverzögerung ist.
3. Die Station gibt das **Stausignal** frei, sobald sie eine Kollision erkennt.
4. Nachdem es zu einer Kollision gekommen ist, stoppt die Sendestation die Übertragung und wartet eine zufällige Zeitspanne, die als "**Back-Off-Zeit**" bezeichnet wird. Nach dieser Zeit sendet der Sender erneut.



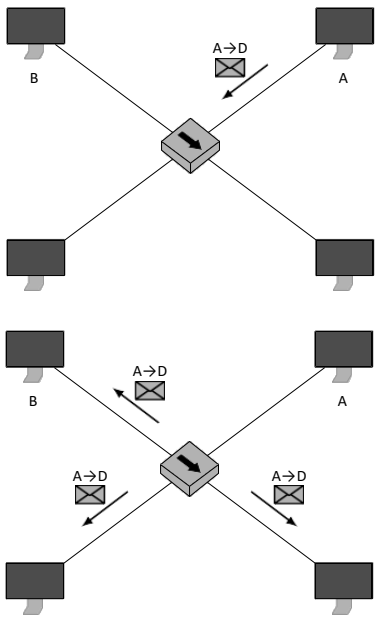
[Quelle: https://www.softwaretestinghelp.com/what-is-csma-cd/ - letzter Abruf 21.07.2025]

04

Verbindung auf Schicht 1 und 2

Verbindung auf Schicht 1: Hub

- **Knoten A sendet einen Rahmen an Knoten D**
- Der **Hub** verbindet die einzelnen Links **zu einem gemeinsamen Bus**
- Der Rahmen erreicht alle Knoten
- Es darf folglich zu jedem Zeitpunkt nur ein Knoten senden, andernfalls treten **Kollisionen** auf
- Wichtig: **Bis auf wenige Ausnahmen arbeitet Schicht 2 verbindungslos**, d. h. es wird keine logische Verbindung zwischen den Kommunikationspartnern aufgebaut.



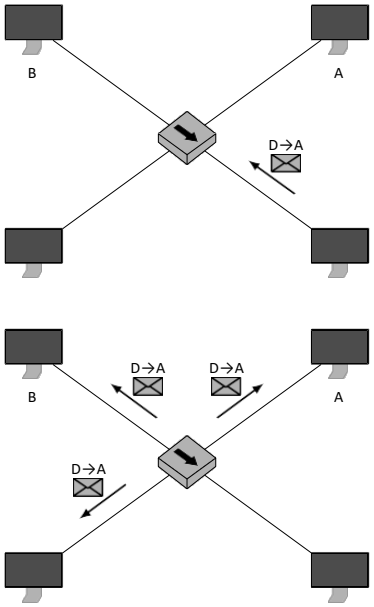
tgm [Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), TU München, Prof. Dr.-Ing. Georg Carle]

Verbindung auf Schicht 1: Hub

- Knoten D antwortet auf den Rahmen von A
- Auch die Antwort erreicht alle Knoten

Definition (Collision Domain)

Unter einer Kollisions-Domäne versteht man den Teil eines Direktverbindungsnetzes, innerhalb dem eine Kollision bei gleichzeitiger Über- tragung mehrerer Knoten auftreten kann. Dieser wird häufig auch als Segment bezeichnet.



tgm [Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), TU München, Prof. Dr.-Ing. Georg Carle]

Verbindung auf Schicht 1: Hub

Sind Hubs mehr als nur Sternverteiler?

- **Aktive Hubs (Repeater) verstärken die Signale** auf der physikalischen Schicht, ohne dabei die in Rahmen enthaltenen Felder wie Adressen oder Checksummen zu prüfen
- **Passive Hubs sind wirklich nur Sternverteiler**

Kann man Hubs kaskadieren?

- Ja, aber es gilt bei Ethernet mit Baumtopologie (802.3a/i) die 5-4-3-Regel:
- Nicht mehr als 5 Abschnitte, verbunden durch 4 Repeater, wobei nur in 3 Abschnitten aktive Endgeräte enthalten sein dürfen.

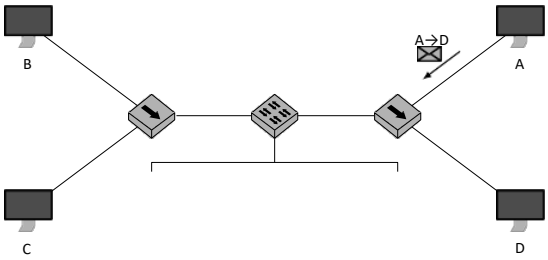
Können Hubs unterschiedliche Medientypen miteinander verbinden?

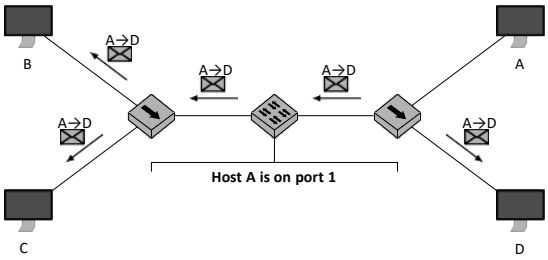
- Ja, wenn auf allen Abschnitten dasselbe Medienzugriffsverfahren genutzt wird (beispielsweise Verbindung Ethernet über BNC- und Patch-Kabel mit jeweils gleicher Datenrate).
- Unterschiedliche Zugriffsverfahren können nicht gekoppelt werden.

tgm [Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), TU München, Prof. Dr.-Ing. Georg Carle]

Verbindung auf Schicht 2: Switch

- Zwei Gruppen von Hosts, die jeweils über Hubs verbunden sind, werden durch einen Switch gekoppelt.
- Der Switch arbeitet zunächst wie ein Hub mit 2 Ports (Learning-Phase).
- Dabei merkt sich der Switch, über welchen Port ein Rahmen empfangen wurde.
- So ordnet er den Ports 0 und 1 die MAC-Adressen der Knoten zu, die an den jeweiligen Port angeschlossen sind.
- Ein Switch mit nur zwei Ports, nennt man auch Bridge.



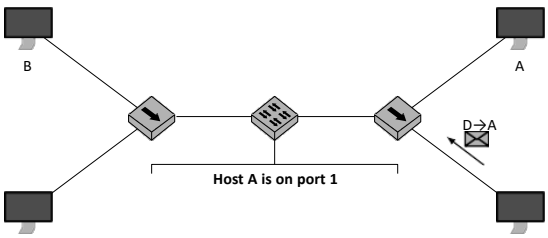


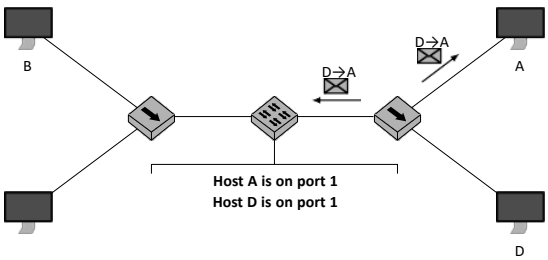
tgm [Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), TU München, Prof. Dr.-Ing. Georg Carle]

93

Verbindung auf Schicht 2: Switch

- Die Ziel-Adresse eingehender Rahmen wird mit den Einträgen in der Switching-Table verglichen.
- Ist ein Eintrag vorhanden, wir der Rahmen nur an den betreffenden Ziel-Port weitergeleitet.
- Ist kein Eintrag vorhanden, so wird der Rahmen an alle Ports weitergeleitet.
- Einträge erhalten einen Zeitstempel (Timestamp) und werden nach einem festen Zeitintervall invalidiert.



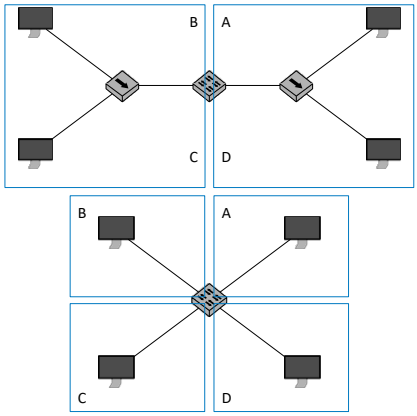


tgm [Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), TU München, Prof. Dr.-Ing. Georg Carle]

94

Verbindung auf Schicht 2: Switch

- Ein Switch bzw. eine Bridge unterbricht Kollisionsdomänen (auch als Segmentierung bezeichnet).
- Wenn ein Switch alle angeschlossenen Geräte kennt, darf in jedem der beiden Segmente jeweils ein Knoten zur selben Zeit senden.
- Ist pro Switchport genau ein Host angeschlossen, spricht man von Microsegmentation oder einem vollständig geswitchtem Netz (heute der Regelfall).
- In diesem Fall können jeweils zwei beliebige Hosts gleichzeitig miteineinander kommunizieren.



[Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), TU München, Prof. Dr.-Ing. Georg Carle]

95

Verbindung auf Schicht 2: Switch

- **Switches sind für Hosts transparent**, d. h. ein Host weiß nicht, dass er über einen Switch mit anderen Hosts kommuniziert.
- **Sender- und Empfänger-Adresse werden von Switches nicht verändert**.
- Switches **schränken nicht die Erreichbarkeit** innerhalb des Direktverbindungsnetzes ein.
- Ein **Broadcast (MAC-Adresse ff:ff:ff:ff:ff:ff)** wird von allen Hosts empfangen (man spricht daher auch von Broadcast-Domänen im Unterschied zu einer Kollisions-Domäne).
- Ein Switch benötigt zur Erfüllung seiner grundlegenden Aufgaben **keine eigene MAC-Adresse**.
- **Weiterleitungsentscheidungen werden auf Basis der Ziel-Adresse** und der Switching-Tabelle getroffen.

Ferner unterscheidet man zwischen zwei unterschiedlichen Switching-Arten:

- **Store-and-Forward:** Eingehende Rahmen werden vollständig empfangen und deren FCS geprüft. Falls der Ausgangsport belegt ist, kann eine begrenzte Anzahl von Rahmen gepuffert werden.
- **Cut-Through:** Beginne mit der Serialisierung des Rahmens, sobald der Ausgangsport bestimmt wurde. Die FCS wird in diesem Fall nicht geprüft.

[Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), TU München, Prof. Dr.-Ing. Georg Carle]

96

WLAN Access Points

WLAN Access Points sind im wesentlichen Brücken zwischen Twisted Pair und Funkübertragung:

- Ein **RJ45-Interface** in Richtung des kabelgebundenen Netzwerks
- Ein **Wireless Transceiver** in Richtung des Funknetzwerks

Allerdings besteht ein wesentlicher **Unterschied zu Brücken bzw. Switches**:

- WLAN Access Points sind für WLAN Clients **nicht transparent auf Schicht 2!**
  - Clients sind sich der Anwesenheit eines Access Points bewusst.
  - Zur Kommunikation untereinander wird der Access Point direkt adressiert.

Gemeinsam mit Switches haben Access Points aber:

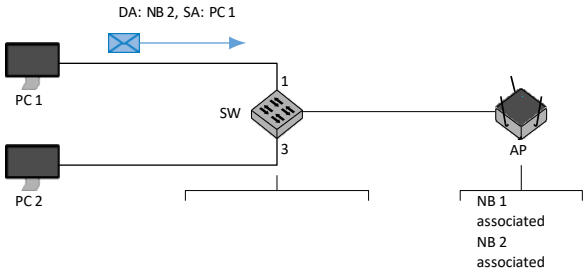
- Sie treffen **Weiterleitungsentscheidungen auf Basis von MAC-Adressen**.
- **Sie unterbrechen Kollisionsdomänen** auf logischer Ebene, d. h. ein Rahmen würde nicht weitergeleitet, sofern der betreffende Empfänger nicht mit dem jeweiligen AP assoziiert (verbunden) ist.
- Wichtig: Da Broadcast-Medium, nur eine Transmission gleichzeitig stattfinden, andernfalls Kollision

97

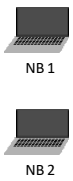
WLAN Access Points

Beispiel: PC 1 will mit NB 2 kommunizieren, wobei wir annehmen, dass

- NB 1 und NB 2 mit dem AP assoziiert (verbunden) sind und
- sonst noch keine Kommunikation im Netzwerk stattgefunden hat.



- PC 1 sendet einen Rahmen an NB 2.
- Source Address (SA) und Destination Address (DA) sind damit zunächst festgelegt.

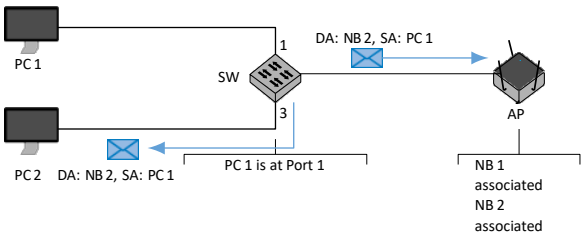


98

WLAN Access Points

Beispiel: PC 1 will mit NB 2 kommunizieren, wobei wir annehmen, dass NB 1 und NB 2 mit dem AP assoziiert (verbunden) sind und sonst noch keine Kommunikation im Netzwerk stattgefunden hat.

- Der Switch SW lernt, dass PC 1 an Port 1 angeschlossen ist.
- Der Empfänger NB 2 ist aber noch unbekannt, weswegen der Rahmen über alle Ports (außer dem, von dem er empfangen wurde) gesendet wird.



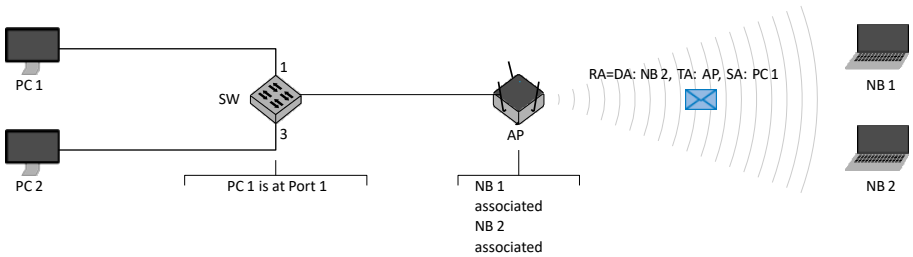
[Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), TU München, Prof. Dr.-Ing. Georg Carle]

99

WLAN Access Points

Beispiel: PC 1 will mit NB 2 kommunizieren, wobei wir annehmen, dass NB 1 und NB 2 mit dem AP assoziiert (verbunden) sind und sonst noch keine Kommunikation im Netzwerk stattgefunden hat.

- AP empfängt den Rahmen - NB 2 assoziierte (verbundene) Station.
- Wandelt von IEEE 802.3 zu IEEE 802.11
- RA entspricht der Destination Address (DA).
- TA ist die MAC-Adresse des AP.
- SA bleibt die Adresse von PC 1.
- NB 2 wird den Rahmen akzeptieren, NB 1 wird ihn ignorieren.



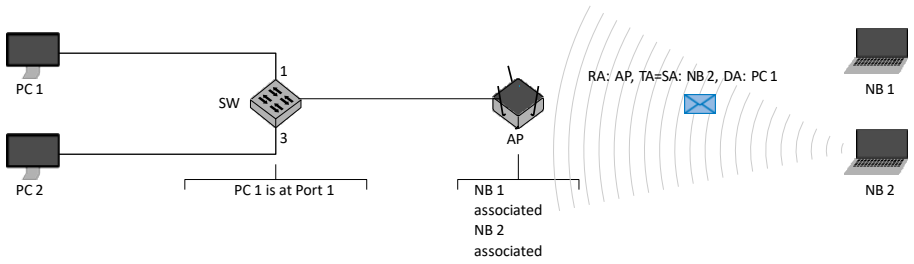
[Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), TU München, Prof. Dr.-Ing. Georg Carle]

100

WLAN Access Points

Beispiel: PC 1 will mit NB 2 kommunizieren, wobei wir annehmen, dass NB 1 und NB 2 mit dem AP assoziiert (verbunden) sind und sonst noch keine Kommunikation im Netzwerk stattgefunden hat.

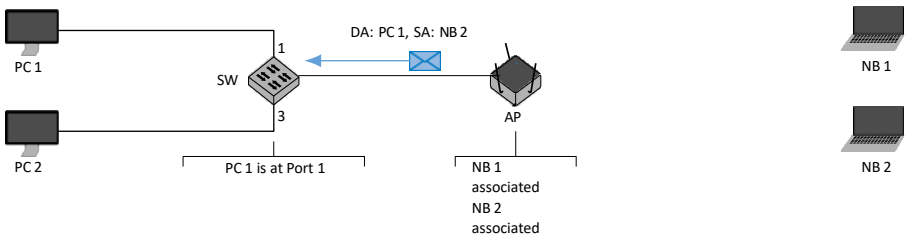
- NB 2 antwortet mit einem neuen Rahmen.
- Receiver Address (RA) ist der AP.
- Transmitter Address (TA) entspricht der Source Address (SA).
- Destination Address (DA) ist PC 1.
- Der AP empfängt den Rahmen und akzeptiert ihn, da er an ihn gerichtet ist (RA)..



WLAN Access Points

Beispiel: PC 1 will mit NB 2 kommunizieren, wobei wir annehmen, dass NB 1 und NB 2 mit dem AP assoziiert (verbunden) sind und sonst noch keine Kommunikation im Netzwerk stattgefunden hat.

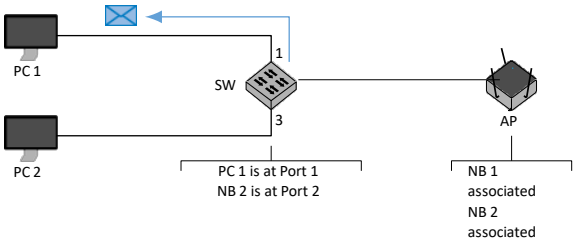
- Der AP weiß, dass PC 1 keine assoziierte Station ist – sich also nicht im WLAN befindet.
- Der AP wird daher den Rahmen von IEEE 802.11 zu IEEE 802.3 zurückübersetzen.
- Source Address (SA) ist NB 2.
- Destination Address (DA) ist PC 1.



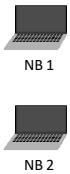
NETZWERKTECHNIK / SEMESTER 1 und 2

WLAN Access Points

Beispiel: PC 1 will mit NB 2 kommunizieren, wobei wir annehmen, dass NB 1 und NB 2 mit dem AP assoziiert (verbunden) sind und sonst noch keine Kommunikation im Netzwerk stattgefunden hat.



- SW 1 lernt, dass NB 2 an über Port 2 erreichbar ist.
- Da PC 1 bekanntlich an Port 1 angeschlossen ist, wird der Rahmen auch nur dort weitergeleitet.
- PC 1 akzeptiert den Rahmen.
- Weder PC 1 noch NB 2 haben das andere Medienzugriffsverfahren bemerkt



tgm [Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), TU München, Prof. Dr.-Ing. Georg Carle]

103

Ethernet Switching

NETZWERKTECHNIK / SEMESTER 1 UND 2

104

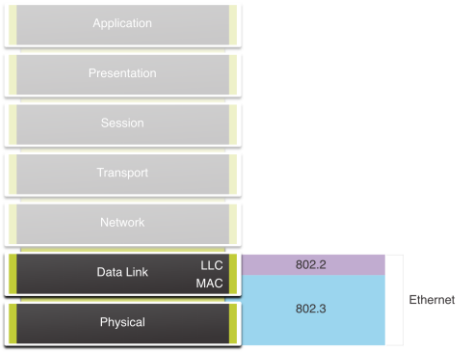
01

Ethernet Frames

105

Ethernet Kapselung

- Ethernet arbeitet in der **Sicherungsschicht** und der physikalischen Schicht.
- Es handelt sich um eine Familie von Netzwerktechnologien, die in den Standards **IEEE 802.2 und 802.3** definiert sind.



[Quelle: CCNAv7: Introduction to Networks (ITN) Companion Guide, Cisco Press]

106

NETZWERKTECHNIK / SEMESTER 1 und 2

Der Frame

- **Aus Sicht der physikalischen Schicht ist eine Nachricht lediglich eine Folge von Bits**.
- Für eine Betrachtung der Sicherungsschicht reicht diese Vorstellung aber nicht mehr aus.

Daher

- Wie werden einzelne Nachrichten auseinandergehalten?
- Welche zusätzlichen Informationen benötigen Protokolle der Sicherungsschicht?
- Wie werden Übertragungsfehler, die trotz Kanalkodierung auftreten, erkannt?

- **Im Kontext der Sicherungsschicht bezeichnen wir Nachrichten fortan als Rahmen (engl. Frame).**

tgm [Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), TU München, Prof. Dr.-Ing. Georg Carle]

107

NETZWERKTECHNIK / SEMESTER 1 und 2

Der Frame

- Die Daten werden von der Sicherungsschicht mit einem Header und einem Trailer gekapselt, um einen Rahmen zu bilden.
  - Header
  - Daten
  - Trailer
- Die Felder des Headers und des Trailers variieren je nach Protokoll der Sicherungsschicht.
- Die Menge der im Frame übertragenen Steuerungsinformationen variiert je nach Zugriffssteuerungsinformationen und logischer Topologie.

tgm [Quelle: Introduction to Networks v7.0 (ITN), Cisco Systems]

108

Fallbeispiele

IEEE 802.3a/i (Ethernet): 10 Mbit/s

- Als Leitungscode wird der **Manchester-Code** verwendet.
- Das Ende eines Frames wird durch **Coderegelverletzung** angezeigt.

IEEE 802.3u (FastEthernet): 100 Mbit/s

- Als Leitungscode wird **MLT-3** in Kombination mit dem **4B5B**-Code verwendet.
- Start und Ende von Rahmen werden durch **Steuerzeichen des 4B5B-Codes** markiert.

IEEE 802.3z (Gigabit Ethernet over Fiber): 1000 Mbit/s

- Als Leitungscode wird **NRZ** in Kombination mit dem **8B10B-Code** verwendet.
- Start und Ende von Rahmen werden durch **Steuerzeichen des 8B10B-Codes** markiert.
- IEEE 802.3ab (Gigabit Ethernet over Copper) verwendet andere Leitungscodes, da die Dämpfung andernfalls zu groß wäre.

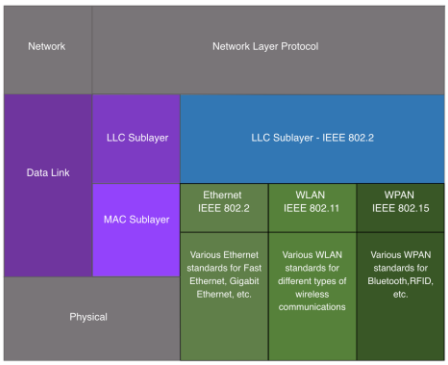
Zusätzlich wird bei all diesen Beispielen jedem Rahmen noch eine Präambel vorangestellt. Diese dient allerdings nur der Taktsynchronisierung zwischen Sender und Empfänger.

tgm [Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), TU München, Prof. Dr.-Ing. Georg Carle]

Sub-Layer der Sicherungsschicht

Die 802 LAN/MAN-Standards, einschließlich Ethernet, verwenden für den **Betrieb zwei separate Unterschichten** der Sicherungsschicht:

- **LLC Sublayer**: (IEEE 802.2) Platziert Informationen im Frame, um zu identifizieren, welches **Netzwerkschichtprotokoll** für den Frame verwendet wird.
- **MAC-Unterschicht**: (IEEE 802.3, 802.11 oder 802.15) Verantwortlich für die Datenkapselung und die **Medienzugriffskontrolle** und bietet die Adressierung der Sicherungsschicht.



tgm

NETZWERKTECHNIK / SEMESTER 1 und 2

Datenkapselung

Die MAC-Unterschicht ist für die **Datenkapselung und den Zugriff auf die Medien** verantwortlich.

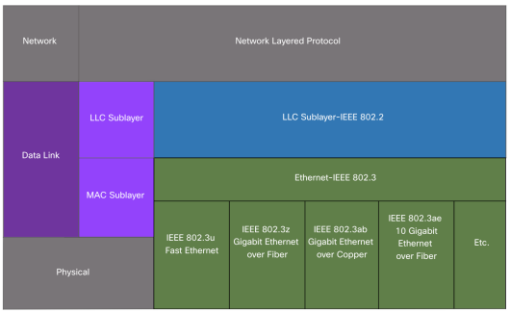
Die **IEEE 802.3**-Datenkapselung umfasst Folgendes:

- **Ethernet-Frame** - Dies ist die **interne Struktur des Ethernet-Frames**.
- **Ethernet-Adressierung** - Der Ethernet-Frame enthält sowohl eine **Quell- als auch eine Ziel-MAC-Adresse**, um den Ethernet-Frame von Ethernet-Netzwerkkarte zu Ethernet-Netzwerkkarte im selben LAN zu übermitteln.
- **Ethernet-Fehlererkennung** - Der Ethernet-Frame enthält einen **Frame Check Sequence (FCS)**-Trailer, der zur Fehlererkennung verwendet wird.

NETZWERKTECHNIK / SEMESTER 1 und 2

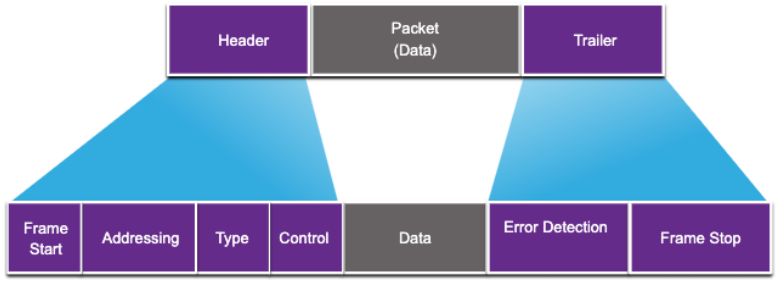
Medienzugriff

- Die IEEE 802.3 MAC-Subschicht enthält die Spezifikationen für verschiedene **Ethernet-Kommunikationsstandards für verschiedene Arten von Medien, einschließlich Kupfer und Glasfaser**.
- Legacy-Ethernet, das eine Bustopologie oder Hubs verwendet, ist ein gemeinsam genutztes Halbduplex-Medium. **Ethernet über ein Halbduplex-Medium verwendet eine konkurrierende Zugriffsmethode, Carrier Sense Multiple Access/Collision Detection (CSMA/CD).**
- In den heutigen Ethernet-LANs werden Switches verwendet, die im V**ollduplex-Modus** arbeiten. Für die Vollduplex-Kommunikation mit Ethernet-Switches ist **keine Zugriffskontrolle über CSMA/CD erforderlich**.



NETZWERKTECHNIK / SEMESTER 1 und 2

Felder eines Frame



Feld	Beschreibung
Frame Start and Stop	Identifiziert Anfang und Ende des Frames
Addressing	Gibt Quell- und Zielknoten an
Type	Identifiziert das gekapselte Layer-3-Protokoll
Control	Identifiziert Flusssteuerungsdienste
Data	Enthält die Frame-Nutzlast
Error Detection	Wird verwendet, um Übertragungsfehler zu ermitteln

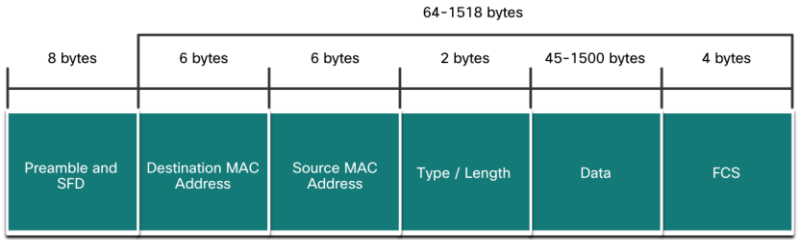
tgm [Quelle: Introduction to Networks v7.0 (ITN), Cisco Systems]

113

NETZWERKTECHNIK / SEMESTER 1 und 2

Ethernet Felder

- Die **minimale Ethernet-Frame-Größe beträgt 64 Byte und die maximale 1518 Byte**. Das Präambelfeld ist bei der Beschreibung der Größe des Rahmens nicht enthalten.
- Jeder Frame mit einer Länge **von weniger als 64 Byte wird als "Kollisionsfragment" oder "Runt-Frame"** betrachtet und automatisch verworfen. Frames mit **mehr als 1500 Bytes an Daten werden als "Jumbo"** oder "Baby Giant Frames" bezeichnet.
- **Wenn die Größe eines übertragenen Frames kleiner als das Minimum oder größer als das Maximum ist, verwirft das empfangende Gerät den Frame.** Ausgelassene Frames sind wahrscheinlich das Ergebnis von Kollisionen oder anderen unerwünschten Signalen.
  Sie gelten als ungültig.
  Jumbo-Frames werden in der Regel von den meisten Fast-Ethernet- und Gigabit-Ethernet-Switches und -Netzwerkkarten unterstützt.



tgm [Quelle: CCNAv7: Introduction to Networks (ITN) Companion Guide, Cisco Press]

114

Fehlererkennung

- **Trotz Kanalkodierung können Übertragungsfehler (Bitfehler) auftreten.**
- Es kann daher passieren, dass eine fehlerhafte Payload an höhere Schichten weitergeleitet wird.
- Um die Wahrscheinlichkeit für derartige Fehler zu weiter zu reduzieren, werden **zusätzlich fehlererkennende Codes eingesetzt** (sog. Prüf- summen, engl. Checksums):
- Im Gegensatz zur Kanalkodierung (fehlerkorrigierende Codes) dient die Prüfsumme eines Schicht-2-Protokolls üblicherweise **nicht der Fehlerkorrektur sondern lediglich der Fehlererkennung**.

Cyclic Redundancy Check (CRC)

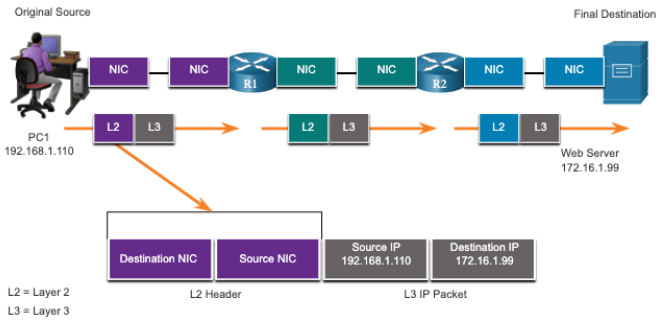
- Im Gegensatz zu fehlerkorrigierenden Codes, handelt sich sich bei **CRC um eine Familie fehlererkennender Codes**. Mit ihrem Einsatz werden folgende Ziele verfolgt:
- Eine **grosse Anzahl von Fehlern** (Einbit-, Mehrbit-, Burstfehler) sollen erkannt werden.
- Die zugefügte **Redundanz soll gering** sein.
- Fehler sollen **lediglich erkannt aber nicht korrigiert** werden können.

02

Ethernet MAC Adresse

Layer 2 Adressen

- Wird auch als **physische Adresse** bezeichnet.
- Enthalten im **Header** des Frame.
- Wird nur für die **lokale Übermittlung** eines Frames auf dem Link verwendet.
- **Wird von jedem Gerät aktualisiert, das den Frame weiterleitet.**

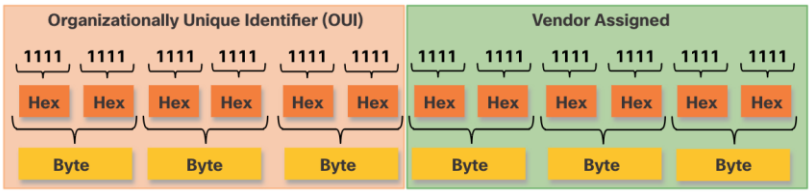


tgm [Quelle: Introduction to Networks v7.0 (ITN), Cisco Systems]

MAC und Hexadezimalschreibweise

- Eine Ethernet-MAC-Adresse besteht aus einem **48-Bit-Binärwert, der durch 12 Hexadezimalwerte** ausgedrückt wird.
- Da 8 Bit (ein Byte) eine übliche binäre Gruppierung sind, kann die Binärzahl **00000000 bis 11111111 hexadezimal als der Bereich 00 bis FF** dargestellt werden.
- Bei der Verwendung von Hexadezimalzahlen werden **immer führende Nullen angezeigt**, um die 8-Bit-Darstellung zu vervollständigen. Zum Beispiel wird der Binärwert 0000 1010 hexadezimal als 0A dargestellt.
- Hexadezimalzahlen werden in der Dokumentation häufig durch den Wert dargestellt, dem **0x vorangestellt** ist (z. B. 0x73), um zwischen Dezimal- und Hexadezimalwerten zu unterscheiden.
- Hexadezimal kann auch durch eine **tiefgestellte 16 oder die Hexadezimalzahl gefolgt von einem H** (z. B. 73H) dargestellt werden.

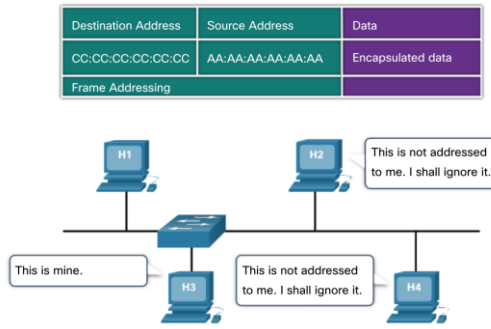
Ethernet MAC Adresse



- In einem **Ethernet-LAN ist jedes Netzwerkgerät mit den gleichen, gemeinsam genutzten Medien verbunden**. Die MAC-Adressierung stellt eine **Methode zur Geräteidentifikation** auf der Sicherungsschicht des OSI-Modells dar.
- Eine Ethernet-MAC-Adresse ist eine 48-Bit-Adresse, die aus 12 Hexadezimalziffern ausgedrückt wird. Da ein Byte 8 Bits entspricht, können wir auch sagen, dass eine **MAC-Adresse 6 Byte** lang ist.
- Alle MAC-Adressen müssen für das Ethernet-Gerät oder die Ethernet-Schnittstelle **eindeutig** sein. Um dies zu gewährleisten, müssen sich alle Anbieter, die Ethernet-Geräte verkaufen, bei der **IEEE registrieren**, um einen eindeutigen 6-Hexadezimal-Code (d. h. 24-Bit- oder 3-Byte-Code) zu erhalten, der als **Organizationally Unique Identifier (OUI)** bezeichnet wird.
- Eine Ethernet-MAC-Adresse besteht aus einem **6-Hexadezimal-OUI-Code, gefolgt von einem 6-Hexadezimal-Vendor-Zuweisungswert**.

Verarbeitung eines Frame

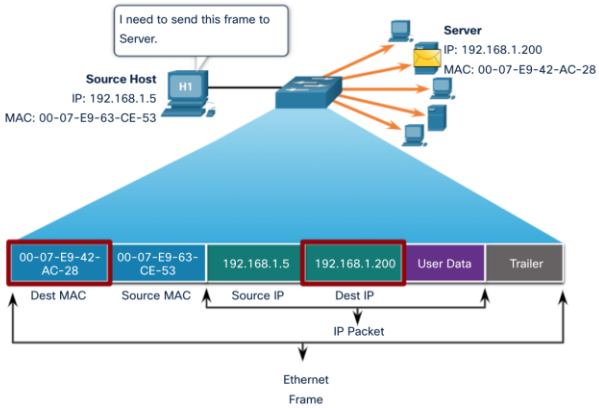
- Wenn ein Gerät eine Nachricht an ein Ethernet-Netzwerk weiterleitet, enthält der Ethernet-Header eine **Quell-MAC-Adresse und eine Ziel-MAC-Adresse**.
- Wenn eine Netzwerkkarte einen Ethernet-Frame empfängt, untersucht sie die Ziel-MAC-Adresse, um festzustellen, ob sie mit der physischen MAC-Adresse übereinstimmt. Wenn es keine Übereinstimmung gibt, verwirft das Gerät den Rahmen. Wenn es eine Übereinstimmung gibt, **wird der Frame an die OSI-Schichten weitergeleitet, wo der Entkapselungsprozess stattfindet**.
- Hinweis: Ethernet-Netzwerkkarten akzeptieren auch Frames, wenn es sich bei der Ziel-MAC-Adresse um einen Broadcast oder eine Multicast-Gruppe handelt, in der er Mitglied ist.
- **Jedes Gerät, das die Quelle oder das Ziel eines Ethernet-Frames ist, verfügt über eine Ethernet-Netzwerkkarte und damit über eine MAC-Adresse.** Dazu gehören Workstations, Server, Drucker, mobile Geräte und Router.



[Quelle: CCNAv7: Introduction to Networks (ITN) Companion Guide, Cisco Press]

Unicast MAC Adresse

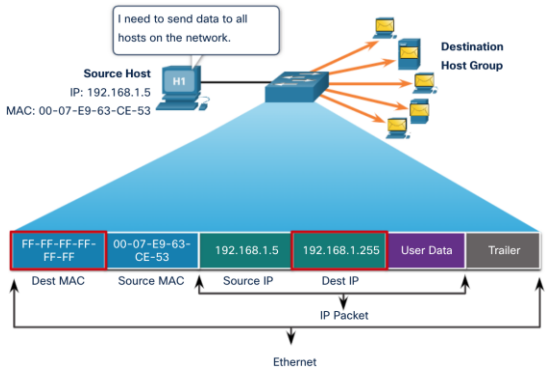
- In Ethernet werden **unterschiedliche MAC-Adressen für Layer-2-Unicast-, Broadcast- und Multicast**-Kommunikation verwendet.
- Eine **Unicast-MAC-Adresse ist die eindeutige Adresse**, die verwendet wird, wenn ein Frame von einem einzelnen Übertragungsgerät an ein einzelnes Zielgerät gesendet wird.
- Der Prozess, den ein Quellhost verwendet, um die MAC-Zieladresse zu bestimmen, die einer IPv4-Adresse zugeordnet ist, wird als **Address Resolution Protocol (ARP)** bezeichnet. Der Prozess, den ein Quellhost verwendet, um die MAC-Zieladresse zu bestimmen, die einer IPv6-Adresse zugeordnet ist, wird als **Neighbor Discovery (ND)** bezeichnet.
- Hinweis: Quell-MAC-Adresse immer Unicast



[Quelle: CCNAv7: Introduction to Networks (ITN) Companion Guide, Cisco Press]

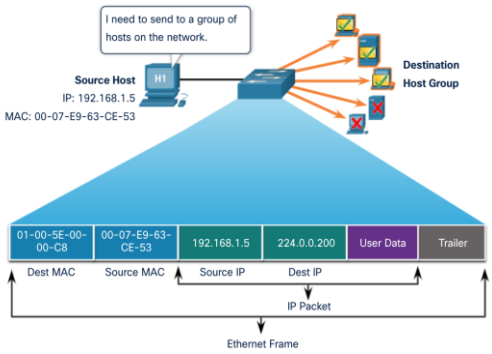
Broadcast MAC Adresse

- Ein Ethernet-Broadcast-Frame **wird von jedem Gerät im Ethernet-LAN empfangen und verarbeitet**. Die Funktionen eines Ethernet-Broadcasts sind wie folgt:
- Es hat eine Ziel-MAC-Adresse von **FF-FF-FF-FF-FF-FF** in hexadezimaler Form (48 Einsen im Binärformat).
- **Es werden alle Ethernet-Switch-Ports mit Ausnahme des eingehenden Ports überflutet**. Es wird nicht von einem Router weitergeleitet.
- Kann nur als Ziel eines Paketes verwendet werden.



Multicast MAC Adresse

- Ein Ethernet-Multicast-Frame **wird von einer Gruppe von Geräten empfangen und verarbeitet**, die zur gleichen Multicast-Gruppe gehören.
- Es gibt eine **Ziel-MAC-Adresse von 01-00-5E**, wenn es sich bei den gekapselten Daten um ein IPv4-Multicast-Paket handelt, und eine **Ziel-MAC-Adresse von 33-33**, wenn es sich bei den gekapselten Daten um ein IPv6-Multicast-Paket handelt.
- Es **gibt andere reservierte Multicast-Ziel-MAC-Adressen**, wenn es sich bei den gekapselten Daten nicht um IP handelt, z.B. Spanning Tree Protocol (STP).
- **Es werden alle Ethernet-Switch-Ports mit Ausnahme des eingehenden Ports überflutet**, es sei denn, der Switch ist für Multicast-Snooping konfiguriert. Er wird nicht von einem Router weitergeleitet, es sei denn, der Router ist für die Weiterleitung von Multicast-Paketen konfiguriert.
- Da Multicast-Adressen eine Gruppe von Adressen darstellen, können sie **nur als Ziel eines Pakets verwendet werden**. Die Quelle ist immer eine Unicast-Adresse.



03

MAC Adresstabelle

QUELLE:

INTRODUCTION TO NETWORKS V7.0 (ITN)

Grundlagen von Switches

- **Ein Layer-2-Ethernet-Switch verwendet Layer-2-MAC-Adressen, um Weiterleitungsentscheidungen zu treffen**.
- Er ist sich nicht bewusst, welche Daten (Protokolle) im Datenteil des Frames übertragen werden, z. B. ein IPv4-Paket, eine ARP-Nachricht oder ein IPv6-ND-Paket. Der Switch trifft seine Weiterleitungsentscheidungen ausschließlich auf der Grundlage der Layer-2-Ethernet-MAC-Adressen.
- Ein Ethernet-Switch **untersucht seine MAC-Adresstabelle, um eine Weiterleitungsentscheidung für jeden Frame zu treffen**, im Gegensatz zu älteren Ethernet-Hubs, die alle Ports mit Ausnahme des eingehenden Ports fluten.
- Wenn ein Switch eingeschaltet wird, ist die MAC-Adresstabelle leer
- Hinweis: Die MAC-Adresstabelle wird manchmal auch als **CAM-Tabelle (Content Addressable Memory)** bezeichnet.

Lernen und Weiterleiten

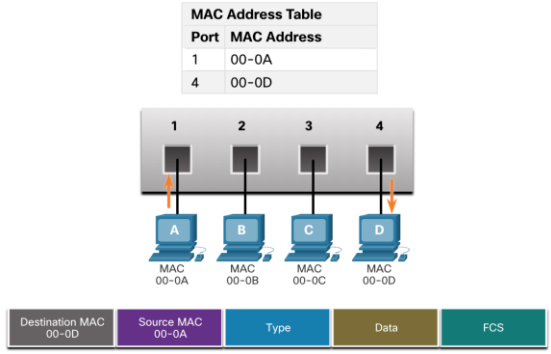
- **Untersuchen der Quell-MAC-Adresse (Lernen)**
- Jeder Frame der bei einem Switch ankommt, wird auf neue Informationen überprüft, die gelernt werden sollen. Dazu werden die Quell-MAC-Adresse des Frames und die Portnummer untersucht, an der der Frame in den Switch eingetreten ist.
  - Wenn die Quell-MAC-Adresse **nicht vorhanden** ist, wird sie zusammen mit der eingehenden Portnummer der Tabelle hinzugefügt.
  - Wenn die Quell-MAC-Adresse **vorhanden** ist, aktualisiert der Switch den Aktualisierungs-Timer für diesen Eintrag. Standardmäßig behalten die meisten Ethernet-Switches einen Eintrag in der Tabelle 5 Minuten lang.
- Hinweis: Wenn die Quell-MAC-Adresse in der Tabelle, aber an einem anderen Port vorhanden ist, behandelt der Switch diese als neuen Eintrag. Der Eintrag wird mit der gleichen MAC-Adresse, aber mit der aktuelleren Portnummer ersetzt.

Lernen und Weiterleiten

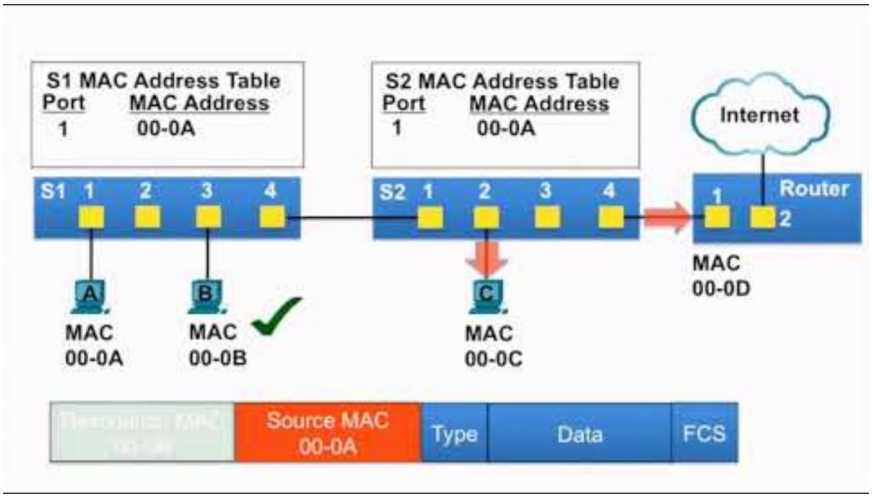
- **Suchen der Ziel-MAC-Adresse (Weiterleiten)**
- Wenn es sich bei der Ziel-MAC-Adresse um eine Unicast-Adresse handelt, sucht der Switch nach einer Übereinstimmung zwischen der Ziel-MAC-Adresse des Frames und einem Eintrag in der MAC-Adresstabelle.
  - Wenn sich die MAC-Zieladresse **in der Tabelle** befindet, wird der Frame an den angegebenen Port weitergeleitet.
  - Wenn die MAC-Zieladresse **nicht in der Tabelle** enthalten ist, leitet der Switch den Frame an alle Ports mit Ausnahme des eingehenden Ports weiter. Dies wird als unbekannter Unicast bezeichnet.
- Hinweis: Wenn es sich bei der Ziel-MAC-Adresse um einen Broadcast oder einen Multicast handelt, wird der Frame auch an allen Ports mit Ausnahme des eingehenden Ports überflutet.

Filtern von Frames

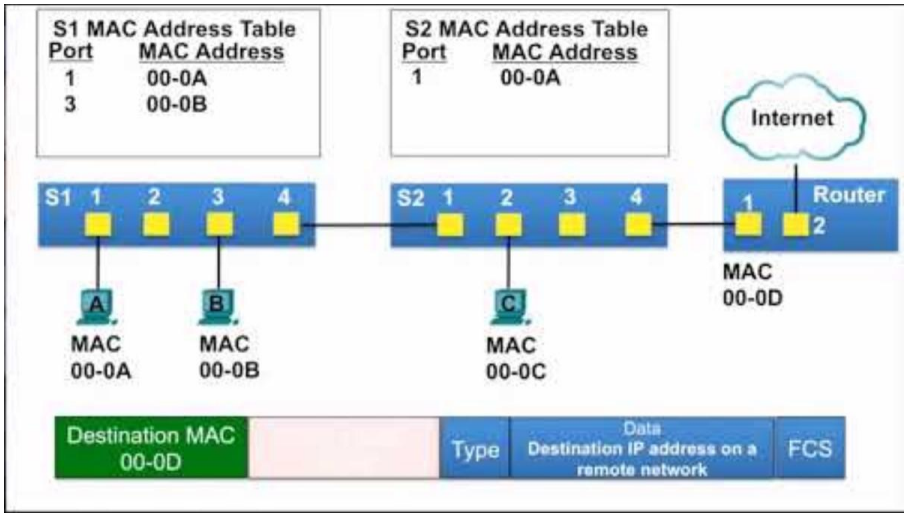
- Da ein Switch Frames von verschiedenen Geräten empfängt, kann er seine MAC-Adresstabelle füllen, indem er die Quell-MAC-Adresse jedes Frames untersucht.
- Wenn die MAC-Adresstabelle des Switches die MAC-Zieladresse enthält, kann er den Frame filtern und auf einem einzelnen Port weiterleiten.



VIDEO – MAC-Adresstabellen auf verbunden Switches



VIDEO - Senden eines Frames zum Default Gateway



[Quelle: CCNAv7: Introduction to Networks (ITN) Companion Guide, Cisco Press]

131

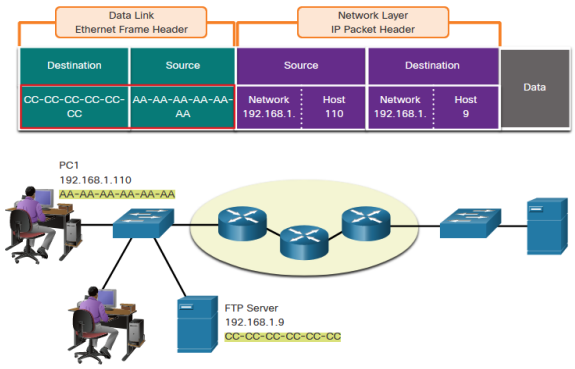
04

Rolle der Adressen der Sicherungsschicht

132

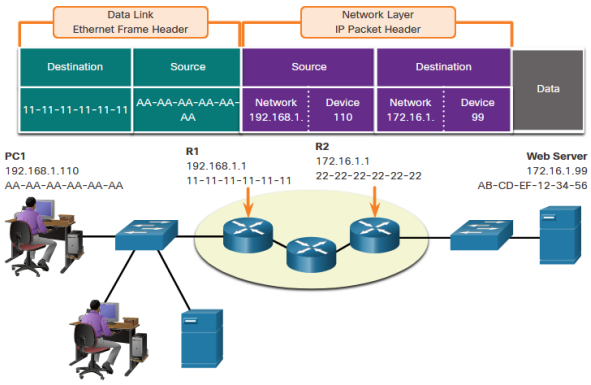
Rolle der Adressen der Sicherungsschicht: Gleiches IP-Netzwerk

- Wenn sich Geräte im selben Ethernet-Netzwerk befinden, verwendet der Data Link Frame die tatsächliche MAC-Adresse der Ziel-Netzwerkkarte.
- MAC-Adressen sind physisch in die Ethernet-Netzwerkkarte eingebettet und dienen der lokalen Adressierung.
- Die Quell-MAC-Adresse ist die des Absenders des Links.
- Die Ziel-MAC-Adresse befindet sich immer auf derselben Verbindung wie die Quelle, auch wenn das endgültige Ziel remote ist.



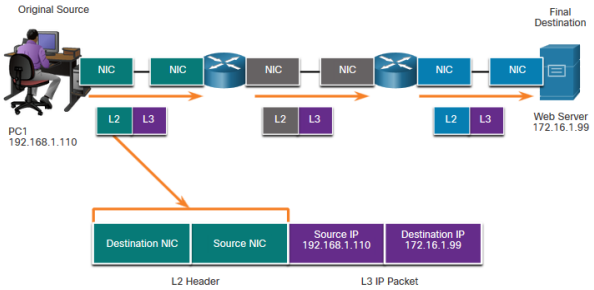
Geräte in einem Remote-Netzwerk

- Was passiert, wenn sich das eigentliche (endgültige) Ziel nicht im selben LAN befindet und remote ist?
- Was passiert, wenn PC1 versucht, den Webserver zu erreichen?
- Wirkt sich dies auf die Netzwerk- und Sicherungsschichten aus?



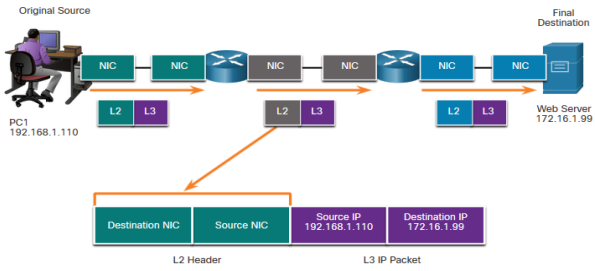
Data-Link Adresse

- Da es sich bei der Datenlink-Adressierung um eine lokale Adressierung handelt, gibt es für jedes Segment oder jeden Hop der Reise zum Ziel eine Quelle und ein Ziel.
- Die MAC-Adressierung für das erste Segment lautet:
- Quelle – (PC1 NIC) sendet Frame
- Ziel – (Erster Router – DGW-Schnittstelle) empfängt Frame



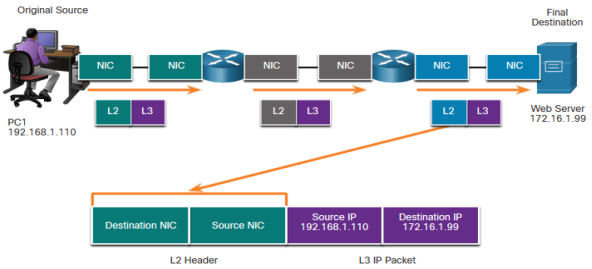
Data-Link Adresse

- Die MAC-Adressierung für den zweiten Hop lautet:
- Quelle – (Erste Router-Ausgangsschnittstelle) sendet Frame
- Ziel – (Zweiter Router) empfängt Frame



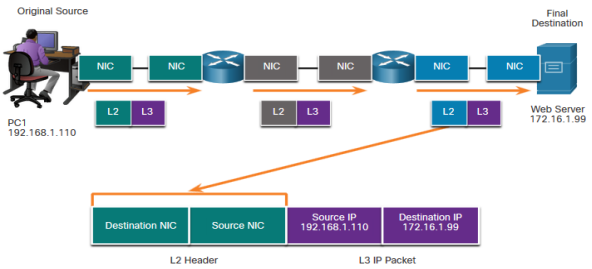
Data-Link Adresse

- Die MAC-Adressierung für das letzte Segment lautet:
- Quelle – (Zweiter Router – Ausgangsschnittstelle) sendet Frame
- Ziel – (Webserver-NIC) empfängt Frame



Data-Link Adresse

- Beachten Sie, dass das Paket nicht geändert wird, sondern der Frame, sodass sich die L3-IP-Adressierung nicht wie bei der L2-MAC-Adressierung von Segment zu Segment ändert.
- Die L3-Adressierung bleibt gleich, da sie global ist und das endgültige Ziel immer noch der Webserver ist.



04

Geschwindigkeit und Weiterleitungs-methoden

QUELLE:

INTRODUCTION TO NETWORKS V7.0 (ITN)

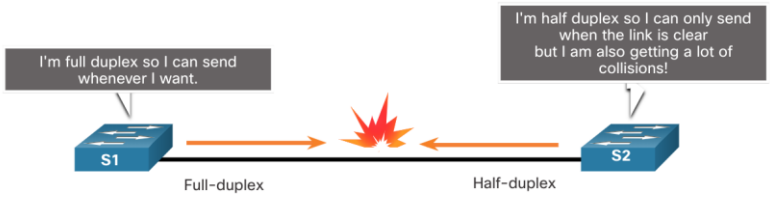
Duplex und Geschwindigkeit

- Zwei der grundlegendsten Einstellungen eines Switches sind die **Bandbreiten- ("Geschwindigkeit") und die Duplex-Einstellungen** für jeden einzelnen Switch-Port.
- Es ist wichtig, dass die **Duplex- und Bandbreiteneinstellungen zwischen dem Switch-Port und den angeschlossenen Geräten übereinstimmen**.
- Es gibt zwei Arten von Duplexeinstellungen, die für die Kommunikation in einem Ethernet-Netzwerk verwendet werden:
  - **Vollduplex** - Beide Enden der Verbindung können gleichzeitig senden und empfangen.
  - **Halbduplex** - Es kann jeweils nur ein Ende der Verbindung gesendet werden.
  - **Autonegotiation** ist eine optionale Funktion, die auf den meisten Ethernet-Switches und Netzwerkkarten zu finden ist. Es ermöglicht zwei Geräten, automatisch die beste Geschwindigkeit und Duplex-Funktionen auszuhandeln.
- Hinweis: Gigabit-Ethernet-Ports arbeiten nur im Vollduplex-Modus.

tgm [Quelle: CCNAv7: Introduction to Networks (ITN) Companion Guide, Cisco Press]

Duplex und Geschwindigkeit

- Duplex-Diskrepanzen sind eine der häufigsten Ursachen für Leistungsprobleme bei 10/100-Mbit/s-Ethernet-Verbindungen. Sie tritt auf, wenn ein Port auf der Verbindung mit Halbduplex arbeitet, während der andere Port mit Vollduplex arbeitet.
- Dies kann der Fall sein, wenn ein oder beide Ports auf einer Verbindung zurückgesetzt werden und der Autonegotiation-Prozess nicht dazu führt, dass beide Verbindungspartner die gleiche Konfiguration haben.
- Es kann auch auftreten, wenn Benutzer eine Seite eines Links neu konfigurieren und vergessen, die andere Seite neu zu konfigurieren. Auf beiden Seiten einer Verbindung sollte die automatische Aushandlung aktiviert sein, oder auf beiden Seiten sollte sie deaktiviert sein. Es empfiehlt sich, beide Ethernet-Switch-Ports als Vollduplex zu konfigurieren.



tgm [Quelle: CCNAv7: Introduction to Networks (ITN) Companion Guide, Cisco Press]

Auto-MDIX

- Für Verbindungen zwischen Geräten war **früher die Verwendung eines Crossover- oder Straight-Through-Kabels erforderlich**. Die Art des erforderlichen Kabels hing von der Art der Verbindungsgeräte ab.
- Hinweis: Eine direkte Verbindung zwischen einem Router und einem Host erfordert eine Crossover-Verbindung.
- Die meisten Switch-Geräte unterstützen jetzt **automatic medium-dependent interface crossover (Auto-MDIX)**. Wenn diese Option aktiviert ist, erkennt der Switch automatisch den Typ des an den Port angeschlossenen Kabels und konfiguriert die Schnittstellen entsprechend.
- Die **Auto-MDIX-Funktion ist standardmäßig auf Switches aktiviert**. Die Funktion kann jedoch deaktiviert sein. Aus diesem Grund sollten Sie immer den richtigen Kabeltyp verwenden und sich nicht auf die Auto-MDIX-Funktion verlassen.
- Auto-MDIX kann mit dem Befehl mdix auto interface configuration aktiviert werden.

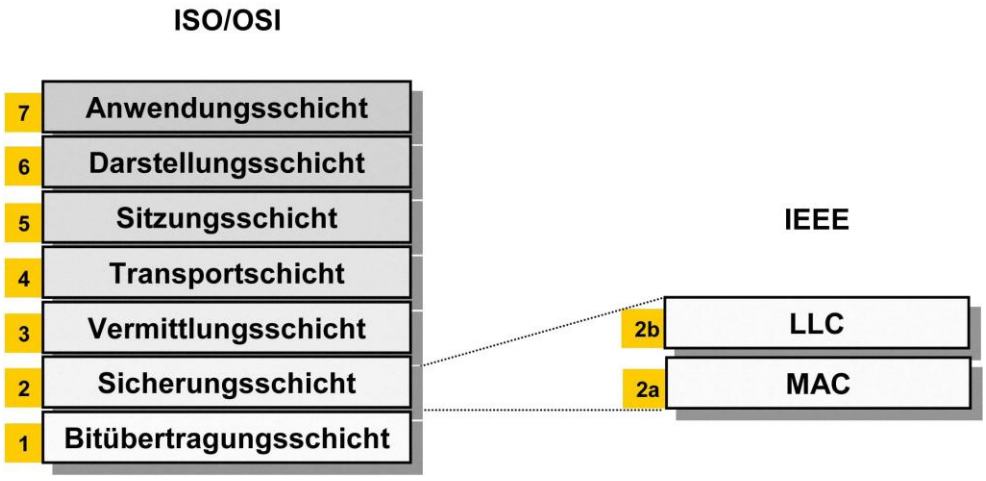
tgm [Quelle: CCNAv7: Introduction to Networks (ITN) Companion Guide, Cisco Press]

Vermittlungsschicht

NETZWERKTECHNIK / SEMESTER 1 UND 2

143

Einordnung im ISO/OSI Modell



[Quelle: https://www.airnet.de/cr1-gfe/de/html/TrFddiIEEE802_learningObject6.xml - letzter Abruf 21.07.2025]

144

Adressierung im Internet

Die **Sicherungsschicht** (Schicht 2) bietet

- fairen Medienzugriff bei von mehreren Hosts geteilten Medien,
- einen „ausreichenden“ Schutz vor Übertragungsfehler und
- Adressierung innerhalb eines Direktverbindungsnetzes.

Die **Vermittlungsschicht** (Schicht 3) ergänzt dies um

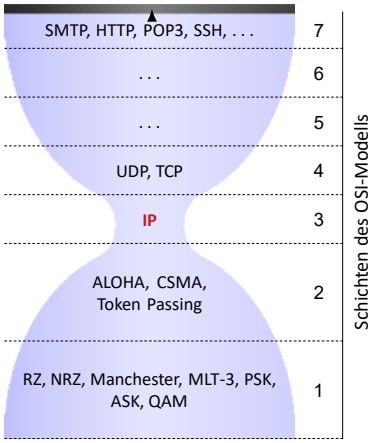
- Global eindeutigen und strukturierten / logischen Adressierung sowie
- Verfahren zur Bestimmung von (möglichst) optimalen Pfaden.

Wir beschränken uns auf die Betrachtung von

- **IPv4** (Internet Protocol v4, 1981) bzw.
- seinem Nachfolger **IPv6** (1998).

Alternative Protokolle der Netzwerkschicht:

IPX (Internetwork Packet Exchange, 1990), DECnet Phase 5 (1987), AppleTalk (1983)

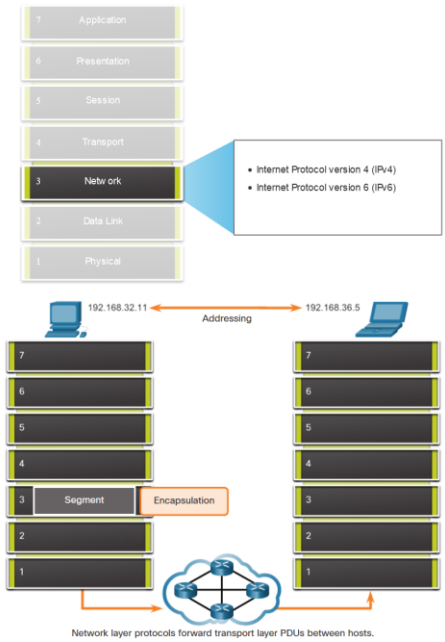


tgm [Quelle: Grundlagen Rechnernetze und Verteilte Systeme (GRNVS), Prof. Dr.-Ing. Georg Carle, TUM, 2025]

145

Die Vermittlungsschicht

- Stellt Dienste bereit, mit denen Endgeräte Daten austauschen können
- **IP Version 4 (IPv4) und IP Version 6 (IPv6)** sind die wichtigsten Kommunikationsprotokolle auf Netzwerkebene.
- Die Netzwerkschicht führt **vier grundlegende Vorgänge** aus:
  - Adressierung von Endgeräten
  - Encapsulation
  - Routing
  - De-Encapsulation

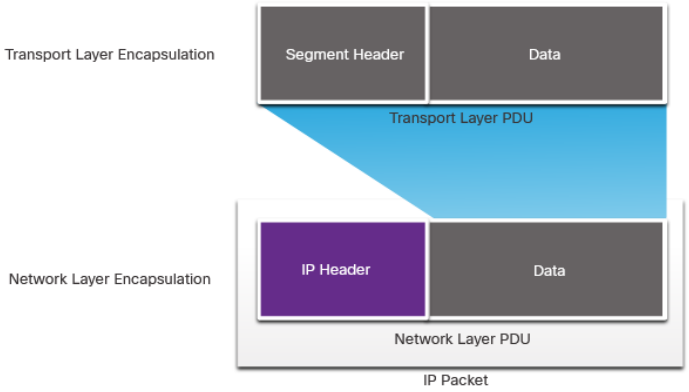


tgm [Quelle: Introduction to Networks v7.0 (ITN), Cisco Systems]

146

Kapselung

- IP **kapselt das Segment** der Transportschicht.
- IP kann **entweder ein IPv4- oder ein IPv6-Paket verwenden** und wirkt sich nicht auf das Layer-4-Segment aus.
- Das IP-Paket wird **von allen Layer-3-Geräten untersucht**, während es das Netzwerk durchläuft.
- Die **IP-Adressierung** ändert sich nicht von Quelle zu Ziel.



Eigenschaften von IP

IP hat einen geringen Overhead und kann wie folgt beschrieben werden:

- **Verbindungslos**
- **Best-Effort („Nach besten Kräften“)**
- **Medienunabhängig**

Verbindungslos

IP ist verbindungslos

- IP baut **vor dem Senden des Pakets keine Verbindung mit dem Ziel** auf.
- Es werden **keine Steuerungsinformationen** (Synchronisationen, Bestätigungen usw.) benötigt.
- Das Ziel empfängt das Paket, wenn es eintrifft, aber es werden **keine Vorabbenachrichtigungen** vom IP gesendet.
- Wenn ein **Bedarf an verbindungsorientiertem Datenverkehr besteht, wird dies von einem anderen Protokoll verarbeitet** (in der Regel TCP auf der Transportschicht).

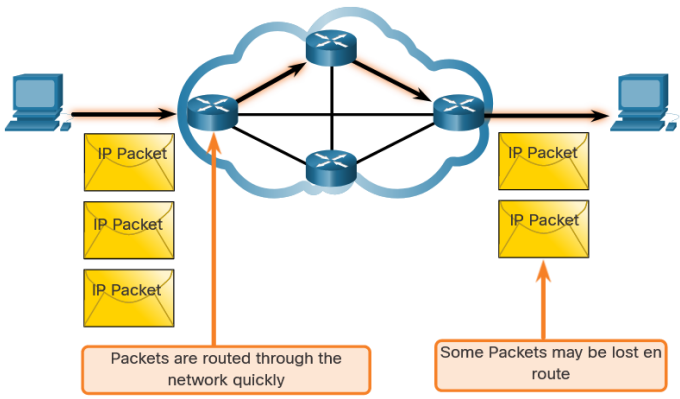
tgm [Quelle: Introduction to Networks v7.0 (ITN), Cisco Systems]

149

Best-Effort

IP ist Best Effort

- IP übernimmt **keine Garantie für die Zustellung** des Pakets.
- IP hat den Overhead reduziert, da es **keinen Mechanismus zum erneuten Senden von Daten** gibt, die nicht empfangen wurden.
- IP erwartet **keine Bestätigungen**.
- IP weiß nicht**, ob das andere Gerät betriebsbereit ist oder ob es das Paket empfangen** hat.



tgm [Quelle: Introduction to Networks v7.0 (ITN), Cisco Systems]

150

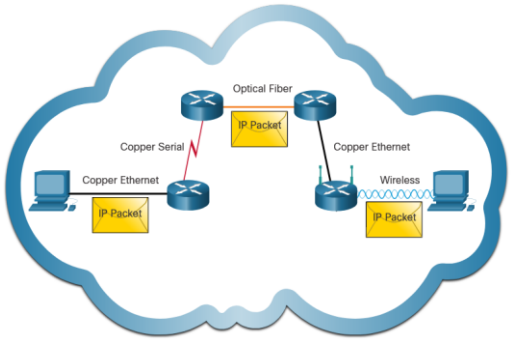
Medienunabhängig

IP ist **unzuverlässig**:

- **Nicht zugestellte oder beschädigte Pakete** können nicht verwaltet oder repariert werden.
- IP kann nach einem **Fehler** nicht erneut übertragen.
- IP kann nicht **Sequenzfehler** (vertauschte Pakete) korrigieren.
- IP muss sich für diese Funktionen auf **andere Protokolle** verlassen.

IP ist **medienunabhängig**:

- IP befasst sich nicht mit der Art des Frames, der auf der Sicherungsschicht erforderlich ist, oder dem Medientyp auf der physikalischen Ebene.
- **IP kann über jeden Medientyp gesendet werden: Kupfer, Glasfaser oder drahtlos.**



Medienunabhängig

- Die Netzwerkschicht legt die **Maximum Transmission Unit (MTU)** fest.
- Die Netzwerkschicht ermittelt dies aus Steuerinformationen, die von der Sicherungsschicht bereitgestellt werden.
- Das Netzwerk ermittelt dann die MTU-Größe.

Fragmentierung liegt vor, wenn Layer 3 das IPv4-Paket in kleinere Einheiten aufteilt.

- Die **Fragmentierung führt zu Latenz**.
- **IPv6 fragmentiert keine Pakete.**
- Beispiel: Der Router wechselt von Ethernet zu einem langsamen WAN mit einer kleineren MTU