

snippet

Silas Hoffmann, inf103088

30. November 2019

Inhaltsverzeichnis

1 marked

Erläutern Sie ganz allgemein den Begriff Lokales Netz bzw. LAN. Welche grundlegende Funktionen bzw. Aufgabe erfüllt so ein LAN?

„LAN-Technologien realisieren den direkten physikalischen Datentransport zwischen einzelnen Netzinterfaces über ein sie verbindendes Medium.“ Ein LAN stellt die technische Infrastruktur zur Punkt-zu-Punkt Kommunikation über ein gemeinsames Medium direkt verbundene Systeme (Interfaces) dar. Die LAN-Technologien umfassen die OSI-Funktionsschichten -1 und -2.

IEEE - Local Area Networks (LANs)

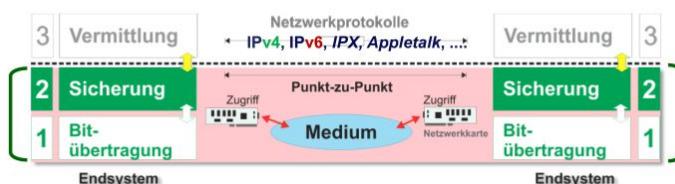


- „**LAN-Technologien** realisieren den **direkten physikalischen Datentransport** zwischen **einzelnen Netzinterfaces** über ein sie **verbindendes Medium**.“

- **Spezifikation** durch **einzelne Projektgruppen** in der **Arbeitsgruppe IEEE 802 LAN/MAN Standards Committee** (gegründet **2/1980**). 

- **LAN-Projektgruppen** legen **IEEE-Standards**^{*)} für **Übertragungstechniken** und **Zugriffsverfahren** mit **Datenraten von aktuell hin zu 100 Gbps**^{*)} fest.

- ☒ Die **LAN-Technologien** umfassen die **OSI-Funktionsschichten -1 und -2**.



Institute of Electronic and Electrical Engineers

*) Später folg(t)en teils identische ISO-8802x Standards

*) bzw. 400Gbit/s seit 12/2017

© Fachhochschule Wedel, Dipl.-Ing.(FH) I. Kaleck <http://www.fh-wedel.de/~kal>

16. Januar 2019

Folie Nr. 3



LANs umfassen unterschiedliche Komponenten



- Ein **LAN** stellt die **technische Infrastruktur** zur **Punkt-zu-Punkt**^{*)} **Kommunikation** für über ein **gemeinsames Medium** **direkt** verbundene Systeme (**Interfaces**) dar.



- **LAN-Übertragungstechnik**

- Stellt Medien-Zugriffverfahren und unterschiedliche **Netztopologien** bereit
 - ↳ CSMA/CD (Bus), CSMA/CA (Drahtlos), Token-Passing (Ring), Demand-Priority (Strom), ...
- Erlaubt dabei unterschiedliche **Übertragungsmedien**
 - ↳ Kupferkabel (Koaxialkabel, Twisted-Pair Kabel)
 - ↳ Lichtwellenleiter (Optische Übertragung)
 - ↳ Drahtlose Übertragung (Wireless LANs)



- **LAN-Komponenten** (zum physikalischen Netzaufbau)

- **Netzwerkarten** (Anschluss für div. Übertragungsmedien)
 - ↳ Ethernet-, Token-Ring- oder Wireless-LAN Karten
- **Koppelemente** (nur auf Layer-1 und -2)
 - ↳ Repeater (LAN, Wireless LAN)
 - ↳ Brücke / Switch (LAN)
 - ↳ Access-Point (Wireless LAN)



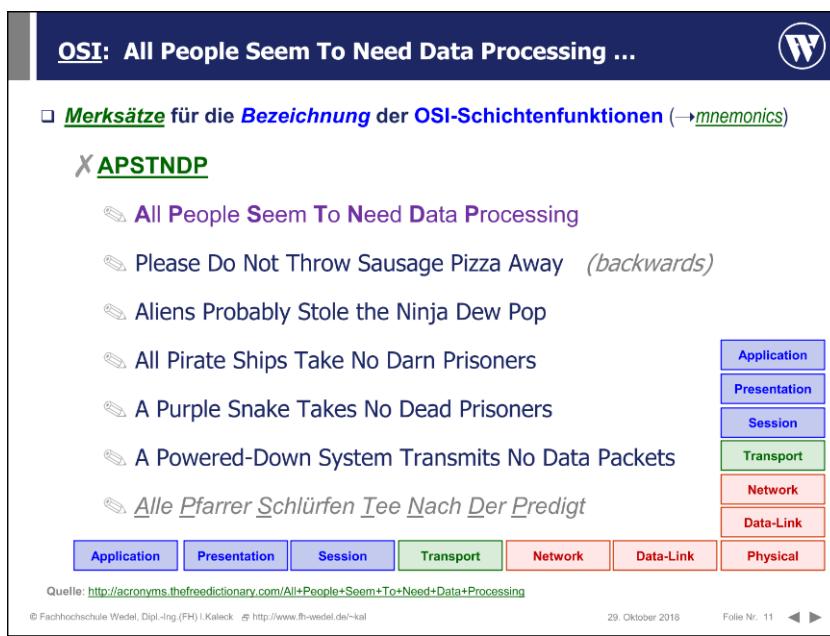
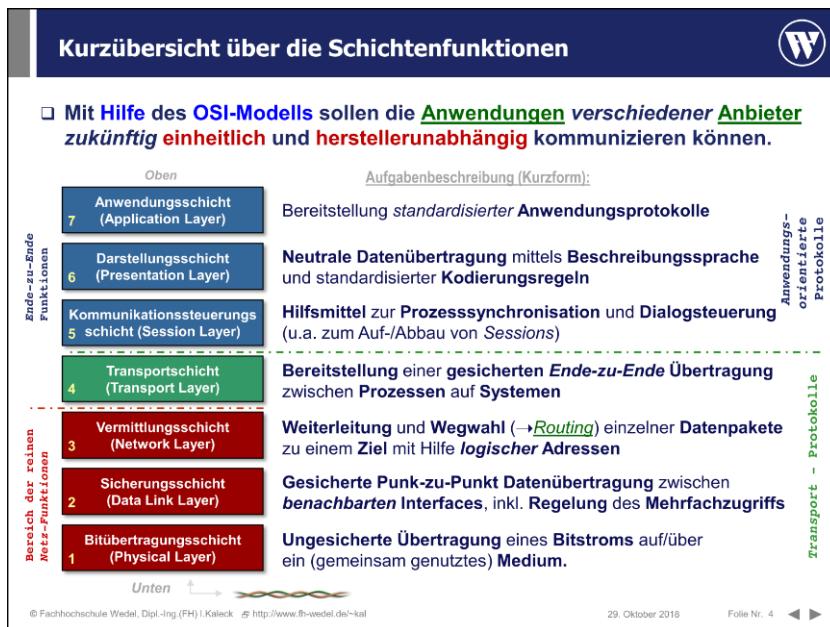
*) bzw. **Punkt-zu-Mehrpunkt** Kommunikation

© Fachhochschule Wedel, Dipl.-Ing.(FH) I. Kaleck <http://www.fh-wedel.de/~kal>

16. Januar 2019

Folie Nr. 4





2 RechnernetzeKlausuren

2.1 SS16

Aufg1

Welche der OSI-Funktionsschichten umfasst dabei die LAN-Technik prinzipiell und was ist deren jeweilige Bezeichnung und deren Aufgabe (Kurzform)?

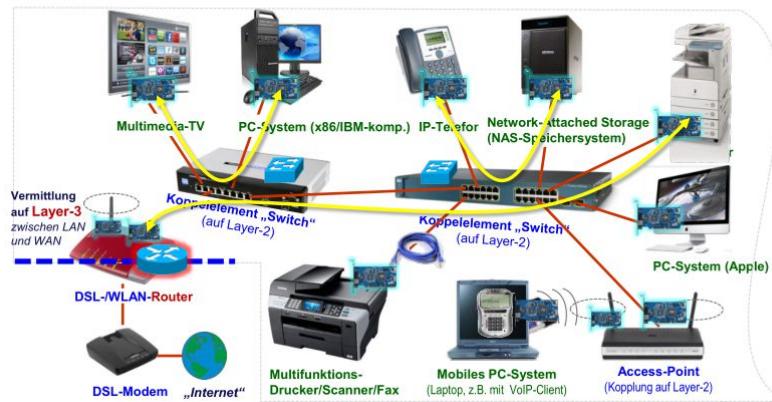
LAN-Technik realisiert den Layer-1 (Bitübertragung) und Layer-2 (Punkt-zu-Punkt/Mehrpunkt-Kommunikation).

Prinzipieller Aufbau eines typ. „Lokalen Netzes“ (LANs)



- Die **LAN-Technik** realisiert einen **direkten, physikalischen Datentransport zwischen einzelnen Netzinterfaces** über ein **sie verbindendes Medium**.

✗ Realisiert dabei den **Layer-1** (Bitübertragung) und **Layer-2** (Punkt-zu-Punkt/Mehrpunkt-Kommunikation)!



© Fachhochschule Wedel, Dipl.-Ing. (FH) I.Kaleck <http://www.fh-wedel.de/~kal>

16. Januar 2019

Folie Nr. 5

Wiederholung: OSI-Schichtenmodell

Kurzübersicht über die Schichtenfunktionen



- Mit Hilfe des **OSI-Modells** sollen die Anwendungen verschiedener Anbieter zukünftig einheitlich und herstellerunabhängig kommunizieren können.



© Fachhochschule Wedel, Dipl.-Ing.(FH) I.Kaleck <http://www.fh-wedel.de/~kal>

29. Oktober 2018

Folie Nr. 4



Welche Aufgabe hat in der IEEE 802 LAN-Architektur speziell der sog. MAC-Layer?

Die MAC ist die zweitunterste Schicht und umfasst Netzwerkprotokolle und Bauteile, die regeln, wie sich mehrere Rechner das gemeinsam genutzte physische Übertragungsmedium teilen. Sie wird benötigt, weil ein gemeinsames Medium nicht gleichzeitig von mehreren Rechnern verwendet werden kann, ohne dass es zu Datenkollisionen und damit zu Kommunikationsstörungen oder Datenverlust kommt. [Wikipedia]

Die Modellstruktur „Lokaler Netze“



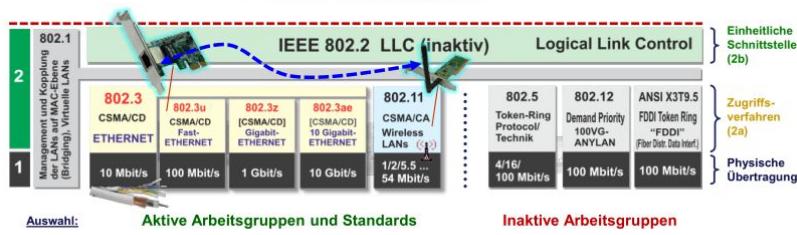
- Das **IEEE 802 LAN-Modell** erweitert den **OSI Data-Link Layer** (-2) um eine zusätzliche Zwischenschicht auf dann **zwei Sublayer** (2a,2b)

- Realisiert so einheitliche Schnittstelle zu den Netzwerkprotokollen

- **LLC – Logical Link Control Sublayer** (2b)
- **MAC – Media Access Control Sublayer** (2a)
- **PHY – PHYSical Control Layer** (1)

- ✗ Kennzeichnung spezifischer IEEE 802.x **Projektgruppen** (Task-Forces) innerhalb der IEEE 802.x Workgroup (WG) durch Suffix-Buchstaben (z.B. IEEE 802.3u)..

🌐 Übersicht z.B. unter "[IEEE 802.3 Ethernet Working Group](#)"



© Fachhochschule Wedel, Dipl.-Ing.(FH) I Kaleck <http://www.fh-wedel.de/~kal>

16. Januar 2019

Folie Nr. 7

Der Media Access Control Layer (MAC-Layer) in LANs



- Der **MAC-Layer** stellt je nach **Topologie** eines Netzes ganz unterschiedliche Arten (Klassen) von Medienzugriffsverfahren (MAC-Protokolle) bereit.

Deterministische Zugriffsverfahren

- ↳ Sendezzeitpunkt liegt in einem irgendwie bestimmbarer Zeitintervall
- ✗ Token-Passing (Token-Ring, FDDI, ArcNet-TokenBus), Demand-Priority (Anylan)



Stochastische Zugriffsverfahren

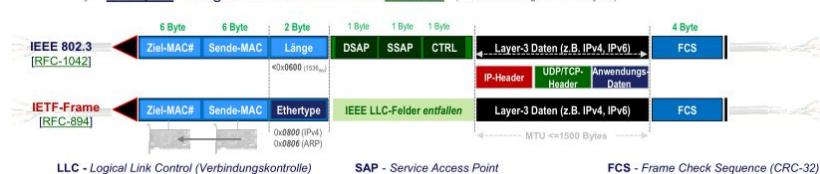
- ↳ Sendezzeitpunkt ist nicht exakt oder gar nicht bestimmbar (berechenbar)
- ✗ CSMA/CD (Ethernet), CSMA/CA (Wireless LANs im DCF-Betrieb)



Speicherung notwendiger Zusatzinformationen im MAC-Header

- ↳ Unterschiedliche MAC-Headerstrukturen je nach Zugriffsverfahren!

- ✗ Beispiel: Mögliche Ethernet MAC-Frames (Maximale Länge <= 1518 Bytes)



© Fachhochschule Wedel, Dipl.-Ing.(FH) I Kaleck <http://www.fh-wedel.de/~kal>

16. Januar 2019

Folie Nr. 10

Wozu genau dient beim MAC-Layer eine MAC-Adresse und wie sieht diese strukturell aus (mit Notation!)?

Anmerkungen zur MAC-Adresse in LANs



- Die **MAC-Adresse** ist die i.d.R. **weltweit eindeutige Adresse eines Netzwerk-interfaces für die Punkt-zu-Punkt/Mehrpunkt Kommunikation auf Layer-2**.

- Die Länge der Adresse beträgt **aktuell 6 Bytes bzw. 48-Bit**

~~X 3-Bytes~~ als Herstellerangabe (Organizationally Unique Identifier, OUI)

~~X 3 Bytes~~ durch den Hersteller frei nutzbar (z.B. laufende Kartennummer)



- Unterschiedliche Notationsformen:

AC-8E-48-F0-41-45 oder ac:8e:48:f0:41:45 oder ac8e.48f0.4145 (Cisco) ...

- **Layer-2 Broadcast Adresse** lautet **ff:ff:ff:ff:ff:ff**

• Zieladresse zum Erreichen aller Interfaces in gleichen Layer-2 Teilnetz.

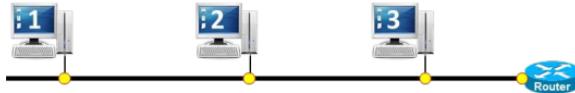
~~X~~ Empfangsbereich bildet umgekehrt eine Layer-2 Broadcast-Domain

• Erlaubt **Punkt-zu-Mehrpunkt** Kommunikation (in „Diffusionsnetzen“)

IEEE MAC-OUI Registrierung

- c) Wozu dient in einem LAN beim Transport von IPv4-Datenpaketen von einem zum anderen System speziell das „ARP“ (Protokoll) und wie ist dabei der Ablauf?

Erläutern Sie diesen Ablauf anhand der nachfolgenden Grafik:



Wikipedia: Es wird eine ARP-Anforderung (ARP Request) mit der MAC-Adresse und der IP-Adresse des anfragenden Computers als Senderadresse und der IP-Adresse des gesuchten Computers als Empfänger-IP-Adresse an alle Computer des lokalen Netzwerkes gesendet. Als Empfänger-MAC-Adresse wird dazu die Broadcast-Adresse ff-ff-ff-ff-ff-ff16 verwendet. Empfängt ein Computer ein solches Paket, sieht er nach, ob dieses Paket seine IP-Adresse als Empfänger-IP-Adresse enthält. Wenn dies der Fall ist, antwortet er mit dem Zurücksenden seiner MAC-Adresse und IP-Adresse (ARP-Antwort oder ARP-Reply) an die MAC-Quelladresse des Anforderers. Dieser trägt nach Empfang der Antwort die empfangene Kombination von IP- und MAC-Adresse in seine ARP-Tabelle, den sogenannten ARP-Cache, ein. Für ARP-Request und ARP-Reply wird das gleiche Paket-Format verwendet. In eigenen Worten: Zwei Computer möchten mittels der LAN-Technologie miteinander kommunizieren. Der anfragende PC schickt eine ARP-Request. Diese besteht aus folgenden Feldern: - Mac und IP-Adresse des Senders- Mac und IP-Adresse des Empfängers. Beim Request füllt der Sender seine Felder entsprechend aus, setzt die gewünschte IP-Adresse des Empfängers und gibt als Mac-Adresse die Broadcast Adresse an. Nun wird dieses Paket an alle Interfaces des Netzwerks weitergeleitet und der entsprechende PC antwortet mit einem ähnlich ausgefüllten Paket, dieses Mal nur mit ausgefüllter Mac-Adresse des Senders.

Übersicht: Das Address Resolution Protocol (ARP) im IPv4



- Das **ARP** dient in **LANS** zur Auflösung der **logischen Layer-3 Adresse (IPv4)** in die zugehörige **physikalische Layer-2 Adresse (IPv4- in MAC-Adresse)**.

- Spezifikation im [RFC-826: Ethernet Address Resolution Protocol] (STD 37)**

- ARP universell für Ethernet-, Arcnet-, Firewire-, ... Übertragungsnetze
- ✗ Eigene Layer-2 Protokoll bzw. MAC-Frametyp (Ethernettype-ID ist 0x0806).



- Ablauf**

- (1) Abfrage per **ARP-Request** als Layer-2 Broadcast (→FF:FF:FF:FF:FF:FF)
- (2) Empfänger sendet per **Unicast** einen **ARP-Reply** (mit eigener MAC-Adresse)
- Speicherung der Auflösung in Zwischenspeicher (**ARP-Cache**)

- Verwandte Funktionen**

- ✗ **Proxy-ARP** (Stellvertretender ARP-Reply für andere LAN-Interfaces)
- ✗ **Reverse-ARP** (Welche IPv4-Adresse gehört zur angegebenen MAC# ?)
- ✗ **Gratuitous-ARP** (u.a. zur Prüfung, ob eigene IPv4-Adresse bereits verwendet wird)



- Gefahrenpotential**

- ✗ **ARP-Spoofing** (Beschwindeln mit falschen ARP-Antworten/MAC-Adressen)

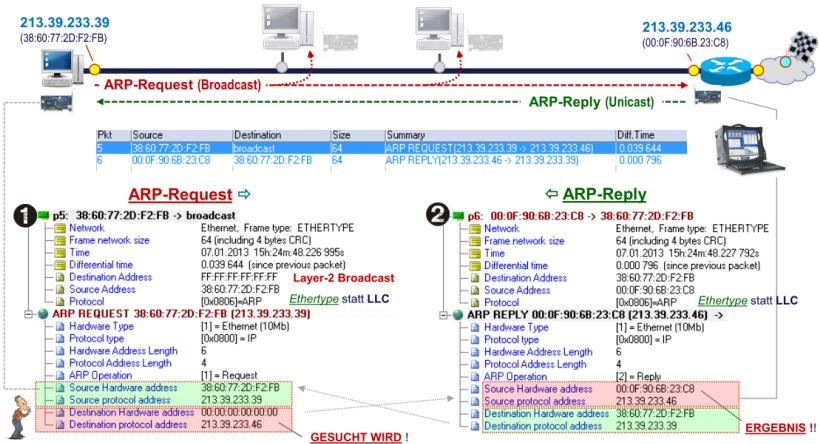
- **ARP-Funktion** wird im IPv6 per **Neighbor Discovery (ND)** Protokoll per **ICMPv6** realisiert

Analyse der Ermittlung einer MAC-Adresse per ARP



- Ein ARP-Request erreicht **alle Interfaces innerhalb des Layer-2 Teilnetzes**.

X Übermittlung im IPv4 per Layer-2 Broadcast; Antwort dann per Unicast-Nachricht



© Fachhochschule Wedel, Dipl.-Ing.(FH) I.Kaleck <http://www.fh-wedel.de/~kal>

16. Januar 2019

Folie Nr. 19

Wozu dient speziell das ARP-Dienstprogramm auf z.B. einem Windows-/Linux-System?

Der ARP-Zwischenspeicher (Cache)



- Das Dienstprogramm **arp** erlaubt die **Anzeige und Manipulation des lokalen ARP-Caches** auf einer Arbeitsstation.

Ändert oder zeigt „IP- zu MAC-Adressen“ - Umsetzungstabelle an.

ARP –? gibt ausführliche Hilfeinformationen

ARP -a [IP-Adresse] [-N Schnittstelle] [-v]

- Zeigt aktuelle ARP-Einträge für einzelne Adresse oder Schnittstellen als Tabelle an.

ARP -d IP-Adresse [Schnittstelle]

- Löscht den für eine Adresse angegebenen Hosteintrag, „*“ für alle Adressen

ARP -s IP-Adresse Ethernet-Adresse [Schnittstelle]

- Erlaubt statische Zuordnung von MAC-Adresse zu IP-Adresse

X Maßnahme u.a. gegen ARP-Spoofing (→IT-Sicherheit)



```
C:\>arp -a
Schnittstelle: 213.39.233.39 --- 0x20
  Internetadresse          Physische Adresse      Typ
  213.39.233.37            00-1c-c0-5c-f7-01    dynamisch
  213.39.233.46            00-0f-90-6b-23-c8    dynamisch
  213.39.233.47            ff-ff-ff-ff-ff-ff    statisch
  224.0.0.13               01-00-5e-00-00-0d    statisch
  255.255.255.255         ff-ff-ff-ff-ff-ff    statisch
```

engl. spoofing ... beschwindeln

© Fachhochschule Wedel, Dipl.-Ing.(FH) I.Kaleck <http://www.fh-wedel.de/~kal>

16. Januar 2019

Folie Nr. 20

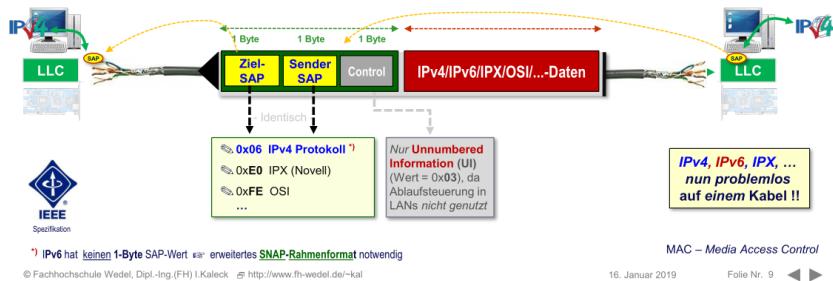
Wie kann der Empfänger eines Datenpaketes (Frames) in einem LAN prinzipiell feststellen ob ein Paket bei ihm wirklich fehlerfrei angekommen ist?

Da im LAN IPv4 Pakete übertragen werden ist es möglich anhand der Pakete selbst mittels der Prüfsumme zu überprüfen, ob die empfangenen Daten auch genauso abgeschickt wurden, da diese Teil des Paketes sind.

IEEE 802.2 – Logical Link Control Sublayer (LLC)

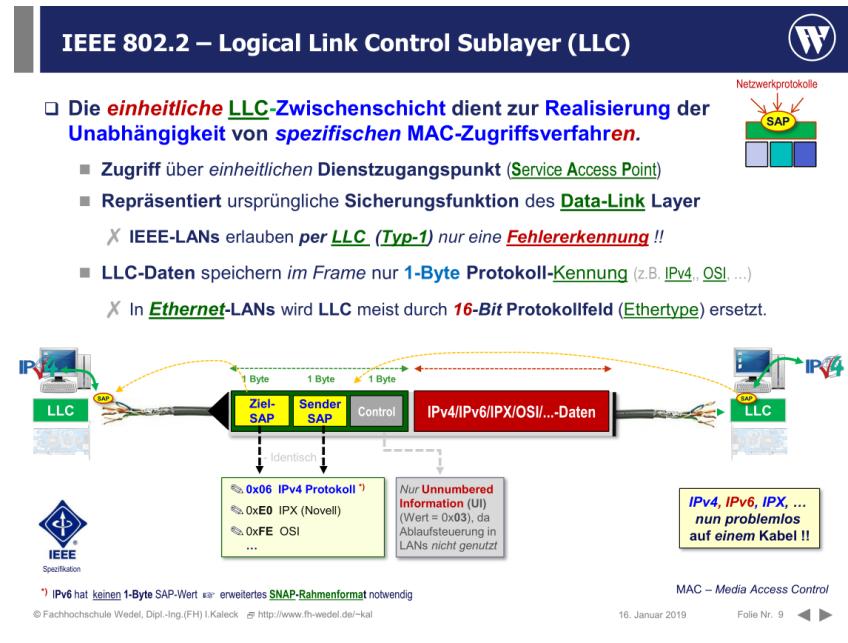


- Die **einheitliche LLC-Zwischenschicht** dient zur Realisierung der **Unabhängigkeit von spezifischen MAC-Zugriffsverfahren**.
 - Zugriff über **einheitlichen Dienstzugangspunkt (Service Access Point)**
 - Repräsentiert ursprüngliche Sicherungsfunktion des **Data-Link Layer**
 - ✗ IEEE-LANs erlauben per **LLC (Typ-1)** nur eine **Fehlererkennung !!**
 - LLC-Daten speichern im Frame nur **1-Byte Protokoll-Kennung** (z.B. **IPv4**, **OSI**, ...)
 - ✗ In **Ethernet-LANs** wird LLC meist durch **16-Bit Protokollfeld (Ethernetype)** ersetzt.



Zusatz: Beschreiben Sie die obere der beiden Layer-2 Sub-Schichten.

In eigenen Worten: Die obere Sub-Schicht der beiden Layer 2 Schichten stellt vier mögliche Dienstprotokolle zur Übertragung von Datenpaketen im LAN bereit. LLC (Logical Link Control):- Typ-1: verbindungsloser / ungesicherter Datagrammdienst- Typ-2: verbindungsorientierter Dienst- Typ-3: verbindungsloser Datagrammdienst mit Bestätigung- Typ-4: Punkt-zu-Punkt-Verbindung
ITWissen: Logical Link Control (LLC) ist ein OSI-Protokoll, das von der IEEE-Arbeitsgruppe 802 entwickelt wurde und für alle LAN-Subsysteme im Rahmen des Standards IEEE 802 gleich ist. Es handelt sich um die Steuerung der Datenübertragung auf der oberen Teilschicht der Sicherungsschicht, die im Ethernet-Schichtenmodell in die Sublayers Logical Link Control und Medium Access Control (MAC) unterteilt wurde. Logical Link Control kennt vier Dienstformen: Typ 1 kennzeichnet einen verbindungslosen, ungesicherten Datagrammdienst. Typ 2 kennzeichnet einen verbindungsorientierten Dienst. Typ 3 bezeichnet einen verbindungslosen Datagrammdienst mit Bestätigung und Typ 4 für Punkt-zu-Punkt-Verbindungen.

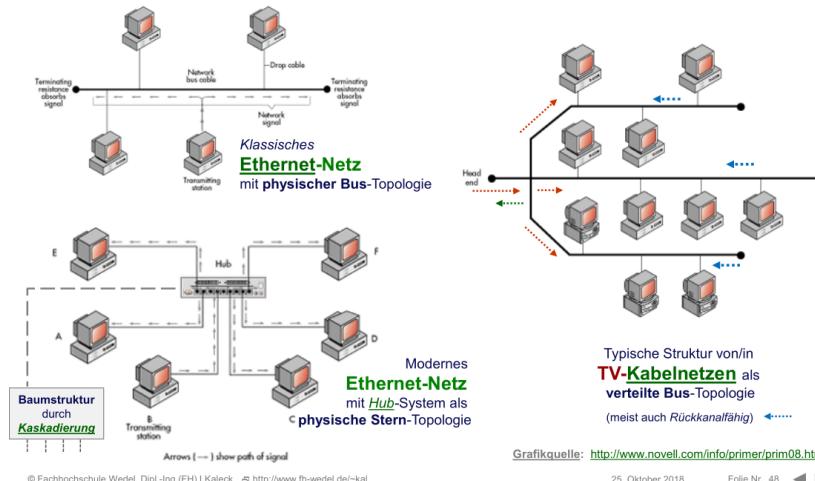


Erläutern Sie nun ganz allgemein den Begriff Hub-System zum technischen Aufbau eines Netzes. Welche physikalische Topologie ergibt sich dadurch und wo liegen hier Vorteile/Nachteile?

Unterschiedliche Topologie-Formen in Datennetzen (1)



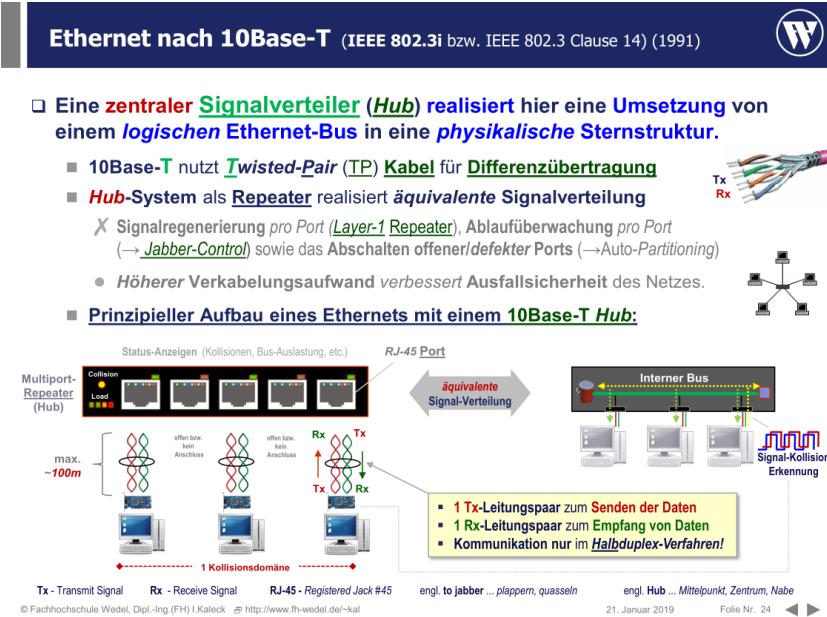
- **Sternstrukturen** schaffen i.d.R. (kosten-) effizient **sichere Übertragungswege**



Ein Hub-System besitzt einen primären Zugriffspunkt in Form eines Hubs/Routers an den alle Interfaces eines Netzwerks angeschlossen sind. Wenn nun ein Gerät ausfällt ist dies für das gesamte Netzwerk nicht von Bedeutung, es sei denn der Router selbst fällt aus. Da dies allerdings abzusehen ist kann man diesen gesondert schützen (z.B. in Form eines Backupgerätes). Mit einem Hub-System wird eine physikalische Stern-Topologie erzeugt bei welcher der primäre Zugriffspunkts mittig angeordnet ist und alle Geräte an diesen angeschlossen sind.

Skizzieren Sie nun aussagekräftig den Aufbau eines Ethernet-LANs mit so einem Hub-System und zwei PC-Arbeitsstationen nach dem klassischen 10Base-T. Welches bekannte Zugriffsverfahren kommt in diesem Netz zum Einsatz? Was bedeutet dabei der Begriff Kollisionsdomäne? (Zeichnen)

1. Wichtig, pro Arbeitsstation werden zwei Twisted-Pair-Adern-Kabel verwendet um die Ausfallsicherheit zu erhöhen. Wichtig zu erwähnen, der Switch ist sehr langsam... läuft nur im half-Duplex-Mode. Die Zahl, hier die 10 gibt die Datenübertragung in MBits und T steht für das Twisted Pair Kabel mit dem sämtliche Komponenten verbunden sind.



2. Es wird das CSMA/CD-Verfahren verwendet. ITWissen: CSMA/CD (Carrier Sense Multiple Access with Collision Detection) ist ein Zugangsverfahren mit Leitungsabfrage und Kollisionserkennung (Listen While Talking) nach einer Random-Access-Methode, das bei lokalen Netzen (LAN) in Bustopologie mit mehreren Netzwerkstationen den Zugriff auf das Übertragungsmedium regelt. Ist der Kanal frei, wird die Übertragung begonnen, jedoch frühestens nach dem Interframe Gap (IFG) nach Freiwerden des Mediums. Ist der Kanal belegt, wird der Kanal weiter überwacht, bis er als nichtbelegt erkannt wird. Die Zustände des Belegtseins bzw. Nichtbelegtseins werden durch Trägererkennung aus den Pegeländerungen auf dem Übertragungsmedium ermittelt. Tritt nach einer festgelegten Bitzeit eine Pegeländerung auf, so ist ein Trägersignal auf dem Kabel; in allen anderen Fällen gilt das Übertragungsmedium als nicht belegt. Während der Übertragung wird der Kanal weiter abgehört (Listen While Talking). Beginnt gleichzeitig eine zweite Station mit der Übertragung, dann werden die Daten bei der Stationen an einer Stelle des Netzwerks kollidieren, der Signalpegel auf dem Übertragungsmedium steigt an; man spricht vom Kollisionspegel. Da alle sendenden Stationen den Übertragungspegel auf dem Medium ständig überwachen, brechen diese Stationen bei Erkennen einer Kollision die Übertragung sofort ab und schicken ein spezielles Störsignal, das Jam-Signal, auf den Kanal. Nach Aussenden des Störsignals warten die Stationen eine bestimmte Zeit (Backoff)

und beginnen danach erneut die CSMA-Übertragung, beginnend mit dem ersten Schritt, dem Abhören des Mediums (Carrier Sensing).

Das klassische Ethernet-Zugriffsverfahren „CSMA/CD“

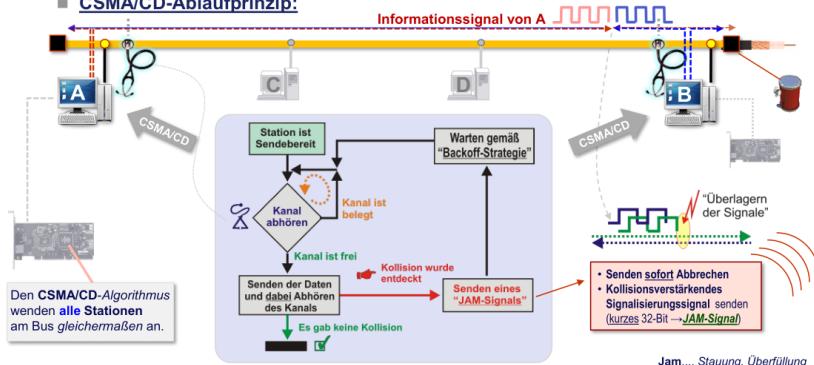


- Das **CSMA/CD** ist ein **Zugriffsverfahren** (Protokoll) für/auf eine **logische Bustopologie** (Bus) mit **mehreren, gleichberechtigten Teilnehmern**

- Carrier Sense, Multiple Access (with) Collision Detection (CD)**

X Zeigt nicht-deterministisches Sendeverhalten; arbeitet dezentral und ungesteuert

- CSMA/CD-Ablaufprinzip:**



© Fachhochschule Wedel, Dipl.-Ing.(FH) I.Kaleck <http://www.fh-wedel.de/~kal>

21. Januar 2019

Folie Nr. 9

Technische Ausführungen des klassischen 10Mbps-Ethernet



- Die **logische Topologie** bei Einsatz des **CSMA/CD-Verfahrens** ist **immer ein Bussystem** mit einem **Mehrfachzugriff** (→**Konkurrenzverfahren**)

X **Physikalisch** ist die **Nutzung unterschiedlicher Medien- und Topologie-Formen** möglich.

10 (Mbps) Base (→Baseband) 5 (Segment Length *100m | Media Indicator)

Standard-Bezeichnung	Gängige Bezeichnung	Darstellung des genutzten Mediums	Kabeltechnik	Physikalische Topologie
10Base-5 (IEEE 802.3)	Yellow-Cable		Massiv geschirmtes Koaxialkabel (Ø10,3mm) vom Typ RG-8 (50Ω)	Bus
10Base-2 (IEEE 802.3a)	Cheapernet bzw. Thin-LAN		Einfaches, flexibles Koaxialkabel (Ø 4,9mm), Typ RG-58 (50Ω)	Bus
10Base-T (IEEE 802.3i)	Twisted Pair		Paarweise verdrillte Kupferkabel (TP, Category-3, 100 Ω, 2 Paare)	Stern (mit Hub)
10Base-F (IEEE 802.3j)	LWL bzw. Fiber Optics Cable		Lichtwellenleiter, Multi- oder Monomode, 1 Faser je Richtung	Stern (mit Sternkoppler)
10Broad-36 (IEEE 802.3b)	Breitbandtechnik		Koaxialkabel, Ankopplung über ein <u>Kabelmodem</u>	Bus
1Base-5 (IEEE 802.3e)	Starlan		Sehr einfaches TP-Telefonkabel (2 Paare + 1 analog TK)	Stern (mit Hub)

Base – Baseband (unmodulierte Basisbandübertragung)

Broad – Broadband (Breitbandbandübertragung, moduliertes Signal auf Trägerfrequenz)

© Fachhochschule Wedel, Dipl.-Ing.(FH) I.Kaleck <http://www.fh-wedel.de/~kal>

21. Januar 2019

Folie Nr. 18

3. Im klassischen Ethernet sind alle Endgeräte an dem gleichen physikalischen Ethernet-Segment angeschlossen und erhalten über das Kollisionsverfahren Zugang auf das Übertragungsmedium. Ein solches Netzsegment mit eigenem Kollisionsverfahren bildet eine Kollisionsdomäne. Eine Kollisionsdomäne ist ein in sich geschlossenes LAN-Segment, das mit autarkem Kollisionsverfahren arbeitet. Der Hintergrund einer autarken Kollisionsdomäne ist in der steigenden Verzögerungszeit zu sehen, die mit der Anzahl der angeschlossenen Stationen

und der erhöhten Anzahl an Zugriffen auf das Übertragungsmedium rapide ansteigt. **Kollisionsdomäne:** Im klassischen Ethernet sind alle Endgeräte an dem gleichen physikalischen Ethernet-Segment angeschlossen und erhalten über das Kollisionsverfahren Zugang auf das Übertragungsmedium. Ein solches Netzsegment mit eigenem Kollisionsverfahren bildet eine Kollisionsdomäne.

In heutigen LANs wird nun aber fast ausschließlich die Switching-Technologie eingesetzt. Erläutern Sie den Begriff Ethernet-Switch. Wie arbeitet so ein Gerät prinzipiell?

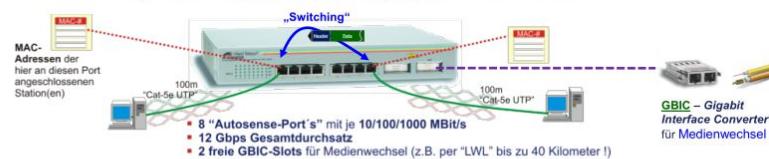
Ein Switch erlaubt die direkte Kopplung von N-Teilnetzen auf Layer-2 mittels N-Port Switch. Hierbei gibt es zwei wesentliche Verfahren. Einmal die cut-through Variante bei der die Weiterleitung direkt bei Erkennung der Ziel MAC Adresse erfolgt und einmal die klassisch genutzte store-and-forward Technik bei der bereits im Switch selbst überprüft wird ob die Pakete soweit in Ordnung sind oder ob sie defekt sind. Falls sie strukturelle Fehler aufweisen oder die Prüfsumme inkorrekt ist werden sie gelöscht. Anschließend wird geprüft ob die MAC Adresse bereits in der FDB gegeben ist oder nicht, falls nein wird das Paket auf allen Port ausgegeben falls ja wird das Paket an diese weitergeleitet.

Grundlegende Switching-Verfahren



■ Direkte Kopplung von N-Teilnetzen auf Layer-2 mittels N-Port Switch.

■ Beispiel: 8 (+2) Port 10/100/1000-Switch [von Allied Telesyn]



■ Store-and-forward (s&f) Technik (klassischer Bridging-Modus)

- Erst vollständige Zwischenspeicherung (Paketprüfung)
 - ↳ Falls korrekt, dann Weiterleitung (somit sicherer)
 - ✗ Unterschiedliche Geschwindigkeiten pro Port möglich (z.B. 10 ↔ 100 Mbps)



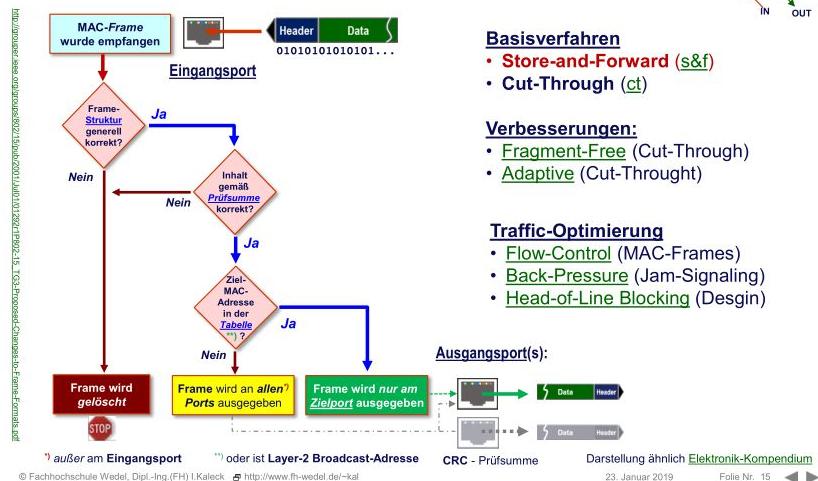
■ Cut-Through (ct) Verfahren (echtes Fast-Packet Switching)

- Weiterleitung bereits nach Erkennung der Ziel MAC Adresse
 - ↳ Transport direkt zum jeweiligen Ausgangsport
 - ↳ Verfahren ist schnell, leitet ggf. aber defekte Pakete weiter.
- ✗ Kein Wechsel der Geschwindigkeit möglich (z.B. 100 ↔ 100 Mbps)

Ablauf des Store-and-Forward-Verfahrens



Ablaufdiagramm zum Prinzip des
Store-and-Forward Verfahrens im Switch



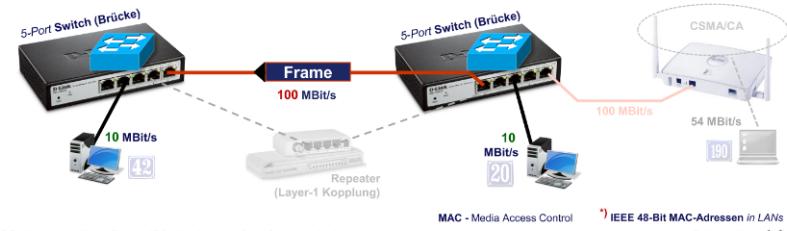
Wiederholung: Definition Switch

Eine Brücke (Switch) zur Kopplung auf dem Layer-2



□ Eine Brücke (Bridge, Switch) dient zur Kopplung auf dem OSI-Layer (2).

- Kopplung benachbarter Teilnetze auf dem Data-Link Layer
 - ↳ Realisiert daher abschnittsweise Punkt-zu-Punkt oder Punkt-zu-Mehrpunkt Kommunikation (ggf. gesichert)
 - ↳ Benötigt einheitliche Layer-2 Adressen für jedes angeschlossene Interface
 - ✗ Es reichen dazu einfache numerische Werte) 20 42 190
- Auch ein Wechsel des Medienzugriffsverfahrens (→MAC-Protocol) ist hier prinzipiell an allen Interfaces („Ports“) dieses Koppelementes möglich.
 - ✗ CSMA/CD (Ethernet) ↔ Token-Passing ↔ CSMA/CA (Wireless LAN)



Welche konkrete Aufgabe hat in einem Ethernet-Switch die interne Forwarding Database (FDB) Tabelle? Skizzieren Sie dazu grob deren prinzipiellen Aufbau. Was wird wozu gespeichert? Woher stammt hier ein Eintrag in dieser Tabelle und wer löscht diesen ggf. wieder? Wann wird in einem Switch ggf. ein MAC-Frame auch mal nicht weitergeleitet.

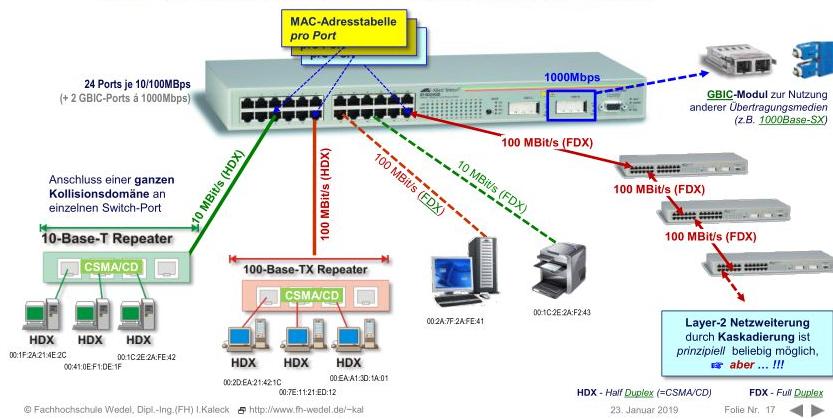
Einträge werden per *Self-Learning Algorithmus* ermittelt. Funktionsweise: Wenn ein Endgerät ein Paket aussendet und der Switch die Sender Adresse nicht kennt wird ein neuer Eintrag angelegt. Wenn die Empfänger Adresse ebenfalls nicht in der FDB steht wird das Paket an alle Ports (bis auf den des Senders) weitergeleitet, ansonsten natürlich nur an die Zieladresse. Dieser Vorgang wird auch als Flooding bezeichnet. Diese Tabelle verbindet die Portnummern mit allen an dem jeweiligen Port angeschlossenen Endgeräten. Wichtig hierbei, falls weitere Hub-Systeme an einem Port angeschlossen sein sollten wird die Adresse des Switches, etc. nicht in die FDB der Parent-Instanz eingetragen. Diese Tabelle wird vom Switch selbst genutzt um Datenpaketen den Empfänger / Absender mit den MAC-Adressen der Pakete in Verbindung zu bringen.

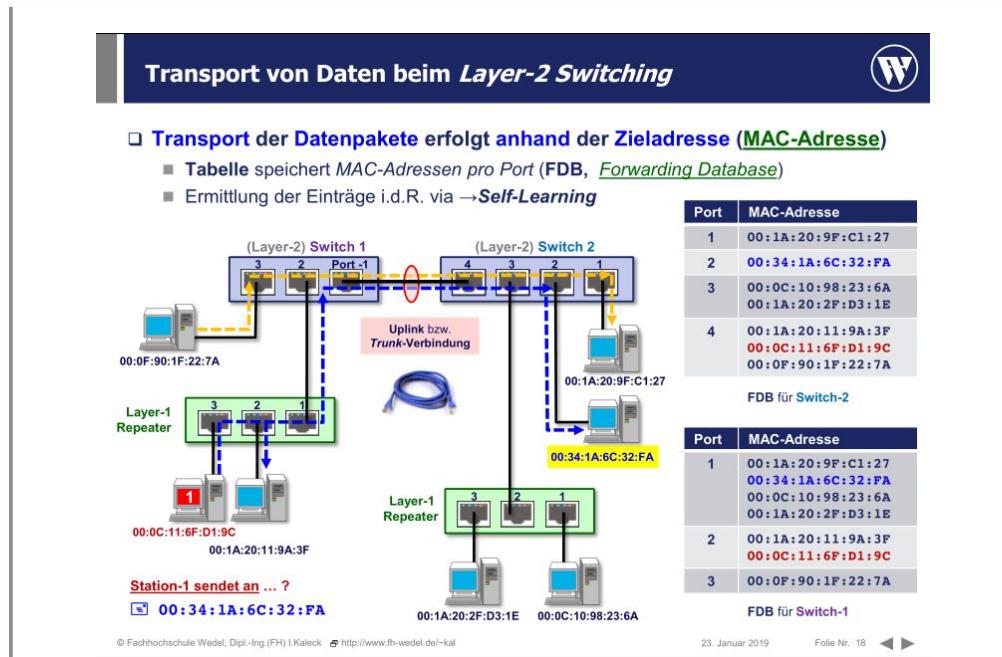
Anschlussmöglichkeiten an einen „Switch“ (Switching Hub)



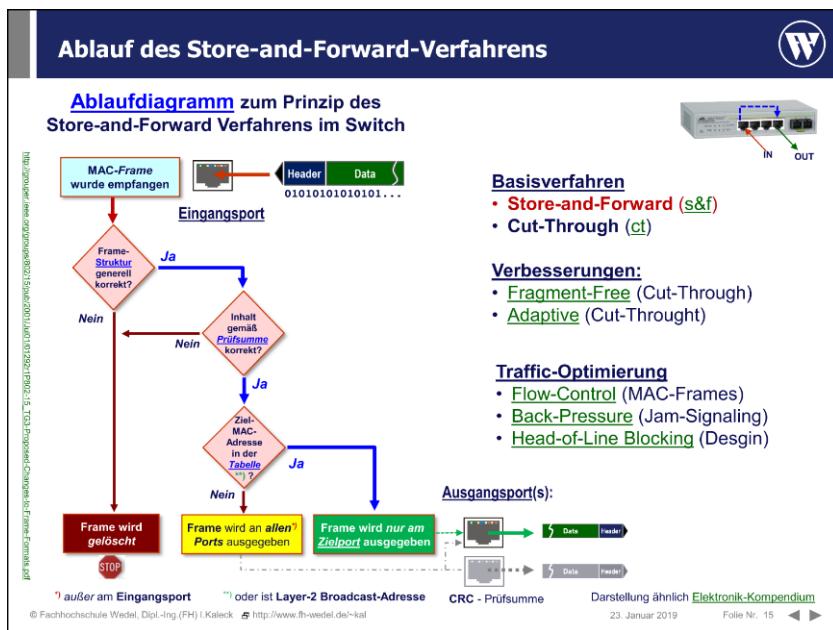
- An einen **Switch-Port** können **einzelne Endgeräte**, aber auch **weitere Hubsysteme** (z.B. Switch- bzw. Repeater-Interfaces) angeschlossen werden.

- **Senden/Empfangen im Full-Duplex Modus** wird *pro Port* entschieden
- **Tabelle** speichert MAC-Adressen pro Port (**FDB**, *Forwarding Database*)





Todo: Besprechen Wenn mittels Store-and-Forward gearbeitet wird und die Struktur des Frames oder die Prüfsumme inkorrekt ist wird der Frame verworfen. Außerdem muss das TTL größer Null sein.



Welche beiden grundlegenden Switching-Verfahren (Prinzipien) kennen Sie? Erläutern Sie ganz kurz (stichwortartig) deren jeweiliges Arbeitsprinzip und auch wo hier die jeweiligen Vor- bzw. ggf. auch Nachteile liegen?

Store-and-forward Technik: Vollständige Zwischenspeicherung der Pakete um diese einer Prüfung zu unterziehen. (Defekte Pakete werden nicht weitergeleitet, ist allerdings rel. langsam)
Cut-Through Verfahren: Weiterleitung bereits nach Erkennung der Ziel MAC Adresse (Schnelles Weiterleiten, im Zweifelsfall werden aber auch defekte Pakete zugestellt)

Grundlegende Switching-Verfahren



Direkte Kopplung von N-Teilnetzen auf Layer-2 mittels N-Port Switch.

Beispiel: 8 (+2) Port 10/100/1000-Switch [von Allied Telesyn]

- MAC-Adressen der hinter diesen Port angeschlossenen Station(en)
- „Cat-5e UTP“
- „Switching“
- MAC-Adresse
- 100m „Cat-5e UTP“
- GBIC – Gigabit Interface Converter für Medienwechsel
- 8 „Autosense-Port's“ mit je 10/100/1000 MBit/s
- 12 Gbps Gesamtdurchsatz
- 2 freie GBIC-Slots für Medienwechsel (z.B. per „LWL“ bis zu 40 Kilometer !)

Store-and-forward (s&f) Technik (klassischer Bridging-Modus)

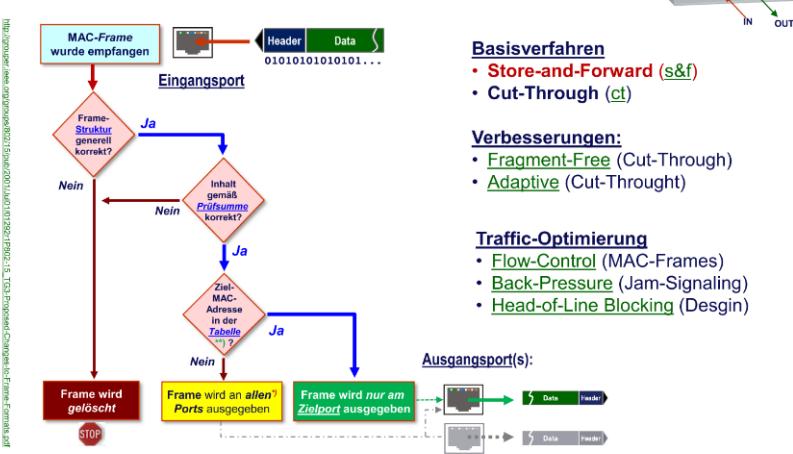
- Erst vollständige Zwischenspeicherung (Paketprüfung)
 - Falls korrekt, dann Weiterleitung (somit sicherer)
 - Unterschiedliche Geschwindigkeiten pro Port möglich (z.B. 10 ↔ 100 Mbps)

Cut-Through (ct) Verfahren (echtes Fast-Packet Switching)

- Weiterleitung bereits nach Erkennung der Ziel MAC Adresse
 - Transport direkt zum jeweiligen Ausgangsport
 - Verfahren ist schnell, leitet ggf. aber defekte Pakete weiter.
- Kein Wechsel der Geschwindigkeit möglich (z.B. 100 ↔ 100 Mbps)

Ablauf des Store-and-Forward-Verfahrens

Ablaufdiagramm zum Prinzip des Store-and-Forward Verfahrens im Switch



```

graph TD
    A[MAC-Frame wurde empfangen] --> B{Frame-Struktur generell korrekt?}
    B -- Ja --> C{Inhalt genauso Prüfsumme korrekt?}
    C -- Ja --> D{Ziel-MAC-Adresse in der Tabelle?}
    D -- Ja --> E[Frame wird nur am Zielport ausgegeben]
    D -- Nein --> F[Frame wird an allen Ports ausgegeben]
    C -- Nein --> G[Frame wird gelöscht STOP]
    E --> H[Ausgangsport(s):]
    F --> H
    H --> I[CRC - Prüfsumme]
    I --> J[„ oder ist Layer-2 Broadcast-Adresse“]
  
```

Basisverfahren

- Store-and-Forward (s&f)
- Cut-Through (ct)

Verbesserungen:

- Fragment-Free (Cut-Through)
- Adaptive (Cut-Through)

Traffic-Optimierung

- Flow-Control (MAC-Frames)
- Back-Pressure (Jam-Signaling)
- Head-of-Line Blocking (Desgin)

Ausgangsport(s):

* außer am Eingangsport ** oder ist Layer-2 Broadcast-Adresse

© Fachhochschule Wedel, Dipl.-Ing.(FH) I.Kaleck <http://www.fh-wedel.de/~kal>

CRC - Prüfsumme Darstellung ähnlich Elektronik-Kompendium

Erläutern Sie nun kurz bzw. stichwortartig die wesentlichen Eigenschaften der in der Internet-Architektur zur Verfügung stehenden beiden Transportprotokolle TCP und UDP.

UDP: *User Datagram Protocol* Das UDP stellt eine sehr einfach, verbindungslose und ungesicherte Datenübertragung zwischen Anwendungsprozessen bereit. (+ Schnelle Übertragung - da keine Verbindung aufgebaut werden muss; - ungesichert - Pakete können verändert / verloren gehen)

TCP: *Transmission Control Protocol* Das TCP realisiert eine verbindungsorientierte, gesicherte Übertragung von Datenströmen zwischen jeweils (genau) zwei Prozessen. (+ Gesicherte Übertragung - Was gesendet wurde kommt sicher an; - Zeit-/Ressourcenaufwendig)

Die Eigenschaften des User Datagram Protocols (UDP)



- Das **UDP** stellt eine sehr **einfache, verbindungslose** und **ungesicherte** Datenübertragung zwischen **Anwendungsprozessen** bereit [RFC 768, STD 6].

- Bietet einen rein **nachrichtenorientierten Datenaustausch**

- Übermittlung einzelner, unabhängiger **Datagramme** (UDP-Pakete).

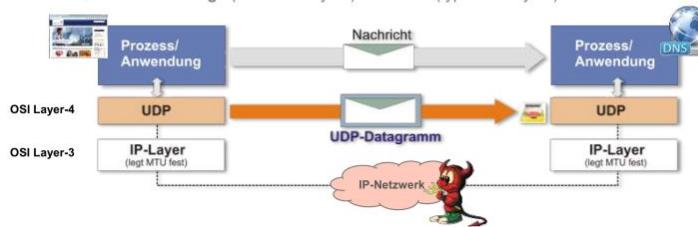


- **Maximale Länge einer UDP-Nachricht** durch **IP-Layer beschränkt**.

- ✗ IP und UDP verwenden je ein **16-Bit Längenfeld** (0 ... $2^{16}-1$ bzw. 65535 Bytes).

- ✗ IP-**Fragmentierung** bereits durch den **Absender** möglich/nötig.

- ↳ UDP-Paketlänge (z.B. 4000 Bytes) > IP-MTU (typ. 1500 Bytes)



DNS - Domain Name System (Namensauflösung in IP-Adressen)

MTU - Maximum Transmission Unit (Ethernet~1500 Bytes)

© Fachhochschule Wedel, Dipl.-Ing. (FH) I.Kaleck, <http://www.fh-wedel.de/~kal>

19. November 2018

Folie Nr. 10

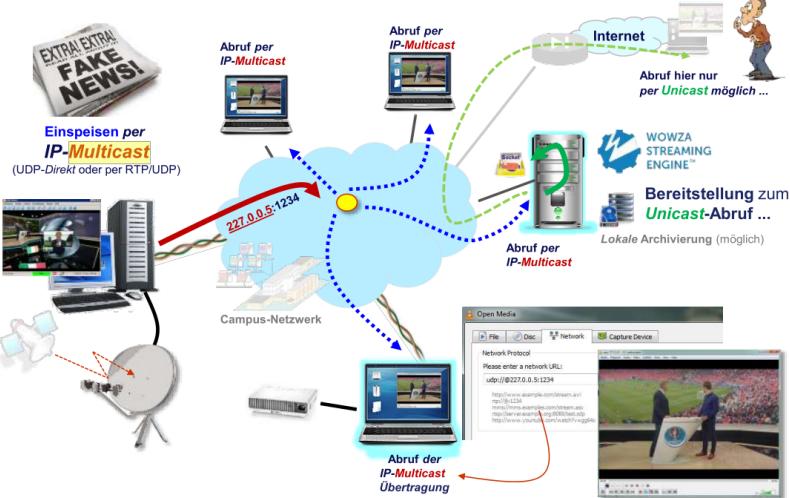


Aufg2

Erläutern sie kurz an einem Anwendungsbeispiel den Begriff des **IP-Multicasting**. Wozu dient diese Technik und welche Art von IPv4-Adressen wird dabei verwendet? Geben sie auch ein konkretes Adressbeispiel mit an. Warum ist diese Technik der traditionellen Broadcast-Addressierung ggf. vorzuziehen (Vorteile)? Wie kann im IPv4 die Reichweite (Verteilungsbereich) einer Multicast-Übertragung im gesamten Netz geregelt werden (z.B. beim IP-TV)?

In eigenen Worten: Mit IP-Multicast ist es möglich z.B. einen Videostream nur einer Gruppe von Rechnern aus dem eigenen Teilnetz zu zeigen. Hierzu wird eine Class D Adresse verwendet. Die Rechner der Gruppe können sich über das IGMP in die Gruppe *einschreiben* bzw. aus ihr *austreten*. Beispieladresse: 227.0.0.3:1234 ITWissen: IP-Multicast ist eine Routing-Technik, bei der der IP-Verkehr von einer oder von mehreren Datenquellen an mehrere Zielstationen gesendet wird. Es kann sich also um eine Punkt-zu-Mehrpunkt-Verbindung (P2MP) handeln oder um eine Mehrpunkt-zu-Mehrpunkt-Verbindung. Vorteil: Verwendung Multicast gegenüber Broadcast-Da per Multicast nur ausgewählte Gruppen mit Informationen versorgt werden schont dies die Traffic-Auslastung des Netzwerks. Es werden keine bzw. wenig unnötige Pakete versendet was beim Broadcast unvermeidbar ist.

Beispiel: „Event-TV“ auf dem Campus empfangen ...



© Fachhochschule Wedel, Dipl.-Ing (FH) I. Kaleck <http://www.fh-wedel.de/~kal>

19. November 2018

Folie Nr. 21

Wiederholung: Aufschlüsselung der einzelnen Adressklassen

Übersicht: Einfache IPv4-Netzklassen (Classfull IP-Addressing)



- Der [RFC-791: Internet Protocol] spezifiziert die **implizite Festlegung** einer Grenze zwischen **Netz- und Hostadressanteil** auf **festen Bytegrenzen**.

X Nur der **Hostbereich** (Bits) steht dem **Netzinhaber** zur lokalen Vergabe frei !



Klasse	1. Byte	2. Byte	3. Byte	4. Byte	Netze/Hosts
A	0nnnnnnn 0-127	hhhhhhh 0-255	hhhhhhh 0-255	hhhhhhh 0-255	128 $/2^{24}$
B	10nnnnnn 128-191	nnnnnnnn 0-255	hhhhhhh 0-255	hhhhhhh 0-255	16.384 $/2^{16}$
C	110nnnnn 192-223	nnnnnnnn 0-255	nnnnnnnn 0-255	hhhhhhh 0-255	2.097.152 $/2^8$
D	1110gggg 224-239	gggggggg 0-255	gggggggg 0-255	gggggggg 0-255	2²⁸ Gruppen-adressen
E	1111xxxx 240-255	xxxxxxxx	xxxxxxxx	xxxxxxxx	Rein experimenteller Bereich (reserviert)

*) in der Adresse **selbst** hinterlegt bzw. kodiert.

$2^{32} = \sim 4$ Mrd.

$2^{24} = \sim 16$ Mio.

© Fachhochschule Wedel, Dipl.-Ing.(FH) I.Kaleck <http://www.fh-wedel.de/~kal>

19. November 2018

Folie Nr. 38



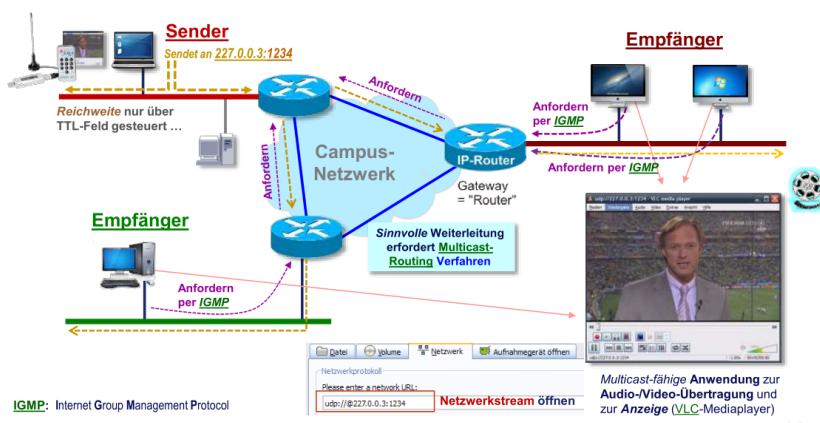
Welches der oben genannten Transportprotokolle (UDP / TCP) kann bei der Multicast-Technik zum Einsatz kommen und warum (Begründung)?

Übertragung per IP-Multicasting nur mittels UDP



- Nur mit dem **UDP** können Datenpakete **gleichzeitig** auch an eine **Gruppe** von **unbekannten Empfängern** (~Prozessen, ~Interfaces) übertragen werden.

X **Multicast-Adressen** im Bereich **224.0.0.0/4** dienen zur **Identifikation** einer **Empfängergruppe**



© Fachhochschule Wedel, Dipl.-Ing.(FH) I.Kaleck <http://www.fh-wedel.de/~kal>

19. November 2018

Folie Nr. 22



Beim TCP kommt es sogar schon beim Verbindungsauflauf zu Problemen wenn die Kommunikationspartner nicht genau feststehen.

Welche Bedeutung hat im Rahmen der Kommunikation zwischen Programmen (Prozessen) dabei der Begriff (UDP-/TCP) Socket? Was genau stellen in diesem Zusammenhang sog. Ports (bzw. Portnummern) dar und wie sehen diese hier konkret aus?

Unterschied zwischen Port und Socket: Ein Port ist der physikalische und ein Socket der logische Endpunkt einer Kommunikation (definiert durch eine IP-Adresse und einen Port im Kontext einer bestimmten Verbindung). ITWissen: Als Socket wird die Adressenkombination aus IP-Adresse und Portnummer bezeichnet mit der eine bestimmte Anwendung auf einem bestimmten Rechner angeprochen werden kann. Mit der IP-Adresse wird das Netzwerk und der Rechner bestimmt und mit der die Portnummer die Anwendung auswählt. An einem geg. Port hängt aber nicht nur ein Prozess der so angesteuert werden kann, sondern auch ein Transportprotokoll welches die Daten *in Empfang nimmt*.

Das Prinzip der Kommunikation über „Sockets“



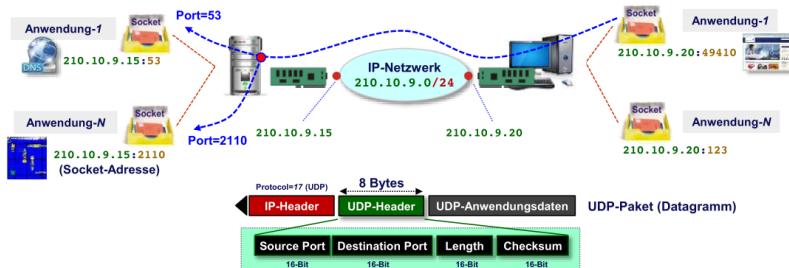
- Der Austausch von UDP-Nachrichten (Datagrammen) zwischen Prozessen erfolgt über zugeordnete Kommunikationsendpunkte (→ Sockets).

X UDP-Sockets dienen zum Senden und Empfangen von Nachrichten.

■ Lokale Kennzeichnung (Adressierung) eines Sockets durch Portnummer („Port“)

↳ 16-Bit Wert (0..65535), lokal mit dynamischer oder manuelle Festlegung.

↳ Eindeutige Socket-Adresse per „IP-Adresse & Portnummer“ (☞ 210.10.9.15:2110)



Bedeutung von Ports: Werden benötigt um einen Prozess eindeutig identifizieren zu können.

Die Bedeutung von *Sockets, Ports, Portnummern, ... ??*

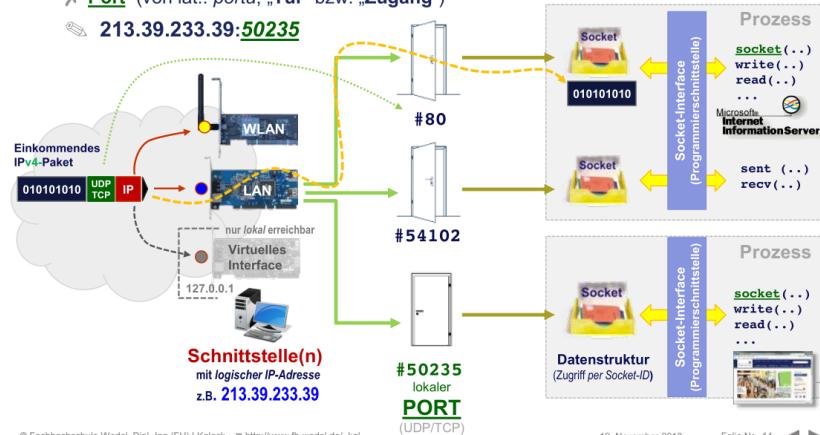


- Ein **Socket** wird über die **eindeutige Socket-Adresse** erreicht (**Lokal, Netz**).

X **Socket** (engl. Sockel, Fassung, Steckdose oder auch Steckverbindung)

X **Port** (von lat.: *porta*, „Tür“ bzw. „Zugang“)

213.39.233.39:**50235**



© Fachhochschule Wedel, Dipl.-Ing.(FH) I. Kaleck ⌂ http://www.fh-wedel.de/~kal

19. November 2018

Folie Nr. 14

Die Bedeutung von „Ports“ (-Nummern)



- Das **Port-Konzept** realisiert die **gleichzeitige**) Übertragung der **Daten** mehrerer Prozesse per **UDP-** bzw. **TCP** über einzelnen IP-Layer

█ [RFC-6335] legt Registrierungsprozess und drei **Bereiche** von **Ports** fest.

X [RFC-3232]: Assigned Numbers: [RFC 1700 is Replaced by an On-line Database](#)



Bereich	Portnummer	Bedeutung	Festlegung
System Ports (well-known)	0 bis 1023 (0x0..0x3ff)	Privilegierte Ports für standardisierte Internet-Systemprozesse (Hinweis: Unix-Prozesse benötigen hierfür i.d.R. eine →root-Kennung)	Zuweisung direkt durch die IETF
User Ports (registered)	1024 bis 49151 (0x400..0xbfff)	Konfliktvermeidung von Ports bei bekannten Anwendungen (...as a convenience to the community...)	Online-Registrierung bei der IANA
Dynamic Ports (private/ ephemeral)	49152 bis 65535 (0xc000..0xffff)	Ports zur kurzfristigen, dynamischen Nutzung durch beliebige Anwenderprozesse; zur Anforderung einer bel. freien Portnummer bei Socket-Initialisierung	Verwaltung des Bereichs <i>lokal</i> durch eigenen IP-Stack (ggf. einstellbar)

↗ **Multiplexing**

ephemeral ... vergänglich, kurzlebig, vorübergehend, flüchtig ...

© Fachhochschule Wedel, Dipl.-Ing.(FH) I. Kaleck ⌂ http://www.fh-wedel.de/~kal



19. November 2018

Folie Nr. 13

Was genau ist eine sog. Socket-Adresse (mit typischer Notation) und wozu ist diese notwendig?

Das Prinzip der Kommunikation über „Sockets“



- Der Austausch von **UDP-Nachrichten** (**Datagrammen**) zwischen **Prozessen** erfolgt über **zugeordnete Kommunikationsendpunkte** (→**Sockets**).

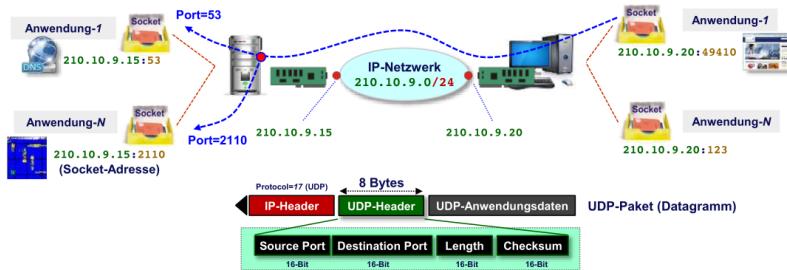
X **UDP-Sockets** dienen zum **Senden** und **Empfangen** von **Nachrichten**.



■ **Lokale Kennzeichnung** (Adressierung) eines **Sockets** durch **Portnummer** („Port“)

↳ 16-Bit Wert (0..65535), lokal mit *dynamischer* oder *manuelle* Festlegung.

↳ Eindeutige **Socket-Adresse** per „**IP-Adresse & Portnummer**“ (↳ 210.10.9.15:2110)



Was genau stellen in diesem Zusammenhang eigentlich Ports (bzw. Portnummern) dar und warum benötigt man so etwas zwingend?

IT-Wissen: Ein Port ist ein Ein- oder Ausgang einer Einheit. Es kann sich um einen Verbindungspunkt für ein Peripheriegerät, für peripherie Einheiten oder ein Anwendungsprogramm handeln. Ein Port kann logisch, physikalisch oder beides sein um einen Prozess eindeutig identifizieren zu können.

Die Bedeutung von *Sockets, Ports, Portnummern, ... ??*



- Ein **Socket** wird über die **eindeutige Socket-Adresse** erreicht (**Lokal, Netz**).

✗ **Socket** (engl. Sockel, Fassung, Steckdose oder auch Steckverbindung)

✗ **Port** (von lat.: *porta*, „Tür“ bzw. „Zugang“)

✗ 213.39.233.39:**50235**



© Fachhochschule Wedel, Dipl.-Ing.(FH) I.Kaleck <http://www.fh-wedel.de/~kal>

19. November 2018

Folie Nr. 14

Die Bedeutung von „Ports“ (-Nummern)



- Das **Port-Konzept** realisiert die **gleichzeitige[†]** Übertragung der **Daten** mehrerer **Prozesse** per **UDP-** bzw. **TCP** über **einzelnen IP-Layer**

■ [RFC-6335] legt **Registrierungsprozess** und **drei Bereiche** von **Ports** fest.

✗ [RFC-3232]: Assigned Numbers: [RFC 1700 is Replaced by an On-line Database](#)

Bereich	Portnummer	Bedeutung	Festlegung
System Ports (well-known)	0 bis 1023 (0x0..0x3ff)	Privilegierte Ports für standardisierte Internet-Systemprozesse (Hinweis: Unix-Prozesse benötigen hierfür i.d.R. eine →root-Kennung)	Zuweisung direkt durch die IETF
User Ports (registered)	1024 bis 49151 (0x400..0xbfff)	Konfliktvermeidung von Ports bei bekannten Anwendungen (...as a convenience to the community...)	Online-Registrierung bei der IANA
Dynamic Ports (private/ ephemeral)	49152 bis 65535 (0xc000..0xffff)	Ports zur kurzfristigen, dynamischen Nutzung durch beliebige Anwenderprozesse; zur Anforderung einer bel. freien Portnummer bei Socket-Initialisierung	Verwaltung des Bereichs <i>lokal</i> durch eigenen IP-Stack (ggf. einstellbar)

[†] ~Multiplexing

ephemeral ... vergänglich, kurzlebig, vorübergehend, flüchtig ...

© Fachhochschule Wedel, Dipl.-Ing.(FH) I.Kaleck <http://www.fh-wedel.de/~kal>



19. November 2018

Folie Nr. 13

Welche drei grundlegenden Bereiche von Ports (bzw. Portnummern) kennen Sie und wozu dienen diese jeweils bzw. was ist ihre jeweilige Bedeutung?

Die Bedeutung von „Ports“ (-Nummern)



- Das **Port-Konzept** realisiert die **gleichzeitige¹⁾ Übertragung der Daten** mehrerer **Prozesse per UDP- bzw. TCP** über **einzelnen IP-Layer**

 [\[RFC-6335\]](#) legt **Registrierungsprozess** und **drei Bereiche** von **Ports** fest.

 [\[RFC-3232\]](#): Assigned Numbers: [RFC 1700](#) is Replaced by an [On-line Database](#)



Bereich	Portnummer	Bedeutung	Festlegung
System Ports (well-known)	0 bis 1023 (0x0..0x3ff)	Privilegierte Ports für standardisierte Internet-Systemprozesse (Hinweis: Unix-Prozesse benötigen hierfür i.d.R. eine →root-Kennung)	Zuweisung direkt durch die IETF
User Ports (registered)	1024 bis 49151 (0x400..0xbfff)	Konfliktvermeidung von Ports bei bekannten Anwendungen (...as a convenience to the community...)	Online-Registrierung bei der IANA
Dynamic Ports (private/ ephemeral)	49152 bis 65535 (0xc000..0xffff)	Ports zur kurzfristigen, dynamischen Nutzung durch beliebige Anwenderprozesse; zur Anforderung einer bel. freien Portnummer bei Socket-Initialisierung	Verwaltung des Bereichs <i>lokal</i> durch eigenen IP-Stack (ggf. einstellbar)

¹⁾ **Multiplexing**

ephemeral ... vergänglich, kurzlebig, vorübergehend, flüchtig ...



Internet Assigned Numbers Authority

© Fachhochschule Wedel, Dipl.-Ing.(FH) I.Kaleck <http://www.fh-wedel.de/~kal>

19. November 2018

Folie Nr. 13



Wie bzw. mit welchem bekannten Dienstprogramm kann man (per Kommandozeile) abprüfen, ob auf dem eigenen System im Hintergrund z.B. ein TELNET-Server oder auch andere Anwendungen (Prozesse) auf einkommende Verbindungen warten? Wie lautet dazu der typische Aufruf (z.B. unter Windows)?

(C://) netstat -n Erklärung -n: Zeigt Adressen und Portnummern numerisch an.

Kann man mit dem bekannten PING-Dienstprogramm interaktiv (per Kommandozeile) abprüfen ob auf einem entfernten System ein HTTP-Serverdienst tatsächlich aktiv bzw. erreichbar ist? Erläutern Sie dazu kurz aber hinreichend detailliert diesen Sachverhalt bzw. die Arbeitsweise dieses Dienstprogramms. Wie lautet (z.B. unter Windows) der Aufruf eines dafür geeigneten Dienstprogramms?

Das Dienstprogramm PING fordert mit der ICMP-Funktion ECHO-Request einen zugehörigen ECHO-Reply an. Dazu sendet es mehrere Pakete und misst dabei jeweils die Zeit bis zur Ankunft der Antwort. Falls ein Paket unterwegs verloren gegangen sein soll kann dies mehrere Gründe haben (siehe Screenshot).

Zugehörige TCP/IP Dienstprogramme (1)



- Das Dienstprogramm **PING** (→Packet Internet Groper) fordert mit der **ICMP-Funktion ECHO-Request** einen zugehörigen **ECHO-Reply** an.

- **PING** sendet mehrmals und misst jeweils die Zeit bis zur Antwort der Antwort.

Request-Paket wird mit Dummy-Daten aufgefüllt, Länge ist einstellbar

ping localhost (ping 127.0.0.1) prüft lokale IP-Konfiguration (IP-Stack)

ipconfig (Windows) bzw. ifconfig (Linux) zur Interface-Anzeige.

```
C:\>ping stud
Ping für vsrv-stud.fh-wedel.de [213.39.232.215] mit 32 Bytes Daten:
Antwort von 213.39.232.215: Bytes=32 Zeit<1ms TTL=62

Ping-Statistik für 213.39.232.215:
  Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0(0% Verlust),
  Ca. Zeitangaben in Millisek.:
    Minimum = 0ms, Maximum = 0ms, Mittelwert = 0ms
C:\>
```

Beachte: Der reine Hostname **stud** wird zunächst vom Client-Resolver auf **stud.fh-wedel.de (FQDN)** erweitert.

Groper ... engl. Abtaster

© Fachhochschule Wedel, Dipl.-Ing.(FH) I.Kaleck <http://www.fh-wedel.de/~kal>

16. Januar 2019

Folie Nr. 6

PINGing von Zielen im NETZ



- Das **PING-Programm** sendet den **ICMP-Request** direkt an das **Ziel**system.

- Bleibt ein ICMP-**Reply** Antwortpaket aus, ist die Ursache dafür nicht eindeutig!

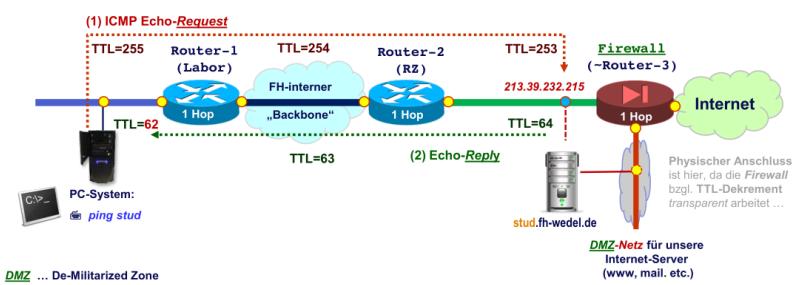
(1) Einer der beteiligten Router kennt **keinen Weg** zum Zielnetz.

(2) Das Zielsystem (ein Host oder Router) ist **selbst gar nicht aktiv**

(3) Einer der Router oder das Ziel **selbst kennt keinen Weg zurück** (zum Sender)

- ✗ Mittels ICMP ist **keine Aussage** über auf dem Zielsystem **laufende Prozesse** möglich!

Eingabe von „telnet <ip-adresse> <port>“ prüft direkt die Erreichbarkeit von TCP-Sockets



© Fachhochschule Wedel, Dipl.-Ing.(FH) I.Kaleck <http://www.fh-wedel.de/~kal>

16. Januar 2019

Folie Nr. 8

Skizzieren Sie abschließend ganz grob den strukturellen Aufbau eines vollständigen IPv4-Paktes, welches SSH-Anwendungsdaten in einem Netz transportiert. Stellen Sie auch dar, woran der Empfänger des IPv4-Paketes in der Struktur erkennen kann, welche Anteile (z.B. welches Transportprotokoll) hier jeweils nacheinander folgen?

Ähnliche Frage aus der WS15 Klausur: Skizzieren Sie grob den Aufbau eines Paketes welches SMTP-Daten transportiert... eigentlich müssten die übertragenden Daten irrelevant sein.

Struktureller Aufbau eines IPv4-Datenpaketes

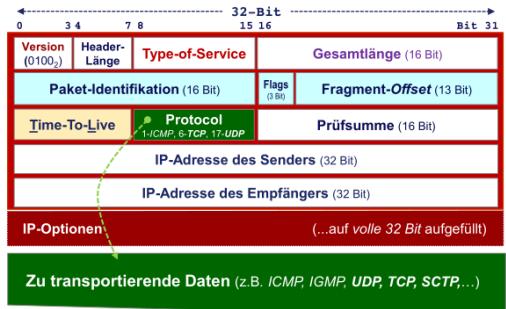


- **Zusätzliche Protokollinformationen¹⁾** im **IP-Header** ergeben sich **direkt** aus gewünschten **Transporteigenschaften** des „Internet-Protokolls“ (**IP**).

- [RFC-791: IP - DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION] (1981) [STD-5]

X Minimale IP-Paketlänge beträgt hier nur 68 Byte

X IP-Headerlänge beträgt typ. 20 Bytes (ohne Optionen)



Wesentliche Eigenschaften:

- IP-Adressen (2*32-Bit)
- Variable Paketlänge
- Fragmentierungsinformation (Zerlegung des Paketes)
- Transport unterschiedlicher Daten möglich (Protokolle)
- Behandlung der Pakete beim Weitertransport einstellbar
- Transportbegrenzung (Zeit- bzw. Hop-Counter)
- Optionale Angaben möglich

¹⁾ Detaillierte Beschreibung, siehe [Anhang](#)

© Fachhochschule Wedel, Dipl.-Ing.(FH) I.Kaleck <http://www.fh-wedel.de/~kal>

Da das SSH-Verfahren eine verschlüsselte Verbindung aufbaut wird hier das TCP im Protokoll-Feld angegeben.

Das Übertragungsprinzip einer SSH-Verbindung

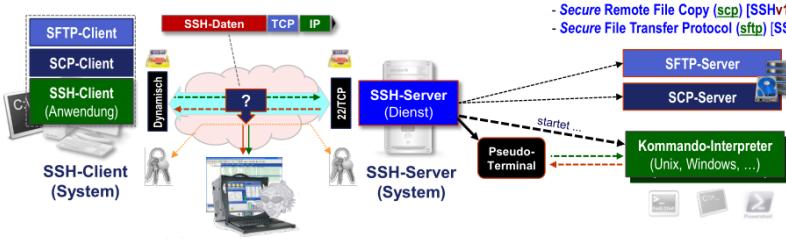


- Die **SSH-Architektur** nutzt zwischen **SSH-Client** und **SSH-Server** nur einen **einzigen, abgesicherten TCP-Übertragungskanal**
 - Einsatz eines **symmetrischen Verschlüsselungsverfahrens**
 - Sichert Datentransport durch gemeinsamen **Session-Key** (des Clients)
 - Einsatz eines **asymmetrischen Verschlüsselungsverfahrens**
 - Dient dem *initialen Schlüsseltausch (Key Exchange)* des Session-Keys
- ✗ **SSH** bietet neben einem **Netzwerk-Terminal** auch weitere Funktionen an.



SSH-Implementierungen bieten oftmals auch:

- Secure Remote File Copy (**scp**) [**SSHv1**]
- Secure File Transfer Protocol (**sftp**) [**SSHv2**]



© Fachhochschule Wedel, Dipl.-Ing.(FH) I. Kaleck <http://www.fh-wedel.de/~kal>

17. Dezember 2018

Folie Nr. 35

Warum kreist ein IPv4-Paket nicht endlos im Netz herum, falls die Zieladresse (-netz) nie gefunden werden kann (weil z.B. gar nicht vergeben)?

Im Paket selbst gibt es ein Feld um festzulegen wie viele Interfaces das Paket eigentlich bei seiner Reise durchs Netz passieren darf. Jedes Interface (Router) dekrementiert dieses und verwirft es falls der Wert 0 erreichen sollte.

Warum kreist ein IP-Paket nicht *endlos* im Netz ?

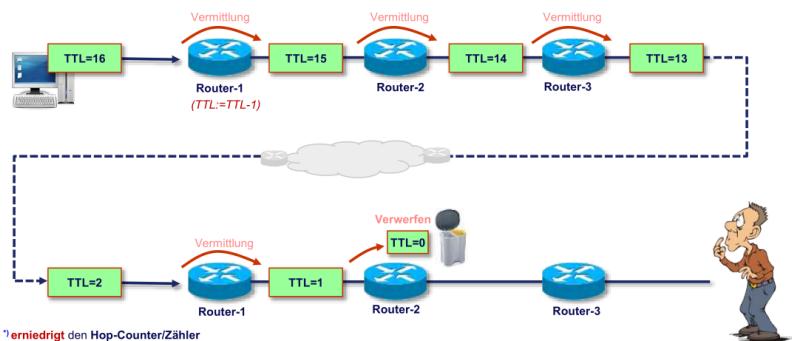


- Jeder Router dekrementiert⁷⁾ das Time-To-Live Feld stets um den Wert „1“.

■ Erreicht das Feld vor dem Ziel den Wert **0**, wird das **Paket verworfen** !

■ Aktueller [RFC 791] legt das **TTL-Feld** als einen „**Hop-Counter**“ fest.

✗ Erster [RFC 760]: „IP“ spezifizierte TTL zunächst in Einheiten von Sekunden...



© Fachhochschule Wedel, Dipl.-Ing.(FH) I.Kaleck Ⓛ http://www.fh-wedel.de/~kal

19. November 2018

Folie Nr. 57

Wiederholung: Aufbau eines IPv4-Datenpaketes

Struktureller Aufbau eines IPv4-Datenpaketes

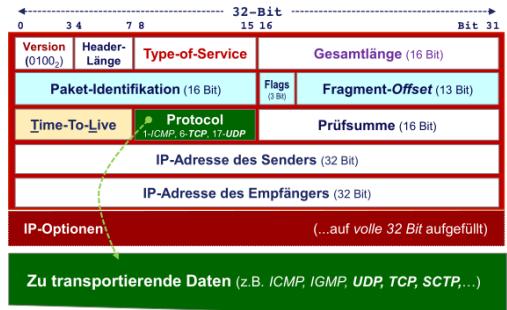


- **Zusätzliche Protokollinformationen⁷⁾** im **IP-Header** ergeben sich **direkt** aus gewünschten **Transporteigenschaften** des „Internet-Protokolls“ (**IP**).

■ [RFC-791: IP - DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION] (1981) [STD-5]

✗ Minimale IP-Paketlänge beträgt hier nur 68 Byte

✗ IP-Headerlänge beträgt typ. 20 Bytes (ohne Optionen)



- IP-Adressen (2*32-Bit)
- Variable Paketlänge
- Fragmentierungsinformation (Zerlegung des Paketes)
- Transport unterschiedlicher Daten möglich (Protokolle)
- Behandlung der Pakete beim Weitertransport einstellbar
- Transportbegrenzung (Zeit- bzw. Hop-Counter)
- Optionale Angaben möglich

⁷⁾Detaillierte Beschreibung, siehe Anhang

© Fachhochschule Wedel, Dipl.-Ing.(FH) I.Kaleck Ⓛ http://www.fh-wedel.de/~kal

19. November 2018

Folie Nr. 55

Aufg3

Erläutern Sie allgemein den Begriff Domain Name System (DNS) in der Internet-Architektur. Was ist das bzw. wozu dient es genau?

Das Domain Name System (DNS)



- Das **Domain**) **Name System (DNS)** des **Internet** ist ein **hierarchisch organisiertes Auskunftssystem** auf **Basis einer verteilten Datenbank**

X Wesentliche Zielsetzung des DNS:

- (1) Nutzung von Hostnamen an Stelle **numerischer IP-Adressen** (z.B. in Anwendungen)
- (2) Speicherung von **Zusatzinformationen** für **Netzbetreiber** (z.B. Mailserver-Adressen)



- Anfangs erfolgte Speicherung der **Zuordnungen** (~Datensätzen) von IP-Adressen zu Hostnamen (→ nur in einer **lokalen Textdatei** („hosts“))

- **Zentrale Pflege** und täglicher **Austausch** per Kopiervorgang ...
- Zugriff auf Tabelle über **Socket-Funktionen** zur Namensauflösung
- **Später** durch eine **verteilte** Datenbank ersetzt ([\[RFC 882\]](#) aus 1983)

↳ inkl. einem **DNS-Abfrage** und **Antwortdienst** (an/von [DNS-Server](#))



↑ von lateinisch *dominium* bzw. französisch *domaine* „Herrschaft“, Herrschaftsbereich“, ...

© Fachhochschule Wedel, Dipl.-Ing.(FH) I.Kaleck Ⓛ <http://www.fh-wedel.de/~kal>

17. Dezember 2018

Folie Nr. 5



Was genau verstehen Sie unter einer so genannten Domäne (engl. Domain) und wie wird diese im globalen DNS gekennzeichnet?

Eine Domäne ist ein eigenständiger Verwaltungsbereich mit einem eindeutigen Domänennamen und einem eigenen DNS-Server zur Verwaltung.

Hierarchische Speicherung von Informationen im DNS



- **Verwaltung der Datensätze** erfolgt heute **dezentral** in einzelnen **Domänen**.

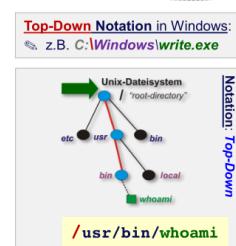
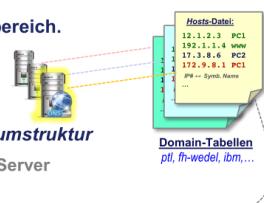
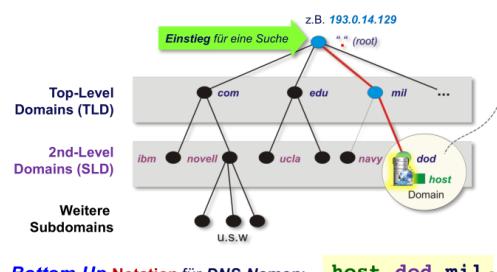
- **Domäne** (engl. *domain*) ist **eigenständiger** Verwaltungsbereich.

✗ Eindeutiger Domänenname (z.B. fh-wedel, google, ...)

✗ Domain Name System (DNS-) Server zur Verwaltung

- **Globales DNS** (im Internet) verknüpft **Domains** in **Baumstruktur**

↳ Einstiegspunkt bilden IP-Adressen namenloser **Root-Server**



© Fachhochschule Wedel, Dipl.-Ing.(FH) I.Kaleck Ⓛ <http://www.fh-wedel.de/~kal>

17. Dezember 2018

Folie Nr. 7



Was ist bzw. wozu dient im Rahmen des DNS ein sog. Resource Record (RR)? Nennen Sie dazu wenigstens zwei konkrete Beispiele (inkl. der jeweiligen Bedeutung).

Als Resource Records (RR) werden Informationseinträge im Domain Name System (DNS) und in einer Zonendatei für die Verwaltung einer Domain bezeichnet. Resource Records haben eine feste Struktur: Domain (NAME) - Klasse (CLASS) - Typ (TYPE) - Eintrag (RDATA).

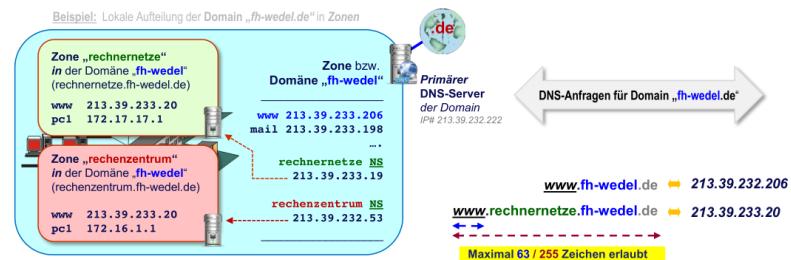
Aufteilung einer Domäne (domain) in Zonen (zone)

- ❑ Für eine Domänendatenbank ist oftmals nur ein einzelner DNS-Server zur Speicherung der zugehörigen Datensätze (Records) zuständig.



✗ Die Aufteilung des eigenen Namensraumes (Domäne) in einzelne Zonen ist lokal möglich (erzeugt Subdomains)

- Für jede dieser Zonen kann ein eigener DNS-Server delegiert sein.
 - Zone: Eigenständiger Verwaltungsbereich in einer Domain
 - Domäne: Zusammengefasster Bereich aller (untergeordneten) Zonen



© Fachhochschule Wedel, Dipl.-Ing.(FH) I Kalleck → http://www.fh-wedel.de/~kal

17. Dezember 2018

Folie Nr. 13

Der DNS-Server als „Datenbankserver“

- ❑ Ein DNS-Server kann eine Vielzahl an (weiteren) Informationen mittels dazu festgelegter Datensätze (Resource Record Types) speichern.

✗ Normale DNS-Abfrage („Query“)¹⁾ erfolgt immer mittels UDP (Port 53)

↳ Ergänzt um jeweiligen Abfragetyp (Querytype = A, CNAME, PTR, MX,...)

Resource Record (RR) Typen (Auswahl)

SOA-Record (Start of Authority)
legt die primäre Autorität für eine Domäne/Zone fest
NS-Record (NameServer)
legt (weitere) Nameserver für eine Domäne fest
A-Record (Address Record)
Zuordnung einer IP-Adresse zu einem Host-/Domainnamen
CNAME-Record (Canonical Name)
legt für den ursprünglichen FQDN in Domäne einen Alias fest
PTR-Record (Pointer Record)
zeigt auf einen FQDN, der zu der IP-Adresse gehört
MX-Record (Mail-Exchanger Record)
speichert den FQDN eines Mailservers für diese Domain

☞ Weitere RR-Typen in ergänzenden RFCs ...

© Fachhochschule Wedel, Dipl.-Ing.(FH) I Kalleck → http://www.fh-wedel.de/~kal

17. Dezember 2018

Folie Nr. 18

Was stellt in diesem Zusammenhang eigentlich eine DNS-Zone dar? Wo liegt hier ein Unterschied zu einer DNS-Domäne?

Ein DNS-Server ist zum Auflösen eines Namensraums zuständig. Wenn er nun auf einem höheren Level des DNS-Namensbaumes rangiert wird er in der Regel die Anfragen an diverse Subdomains weiterleiten. Dazu wird er die entsprechenden DNS-Server kontaktieren. Wenn die Anfrage bei einem Server ankommt welche in der Lage ist den Namen in eine IP-Adresse zu übersetzen wird er auf seine Zonendatei zugreifen. Eine Zone beschreibt also den eigenständigen Verwaltungsbereich seiner Domäne.

Aufteilung einer Domäne (domain) in Zonen (zone)



- Für eine **Domänendatenbank** ist oftmals nur ein **einzelner DNS-Server** zur **Speicherung der zugehörigen Datensätze (Records)** zuständig.

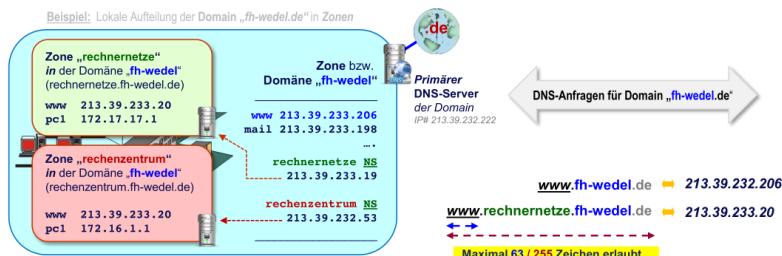


- Die **Aufteilung des eigenen Namensraumes** (Domäne) in einzelne **Zonen** ist *lokal* möglich (erzeugt **Subdomains**)

- Für jede dieser **Zonen** kann ein eigener **DNS-Server** delegiert sein.

- **Zone:** Eigenständiger Verwaltungsbereich *in* einer Domain
 - **Domäne:** Zusammengefasster Bereich aller (untergeordneten) **Zonen**

Beispiel: Lokale Aufteilung der Domain „fh-wedel.de“ in Zonen



© Fachhochschule Wedel, Dipl.-Ing.(FH) I Kaleck → http://www.fh-wedel.de/~kal

17. Dezember 2018

Folie Nr. 13 ◀ ▶

Was genau versteht man unter einem Full Qualified Domain Name (FQDN)?

Ein Fully Qualified Domain Name (FQDN) ist ein vollständiger Domainname mit Dienstangabe, der für jeden Domain-Level einen Eintrag hat, von der Third Level Domain oder Subdomain, über die Second Level Domain bis zur Top Level Domain (TLD).

Welche konkrete Aufgabe hat im DNS also ein DNS-Server (Dienst)?

Ein DNS-Server besitzt die Aufgabe einen FQDN in ein IP-Adresse (Forward Lookup) oder eine Adresse in einen FQDN (Reverse Lookup) aufzulösen.

Speicherung von Informationen im *globalen* DNS



- Zur Verwaltung *globaler Domänen* sind mindestens **zwei DNS-Server nötig**.

✗ Primärer und. sekundäre(r) DNS-Server (→ *Primary*, → *Secondary*)

■ Gefordert ist Eindeutigkeit der *Hostnamen* in jeder Domäne¹⁾

- www, mail, ftp, stud, kal, pc01, www2, wwwab, ftplib, r1-pc01, r2-pc01, ...

■ Globale Eindeutigkeit durch „Fully Qualified Domain Name“ (**FQDN**)

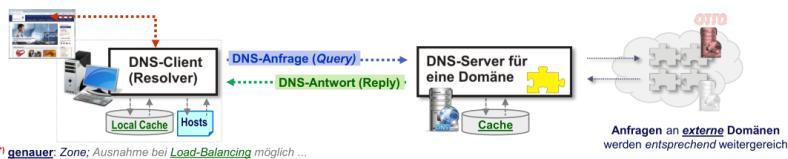
☞ Notation als *hostname • domäne* (z.B. www • fh-wedel • de, ...)

■ Abfragen an einen *DNS-Server* immer nur als **FQDN**

① Auflösung eines **FQDN** in zugehörige IP-Adresse (Forward Lookup)

② Auflösung einer IP-Adresse in den zugehörigen **FQDN** (Reverse Lookup)

☞ Ablauf und Datenstrukturen u.a. in [RFC-1034] und [RFC-1035]



© Fachhochschule Wedel, Dipl.-Ing.(FH) I.Kaleck ☎ http://www.fh-wedel.de/~kal

17. Dezember 2018

Folie Nr. 12

Wozu dient auf einem System, welches per IP kommuniziert (z.B. ein Windows-PC), auch heute noch die klassische Hosts-Datei und wann kommt diese jeweils zum Einsatz? Wozu könnte sie missbraucht werden bzw. wo liegt hier ggf. eine Gefahr?

Diese Datei kann eine Übersetzungstabelle verwalten, ähnlich wie es ein DNS-Server tut. Es wird beim auflösen eines Namens stets erst diese Datei durchsucht bevor die Suche per DNS-Server startet. Falls hier jedoch eine falsche Zuordnung zu finden sein sollte, ist es für den User nicht mehr möglich diese Seite auf seinem System anzusteuern (DNS-Spoofing).

Die Nutzung der klassischen „hosts-Datei“ ...



- Die klassische **hosts**-Datei ist auf **IP-basierten Systemen** meist noch vorhanden und wird bei Auflösungen stets **zuerst** ausgewertet.

■ Bei DNS-Auflösungen wird zuerst diese Datei genutzt (siehe [[RFC 883](#)])

☞ Speicherung im **/etc-Konfigurationsverzeichnis**



/etc/hosts



/windows/system32/drivers/etc/hosts

DNS-Namen verweisen nun auf andere IP-Adressen:

```
C:\>ping -a 192.168.10.1
Ping homeoffice-router [192.168.10.1] mit 32 Bytes Daten:
...
C:\>ping www.haspa.de
Ping www.haspa.de [110.10.1.1] mit 32 Bytes Daten:
Antwort von 110.10.1.1: Bytes=32 Zeit=539ms TTL=109
```

```
# Dieses ist eine HOSTS-Beispieldatei
#
# Diese Datei enthält lokale Zuordnungen von IP-Adressen zu Hostnamen.
#
127.0.0.1      localhost
213.39.233.39  kal kaleck stats.sonicfoundry.com www.adobe.com
110.10.1.1      www.haspa.de
213.39.233.20  wwwab xyz.def
#
192.168.10.1    homeoffice-router router.myhome
192.168.10.2    homeoffice-drucker drucker.myhome
192.168.10.254  homeoffice-pcl   pcl.myhome
```

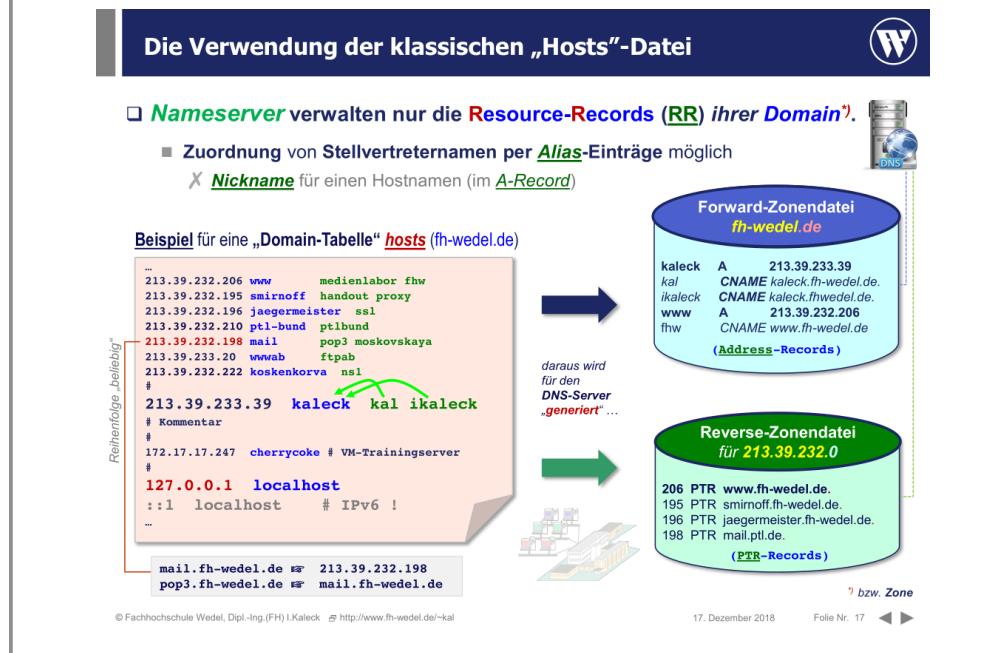
Nur lokal gültige Domäne „myhome“

STOP
Damit nicht mehr im „Internet“ erreichbar!

Umleitung an eine falsche Internet-Adresse (DNS-Spoofing)

Beim Abruf einer Webseite per http (z.B. von www.lidl.de) wird von der Anwendung (Browser) die zugehörige IP-Zieladresse benötigt, auf der dieser http-Dienst läuft. Wo genau und wie (in welcher Form) wird diese Information im DNS gespeichert?

Ein DNS-Server besitzt eine sog. Forward-Zonendatei. In dieser sind alle Ressource Records zum Auflösen eines FQDN zu einer IP-Adresse gespeichert. Außerdem ist ein DNS-Server in der Lage verschiedene RR-Typen zu speichern. Die Toplevel Domains werden stets auf einen NS-Record zugreifen um den Namen aufzulösen, dieser Record-Typ legt weitere Namensserver für die Domäne fest, sie leiten die Anfrage also einfach an eine Subdomain weiter. Beim DNS-Server welcher für die Domain *lidl* zuständig ist wird auf einen A-Record zugegriffen bei welchem die Information (IP-Adresse) enthalten ist und so direkt übersetzt werden kann.



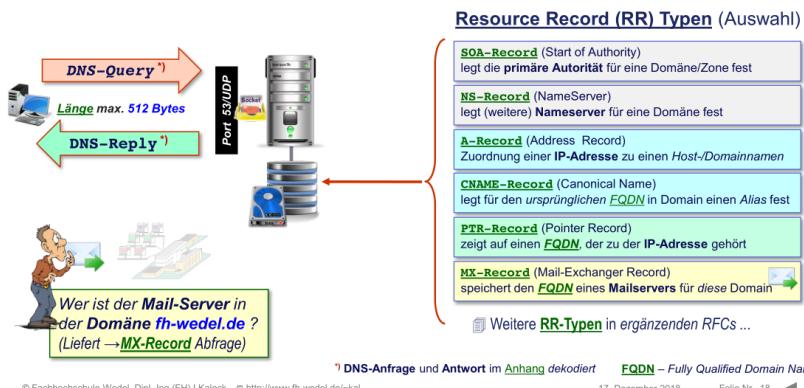
Der DNS-Server als „Datenbankserver“



- Ein DNS-Server kann eine Vielzahl an (weiteren) Informationen mittels dazu festgelegter Datensätze (Resource Record Types) speichern.

X Normale DNS-Abfrage („Query“)^{*)} erfolgt immer mittels **UDP** (Port 53)

↳ Ergänzt um jeweiligen Abfragetyp (Querytype = A, CNAME, PTR, MX,...)

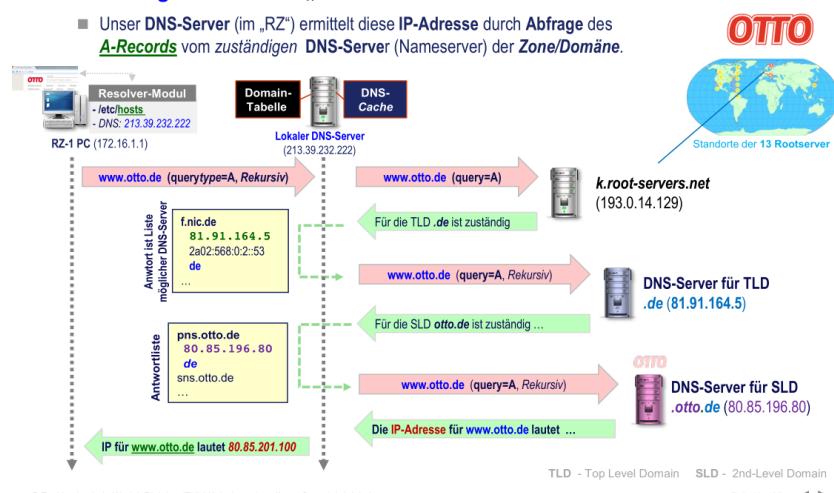


Eine Namensauflösung im globalen DNS (→Forward-Lookup)



- Auflösung des Namens „www.otto.de“ durch einen lokalen DNS-Server

■ Unser DNS-Server (im „RZ“) ermittelt diese IP-Adresse durch Abfrage des A-Records vom zuständigen DNS-Server (Nameserver) der Zone/Domäne.



Beispiel: Struktur einer „Forward-Zonendatei“ (→ BIND-Server)



□ Jeder **DNS-Server**) benötigt **mindestens (s)eine Forward-Zonendatei** ...

✗ Zugehörige Reverse-Lookup Zonendatei ist **optional** und ggf. **nicht erwünscht**.



Verwaltungs-Informationen					
Name-Server	Sub-domain	TTL	CLASS	TYPE	
				RDATA	
				; setting default domain to "fh-wedel.de"	
Mail-Server Records	@	86400	IN	SOA	koskenkorva.fh-wedel.de. root.koskenkorva.fh-wedel.de. (2009111610 ; Serial 28800 ; Refresh 3600 ; Retry 1209600 ; Expire 86400) ; Minimum TTL
	fantasy	86400	IN	NS	koskenkorva wwwab.fh-wedel.de.
	rechnernetze	86400	IN	NS	A 213.39.232.206 → nas.fh-wedel.de.
	fh-wedel.de.		IN	MX 10	exchange.fh-wedel.de.
	fh-wedel.de.		IN	MX 20	mail mx2
	localhost			A	127.0.0.1
	loopback			CNAME	localhost
	...				
	www			A	213.39.232.206 ; vServer Typo-3
	medienlabor			CNAME	www.fh-wedel.de.
fhw			CNAME	www.fh-wedel.de.	
kaleck			A	213.39.233.39	
ikaleck			CNAME	kaleck.fh-wedel.de.	
mail			A	213.39.232.198	
...					

Implizite Zuordnung einer IP-Adresse zur Domäne (Zone)




↑ z.B. der Berkeley Internet Nameservice Daemon (BIND)

© Fachhochschule Wedel, Dipl.-Ing.(FH) I Kaleck → http://www.fh-wedel.de/~kal

17. Dezember 2018 Folie Nr. 20

Was stellt im Zusammenhang der Auflösung von Domainnamen zu IP-Adressen im DNS-Namensraum eigentlich ein sog. ALIAS genau dar und wozu ist so was gut? Wo genau und wie wird diese Angabe im DNS hinterlegt?

Ein ALIAS wird in der Forward-Zonendatei festgelegt. Der RR-Typ *CNAME* wird dafür verwendet. Ein ALIAS macht nichts anderes als einen ursprünglichen FQDN mit einem anderen FQDN zu ersetzen.

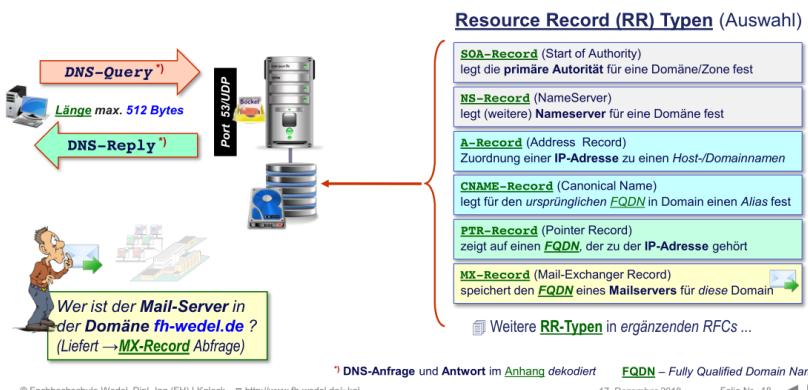
Der DNS-Server als „Datenbankserver“



- Ein DNS-Server kann eine **Vielzahl** an (weiteren) **Informationen** mittels dazu festgelegter **Datensätze (Resource Record Types)** speichern.

- Normale **DNS-Abfrage** („Query“*) erfolgt immer mittels **UDP** (Port 53)

↳ Ergänzt um jeweiligen **Abfragetyp** (Querytype = A, CNAME, PTR, MX,...)



* DNS-Anfrage und Antwort im Anhang dekodiert FQDN – Fully Qualified Domain Name

© Fachhochschule Wedel, Dipl.-Ing (FH) I. Kaleck http://www.fh-wedel.de/~kal

17. Dezember 2018 Folie Nr. 18



Die Verwendung der klassischen „Hosts“-Datei

- **Nameserver** verwalten nur die **Resource-Records (RR)** ihrer **Domain***

- Zuordnung von Stellvertreternamen per **Alias-Einträge** möglich

- Nickname** für einen Hostnamen (im **A-Record**)

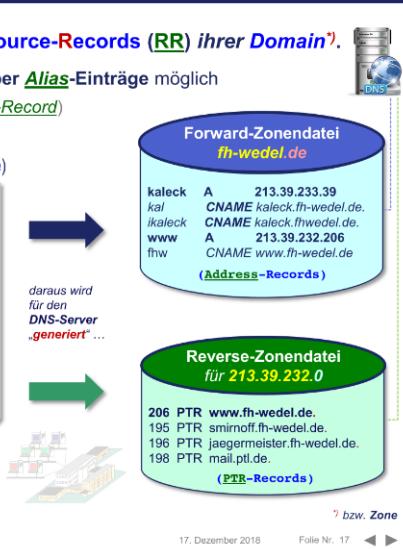
Beispiel für eine „Domain-Tabelle“ **hosts** (fh-wedel.de)

```

...
213.39.232.206 www      medienlabor fhw
213.39.232.195 smirnoff   handout proxy
213.39.232.196 jaegermeister ssl
213.39.232.210 ptl-bund  ptlbund
213.39.232.198 mail      pop3 moskovskaya
213.39.233.20  wwwab     ftplib
213.39.232.222 koskenkorva ns1
#
213.39.233.39 kaleck    kal ikaleck
# Kommentar
#
172.17.17.247 cherrycoke # VM-Trainingsserver
#
127.0.0.1 localhost
::1 localhost      # IPv6 !
-
mail.fh-wedel.de    213.39.232.198
pop3.fh-wedel.de   213.39.232.198

```

Reihenfolge beliebig*



© Fachhochschule Wedel, Dipl.-Ing (FH) I. Kaleck http://www.fh-wedel.de/~kal

17. Dezember 2018

Folie Nr. 17

Skizzieren Sie nun für www.lidl.de den Ablauf der eigenständigen Namensauflösung in die zugehörige IP-Adresse durch einen unserer DNS-Server (hier im Rechenzentrum). Unser DNS-Server hat die öffentliche IP-Adresse 213.39.232.222 und freien Zugang zum Internet. Stellen Sie dar, was hier jeweils genau von wo nach wo übertragen wird (Typ, Inhalt).

(DNS-Server) ----->
(im RZ)



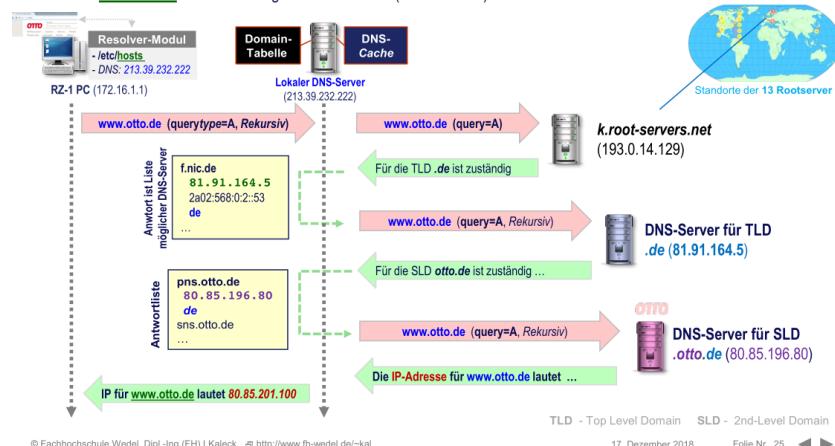
(DNS-Server) <-----

Eine Namensauflösung im globalen DNS (→Forward-Lookup)



□ Auflösung des Namens „www.otto.de“ durch einen lokalen DNS-Server

- Unser DNS-Server (im „RZ“) ermittelt diese IP-Adresse durch Abfrage des A-Records vom zuständigen DNS-Server (Nameserver) der Zone/Domäne.



Erläutern Sie abschließend, was Sie in diesem Zusammenhang unter einer Pointer-Query (PTR-Abfrage) verstehen. Was wird hierbei ermittelt und wie wird es notiert (Beispiel!)?

Unter einer Pointer-Query wird eine Rückwärtsauflösung (also IP - FQDN) verstanden. Hierbei wird die Adresse mit dem Postfix in-addr.arpa versehen und an die entsprechenden DNS-Server geschickt. Es wird als Pointer Query bezeichnet, da die Reverse-Zonendatei mit Zeigern (PTR-Records) gefüllt ist welche auf den jeweiligen FQDN zeigen.

DNS-Organisation zur Rückwärtsauflösung (→Reverse-Lookup)

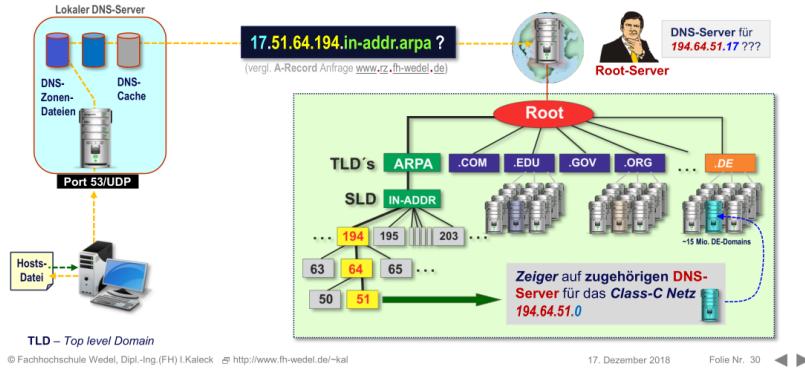
- ❑ Welcher Domänenname gehört **aktuell** zur Klasse-C Adresse **194.64.51.17** ?

■ Ergebnis durch Abfrage des **zugehörigen Datensatzes** in der Reverse Zone

① per Rückwärtsauflösung bzw. „Pointer-Query“ (PTR-Query)

■ Lösung des Suchproblems durch die TLD **.arpa** (TLD—Address and Routing Parameter Area)

② **Bottom-Up Notation** daher **17.51.64.194.in-addr.arpa** (mit Querytype=PTR)



Aufg4

Erläutern Sie kurz bzw. stichwortartig den Begriff SMTP. Wozu dient es und welche wesentlichen Eigenschaften weist es auf? Welches Transportprotokoll wird dabei benutzt.

Transportprotokoll: Abruf der Nachrichten über POP3 oder IMAPv4. Nachrichten unverschlüsselt per TCP übermittelt. Serverdienst nutzt den well-known-Service Port 25

Das Simple Mail Transport Protocol (SMTP)



- Das **SMTP** dient **nur** zur Nachrichtenübermittlung zwischen **SMTP-Servern**.

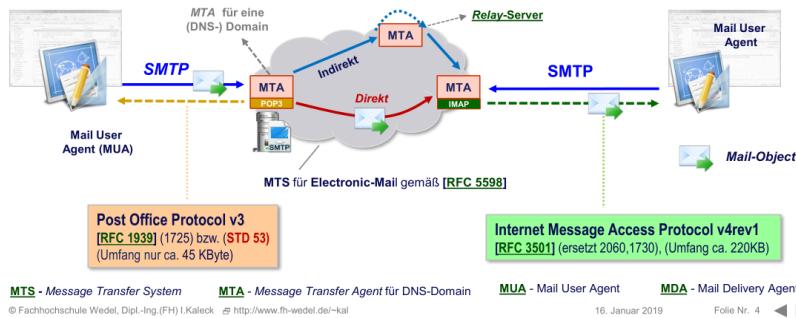
■ Übermittlung gemäß [\[RFC 821\]](#) (1982), aktualisiert im [\[RFC 2821\]](#) bzw. [\[RFC 5321\]](#) (**STD 10**)

■ Ein **SMTP-Server** fungiert dabei als **Message Transfer Agent (MTA)**.

● Nachrichtenweiterleitung per **Store & Forward (s&f) Prinzip**

↳ Indirekte Zustellung über **SMTP-Relay** Server möglich (→[open mail relay](#))

✗ **Abruf** von Nachrichten über **POP3** oder **IMAPv4** (von einem POP3-/IMAP-Server)



Wesentliche Eigenschaften des „SMTP“ im Überblick ...



- Das **SMTP** ist ein **Übertragungsprotokoll** für **Nachrichten (E-Mails)** zwischen einzelnen **SMTP-Servern** (Message Transfer Agents, **MTAs**)

■ Notation der **Zielpostfachadresse** bestimmt auch die **Weiterleitung**

✉ postfach-name@domain (✉ kal@fh-wedel.de)

✉ postfach-name@host.domain (✉ kal@mail.fh-wedel.de)



■ **Einfacher Nachrichtenaufbau** ([\[RFC 5322\]](#) ersetzt [\[RFC 2822\]](#) (**STD 11**))

● **Message-Content** besteht aus **Header** und **Body** (nur 7-bit US ASCII-Zeichen)

● **Kodierungsregeln** erlaubten **heute komplexe Nachrichtenstrukturen** (z.B. [Binärdateien](#))



■ **Nachrichtentransport unverschlüsselt** per **TCP** gemäß [\[RFC 5321\]](#)

● **SMTP-Serverdienst** nutzt den **well-known Port 25/TCP**

◆ Annahme und ggf. Weitertransport **direkt** oder per **SMTP-Relay** zum Ziel
✗ SMTP-Server fügt der Nachricht (Header) seine **Referenz** ein (Message-ID, Zeit).

● **SMTP-Dialog** auf Basis einfacher **Textkommandos** (**HELO**, **DATA**, **QUIT**, ...)

✗ Jedes Kommando ist genau **vier Zeichen** lang ...

⌚ Statusanzeige durch numerischen **Return-Code** (3-stellig, „220 ...“)



Das SMTP konnte erst später in seiner Entwicklung quasi beliebige Informationen übertragen, wie z.B. eine ausführbare (Binär-) Datei. Wie genau wurde das nachträglich gelöst? Kennen Sie dazu ein konkretes Verfahren bzw. eine dabei genutzte Technik?

???; b; todo eventuell im RFC 3030, nochmal nachschauen. extended smtp, ich finde nichts zum verschicken von executables nur über erweiterten Zeichensatz, etc..

Welche Möglichkeiten kennen Sie, um die Nutzung eines SMTP-Servers (Dienstes) in einem Netz gegen einen unbefugten Versand von E-Mails zu beschränken?

SPF: Prüfung von Mail-Adressen durch Hinterlegung gültiger Adressen.

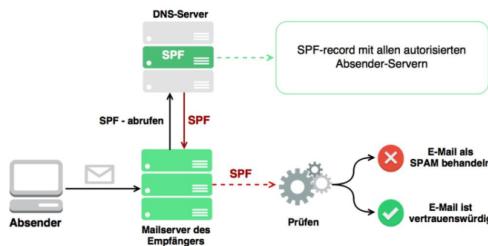
Umstritten: Nutzung des Sender Policy Frameworks (SPF)



□ Das **Sender Policy Framework (SPF)** ist ein **E-Mail Validierungssystem**

- [RFC 7208: Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Vers.1]
- Erlaubt **Prüfung gültiger E-Mail Absender** durch Hinterlegung gültiger IP-Adressen
 - Speicherung gültiger E-Mail Senderadressen (SFP-Infos) einer Domäne in **TXT Records** auf dem DNS-Server der Domain
- **Eintrag u.a. bei GMX seit 2016 verpflichtend ... was Probleme machen kann!**

So funktioniert SPF



Quelle: <http://www.spf-record.de/>

© Fachhochschule Wedel, Dipl.-Ing.(FH) I.Kaleck <http://www.fh-wedel.de/~kal>

16. Januar 2019

Folie Nr. 15



Einsatz verschiedener SMTP-Auth Verfahren möglich ...

□ **ESMTP-Server können zusätzlich AUTH-Verfahren (Kommando) anbieten***

- Darüber können div. **Authentifizierungsverfahren** genutzt werden, wie z.B.
 - **LOGIN** Anmeldung
 - ✗ Benutzername & Passwort werden jeweils nur **Base64-kodiert** (~unverschlüsselt) übertragen
 - **PLAIN** Anmeldung
 - [RFC 4616]: PLAIN Simple Authentication and Security Layer (SASL) Mechanism]
 - ✗ SASL-Authorization-ID, Benutzername & Passwort werden zusammen **Base64-kodiert** übertragen
 - **CRAM-MD5** Anmeldung
 - [RFC-2195]: IMAP/POP AUTHorize Extension for Simple Challenge/Response]
 - **NTLM** (WindowsNT LAN Manager) Anmeldung
 - ✗ Ist ein Challenge-/Response-Authentifizierungsverfahren
 - Siehe z.B. [NT LAN Manager (NTLM) **Authentication Protocol**]
 - **GSSAPI** (Generic Security Services Application Program Interface) Anmeldung
 - ♦ GSS-API/Kerberos Authentication
 - [RFC 2743]: Generic Security Service Application Program Interface 2, Update 1]
- ✗ Basis u.a. im Framework **[RFC-4422]: Simple Authentication and Security Layer (SASL)**
 - bzw. eine Anmeldung erfordern



© Fachhochschule Wedel, Dipl.-Ing.(FH) I.Kaleck <http://www.fh-wedel.de/~kal>

16. Januar 2019

Folie Nr. 17



Wozu dient beim SMTP das Greylisting Verfahren?

Beschränkung von *Massen-Emails*.

Beispiel: Einsatz von Postgrey (Postfix Greylisting Policy Server)



- ❑ Einkommende Mails unbekannter Sender werden **zunächst abgewiesen** ...

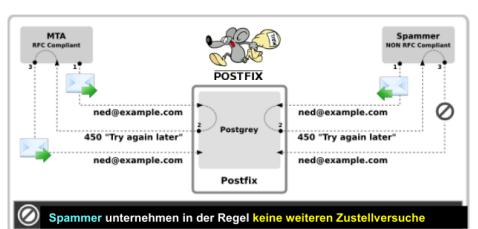
✗ Bereits [\[RFC 821\]](#) erlaubte diese Reaktion (Reply Code) eines SMTP-Servers.

⌚ **450 Requested mail action not taken: mailbox unavailable [E.g., mailbox busy]**

- **Eigenschaften des Postfix Greylisting Policy Servers ("postgrey")**

- Auto-whitelisting vertrauenswürdiger Clients (nach Quarantänezeit)
- Sperrung per *Blacklist*-Datei bzw. Einbindung offizieller SPAM-Listen Anbieter*
- Freischaltung spezifischer Sender oder Mail-Provider statisch in Whitelist-Datei

↳ [192.168.1.10. *googlemail.com, *.gmx.de, postmaster@, abuse@, ...](#)



<http://www.postfix.org/>

* z.B. [SPAMHAUS.ORG](#)

© Fachhochschule Wedel, Dipl.-Ing (FH) I. Kaleck <http://www.fh-wedel.de/~kal>

<http://wiki.centos.org/HowTos/postgrey>

16. Januar 2019

Folie Nr. 20



Beschränkung von „Massen-Emails“ per Greylisting-Verfahren



- ❑ „**Spammer** versenden täglich tausende von Mails in der Hoffnung, dass einige hundert davon zugestellt werden und ein paar Dutzend davon gelesen werden ...“



- Der Verlust einzelner Mails ist dabei *irrelevant* (Fire and Forget-Prinzip)

✗ **Spammer** unternehmen auch bei **temporären Fehlercodes** des SMTP-Servers oftmals keine erneute Zustellung einer Nachricht ...

- **Eine gute SPAM-Begrenzung schafft daher das Greylisting-Verfahren**

↳ **Nachrichten unbekannter SMTP-Server nicht** sofort annehmen !



I. Dazu Festlegung einer Quarantänezeit (z.B. 300 Sekunden)

II. Erst nach Ablauf der Zeit und erneutem Übertragungsversuch wird Absender auf interne Whitelist gesetzt und nachfolgende E-Mails werden angenommen.

✗ Problematisch sind nun eine verzögerte Mailzustellung und ggf. ausbleibende Mails

```
-> MAIL FROM: <sender@somedomain.com>
<- 250 2.1.0 Sender ok
-> RCPT TO: <recipient@otherdomain.com>
<- 451 4.7.1 Please try again later
```

SMTPL erlaubt permanente und temporäre Fehlersituationen:

- **4xx-Codes zeigen temporäre Fehler** an, der Server sollte es später noch einmal versuchen.
- **5xx-Codes sind permanente Fehler** (z.B. user unknown), der Server sollte seine Übertragung abbrechen.



© Fachhochschule Wedel, Dipl.-Ing (FH) I. Kaleck <http://www.fh-wedel.de/~kal>

16. Januar 2019

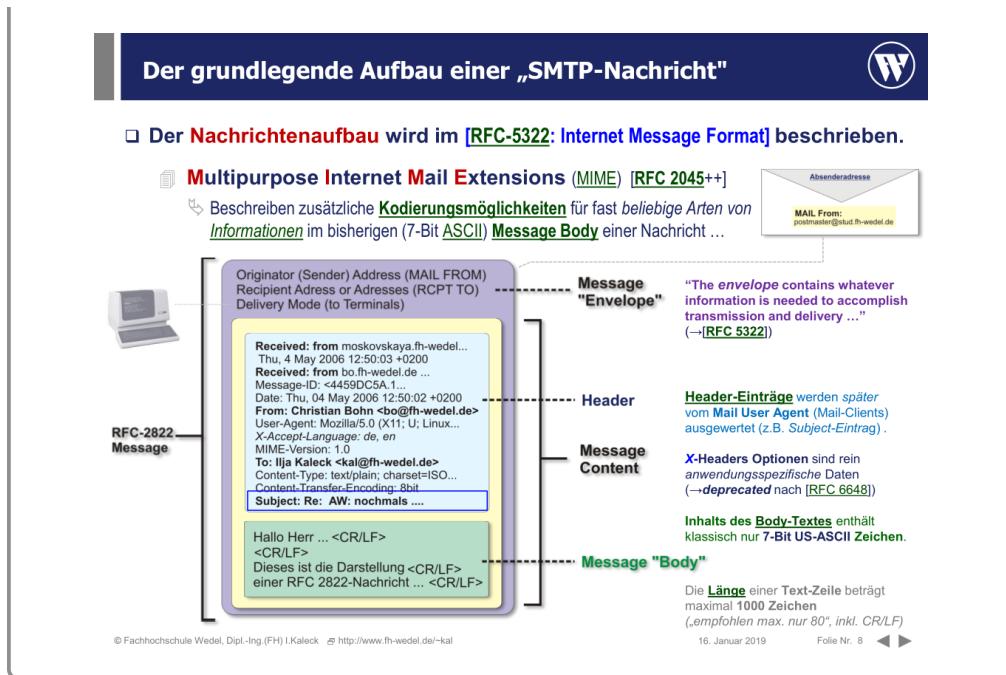
Folie Nr. 19



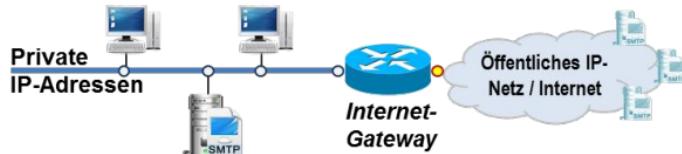
Bei der Übertragung von Nachrichten zu einem Ziel (z.B. service@lidl.de) muss ein SMTP-Server zunächst herausfinden, wohin er die Daten übermitteln soll. Wo und wie wird die dazu notwendige Information ganz konkret gespeichert?

Wesentliche Eigenschaften des „SMTP“ im Überblick ...

- ❑ Das SMTP ist ein Übertragungsprotokoll für Nachrichten (E-Mails) zwischen einzelnen SMTP-Servern (Message Transfer Agents, MTAs)
 - Notation der Zielpostfachadresse bestimmt auch die Weiterleitung
 - ✉ postfach-name@domain (✉ kal@fh-wedel.de)
 - ✉ postfach-name@host.domain (✉ kal@mail.fh-wedel.de)
 - Einfacher Nachrichtenaufbau ([RFC 5322] ersetzt [RFC 2822] (STD 11))
 - Message-Content besteht aus Header und Body (nur 7-bit US ASCII-Zeichen)
 - Kodierungsregeln erlaubten heute komplexe Nachrichtenstrukturen (z.B. Binärdateien)
 - Nachrichtentransport unverschlüsselt per TCP gemäß [RFC 5321]
 - SMTP-Serverdienst nutzt den well-known Port 25/TCP
 - ◊ Annahme und ggf. Weitertransport direkt oder per SMTP-Relay zum Ziel
 - ✗ SMTP-Server fügt der Nachricht (Header) seine Referenz ein (Message-ID, Zeit).
 - SMTP-Dialog auf Basis einfacher Textkommandos (HELO, DATA, QUIT, ...)
 - ✗ Jedes Kommando ist genau vier Zeichen lang ...
 - ⌚ Statusanzeige durch numerischen Return-Code (3-stellig, „220 ...“)



- e) Ein **SMTP-Server** soll *intern* in einem **Unternehmensnetz** installiert und auch **betrieben** werden, welches hier aber nur *private IPv4-Adressen* verwendet.



Was versteht man in diesem Zusammenhang überhaupt unter sog. **privaten IPv4-Adressen**, die aktuell im [RFC-1918] beschrieben werden?

Die Einführung von *privaten IPv4-Adressen* ...



- Im [RFC-1918: Address Allocation for Private Internets] wird ein **kleiner Bereich** von **IPv4-Adressen** zur Verwendung nur im **privaten Bereich** festgelegt.

X Dieser [RFC] hat nur BCP-Status, wird aber allgemein befolgt ...

- Festgelegte private IPv4-Adressenbereiche sind:

Klasse	Von	Bis	Anzahl
A	10.0.0.0	10.255.255.255	1 Netz
B	172.16.0.0	172.31.255.255	16 Netze
C	192.168.0.0	192.168.255.255	256 Netze



X **Pakete mit privaten IP-Adressen** werden im Internet nicht weitergeleitet (geroutet), da dort keine **Eindeutigkeit** mehr gegeben ist.

- Nutzung nur im geschlossenen Standort-Netz, daher keine Weiterleitung
- Zusätzlich **Filterung** solcher Pakete beim Internet Service Provider (ISP).
- ↳ **Ansonsten** ist Adressumsetzung¹⁾ auf dem Internet-Router erforderlich...



BCP – Best Current Practice

¹⁾ z.B. per Network Address Translation (NAT)

© Fachhochschule Wedel, Dipl.-Ing.(FH) I.Kaleck Ⓛ <http://www.fh-wedel.de/~kal>

19. November 2018

Folie Nr. 49



- e) Ein SMTP-Server soll *intern* in einem **Unternehmensnetz** installiert und auch **betrieben** werden, welches hier aber nur *private IPv4-Adressen* verwendet.



Welche bekannten Einschränkungen gibt es bei der Nutzung privater IPv4-Adressen im Rahmen der Kommunikation zwischen Anwendungen in/über Netz, wie z.B. dem Internet?

Pakete mit privaten IP-Adressen werden im Internet nicht weitergeleitet (geroutet), da dort keine Eindeutigkeit mehr gegeben ist. **Richtig verstanden?:** Werden nicht direkt im Router herausgefiltert, sondern erst beim ISP.

Die Einführung von *privaten IPv4-Adressen* ...



- Im [RFC-1918: Address Allocation for Private Internets] wird ein **kleiner Bereich** von **IPv4-Adressen** zur Verwendung nur im **privaten Bereich** **festgelegt**.

Dieser [RFC] hat nur **BCP**-Status, wird aber allgemein befolgt ...

- **Festgelegte private IPv4-Adressenbereiche sind:**

Klasse	Von	Bis	Anzahl
A	10.0.0.0	10.255.255.255	1 Netz
B	172.16.0.0	172.31.255.255	16 Netze
C	192.168.0.0	192.168.255.255	256 Netze



- Pakete** mit **privaten IP-Adressen** werden im **Internet** **nicht** weitergeleitet (*geroutet*), da dort keine **Eindeutigkeit** mehr gegeben ist.

- Nutzung nur im geschlossenen Standort-Netz, daher keine Weiterleitung
- Zusätzlich **Filterung** solcher Pakete beim Internet Service Provider (ISP).

Ansonsten ist Adressumsetzung¹⁾ auf dem Internet-Router erforderlich...



BCP – Best Current Practice

¹⁾ z.B. per Network Address Translation (NAT)

- e) Ein SMTP-Server soll *intern* in einem **Unternehmensnetz** installiert und auch **betrieben** werden, welches hier aber nur *private IPv4-Adressen* verwendet.



Erläutern Sie, wie E-Mails über diesen SMTP-Server (Dienst) auch an Ziele im öffentlichen Internet gesendet werden können und welche Technik dazu hier nötig ist. Welcher konkrete Ablauf in der IP-Kommunikation ergibt sich hierbei?

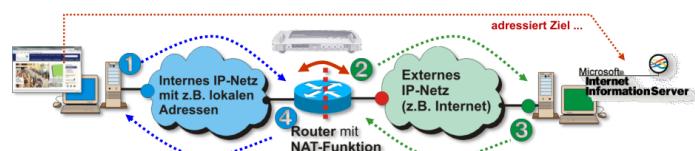
Router des Netzwerks ist in der Lage per NAT-Technik die privaten mit den eigenen öffentlichen weiterzuleiten.

NAT als Funktion auf dem zentralen „Internet-Router“



- Der Einsatz von **Network Address Translation (NAT)** erfordert, dass **alle** ein- und ausgehenden **IPv4-Pakete** über den **gleichen Router** laufen.

X NAT-Aktivierung daher meist auf zentralem Internet-**Gateway** (**Router, Firewall**).



Ablauf:

- ① ② Umschreiben** der IP-Adresse des Senders bei ausgehenden Paketen

↳ Speicherung in einer Zuordnungstabelle

- ③ Rückübersetzung** der Zieladresse eingehender Pakete anhand Tabelle

↳ Eindeutigkeit (z.B. per 1:1-Umsetzung) ist dazu erforderlich!

- ④ Weiterleitung** des Paketes an **ursprüngliche Empfängeradresse**

X Umsetzung arbeitet für **Absende- und Empfängerprozess transparent**.

X Mögliche Probleme, siehe [[RFC-2993](#): Architectural Implications of NAT]

- e) Ein **SMTP-Server** soll *intern* in einem **Unternehmensnetz** installiert und auch **betrieben** werden, welches hier aber nur *private IPv4-Adressen* verwendet.



Der in e) skizzierte interne SMTP-Server soll auch selbst (direkt) aus dem öffentlichen Netz einkommende E-Mails empfangen können. Was ist dazu wiederum wo nötig und wie gestaltet sich hierbei dann die Übertragung bzw. der Kommunikationsablauf? Erläutern Sie ganz kurz.

Nicht sicher, aber wahrscheinlich möchte er hier hören, dass der Server nicht direkt aus dem öffentlichen Netz addressiert werden kann. Hierbei müsste man sich einem Proxy- oder NAT-Dienst bedienen.

Aufg5

Wozu genau dient in einer Routingtabelle speziell ein Default-Router (bzw. -Gateway) Eintrag?

Ein Default-Router bestimmt den Router an welchen ein gegebenes Datenpaket weitergeleitet wird falls eine direkte Übermittlung des Pakets zum Zielinterface nicht möglich ist. (Default-Router - Eintrag als Platzhalter *Wildcard* für unbekannte Zielnetze)

Die Wegwahl- bzw. Routing-Tabelle eines IPv4-Routers

Eine **Routing-Tabelle** ist allgemein eine „Aufstellung der dem Router bekannten Zielnetze und wie sie erreicht werden können ...“.

- Ist Entscheidungsbasis für **lokales Forwarding** von Paketen zum Ziel(netz)

Zielnetz & Subnetzmase	Nächstes Interface	Woher stammt Eintrag	Metrk-Wert
213.39.233.16/28	213.39.233.46	statisch	2 Hops
0.0.0.0/0	213.39.232.11	statisch	1 Hop

Angabe zwingend nötig *Angabe optional*

- Tabelleneinträge können **statisch** und/oder **dynamisch** hinzugefügt werden.
 - ↳ Dynamische Einträge z.B. durch **Austausch** von Wegwahlinformationen mit benachbarten Routern (per **Routing-Protokoll**, wie z.B. dem **RIP**)
- Die **Weiterleitung** durch den Router erfolgt als
 - **Direktes Routing** zum Empfänger (Interface in einem der angeschlossenen Teilnetze)
 - **Indirektes Routing** über einen **weiteren Router** zum Ziel (-netz)
 - ↳ **Default-Router**-Eintrag als Platzhalter (**Wildcard**) für unbekannte Zielnetze
 - ✗ Schleifenbildung unbedingt vermeiden (A → B → A ...) !
- **Zusammenfassen und Verdichten der Tabelleneinträge möglich** (→**Route Aggregation**)
 - ↳ Möglich u.a. per CIDR [[RFC 4632](#)] und einer Variable Length Subnet Mask (VLSM) [[RFC 1812](#)]

© Fachhochschule Wedel, Dipl.-Ing.(FH) I.Kaleck <http://www.fh-wedel.de/~kal> <http://www.vlsm-calc.net/> Seite Nr. 7

13. Juli 2015

Die Wegwahl- bzw. Routing-Tabelle eines IPv4-Routers

Eine **Routing-Tabelle** ist allgemein eine „Aufstellung der dem Router bekannten Zielnetze und wie sie erreicht werden können ...“.

- Ist Entscheidungsbasis für **lokales Forwarding** von Paketen zum Ziel(netz)

Zielnetz & Subnetzmase	Nächstes Interface	Woher stammt Eintrag	Metrk-Wert
213.39.233.16/28	213.39.233.46	statisch	2 Hops
0.0.0.0/0	213.39.233.45	statisch	1 Hop

Angabe zwingend nötig *Angabe optional*

- Tabelleneinträge können **statisch** und/oder **dynamisch** hinzufügt sein.
 - ◆ Dynamische Einträge von Wegwahlinformationen (z.B. durch **Austausch** mit benachbarten Routern (per **Routing-Protokoll**, wie z.B. dem **RIP**)
- **Zusammenfassen von Tabelleneinträge möglich** (→**Route Aggregation**)
 - ◆ Gemäß [[RFC 4632](#) CIDR] und [[RFC 1812](#) Variable Length Subnet Mask (**VLSM**)]
- Die **Weiterleitung** durch den Router erfolgt als/per ...
 - **Direktes Routing** zum Empfängerinterface (in angeschlossenem Teilnetz)
 - **Indirektes Routing** über einen **weiteren Router** zum Ziel (-netz)
 - ↳ **Default-Router**-Eintrag als **Platzhalter** (**Wildcard**) für unbekannte Zielnetze
 - ↳ Schleifenbildung unbedingt vermeiden (Router-A → B → A ... usw.) !

© <http://www.vlsm-calc.net/> <http://www.fh-wedel.de/~kal> 23. Januar 2019 Folie Nr. 24

Wozu wird bei Einträgen in einer Routing-Tabelle oftmals auch eine Metrik-Information hinterlegt?

Ein Metrik-Wert wird in Hops angegeben. Dieser Wert sagt lediglich aus über wie viele Netzwerk-Abschnitte ein Datenpaket übertragen werden muss um an das gegebene Interface zu gelangen. Dieser Eintrag ist wichtig, damit Datenpakete nicht endlos im Netz herumgeschickt werden. (- **nicht ganz sicher**)

Die Wegwahl- bzw. Routing-Tabelle eines IPv4-Routers



Eine **Routing-Tabelle** ist **allgemein** eine „**Aufstellung der dem Router bekannten Zielnetze und wie sie erreicht werden können ...**“.

- Ist Entscheidungsbasis für **lokales Forwarding** von Paketen zum Ziel(netz)

Zielnetz & Subnetzmaske	Nächstes Interface	Woher stammt Eintrag	Metrik-Wert
213.39.233.16/28	213.39.233.46	statisch	2 Hops
0.0.0.0/0	213.39.232.11	statisch	1 Hop

Angabe zwingend nötig *Angabe optional*

- Tabelleneinträge können **statisch** und/oder **dynamisch** hinzugefügt werden.
 - ↳ Dynamische Einträge z.B. durch **Austausch** von Wegwahlinformationen mit benachbarten Routern (per **Routing-Protokoll**, wie z.B. dem **RIP**)
- Die **Weiterleitung** durch den Router erfolgt als
 - **Direktes Routing** zum Empfänger (Interface in einem der angeschlossenen Teilnetze)
 - **Indirektes Routing** über einen **weiteren Router** zum Ziel (-netz)
 - ↳ **Default-Router**-Eintrag als Platzhalter (**Wildcard**) für unbekannte Zielnetze
 - ✗ Schleifenbildung unbedingt vermeiden (A ↗ B ↗ A ...) !
- **Zusammenfassen und Verdichten der Tabelleinträge möglich** (→**Route Aggregation**)
 - ↳ Möglich u.a. per CIDR [**RFC 4632**] und einer Variable Length Subnet Mask (VLSM) [**RFC 1812**]

© Fachhochschule Wedel, Dipl.-Ing. (FH) I.Kaleck <http://www.fh-wedel.de/~kal> <http://www.vlsm-calc.net/> Seite Nr. 7 

2.2 SS17

Aufg1

Welche spezifische Aufgabe hat in der IEEE 802 LAN-Architektur der sog. MAC-Layer und ist dieser in allen aktuellen LAN-Technologien einheitlich (mit Begründung)? Wofür genau steht hier der Begriff MAC?

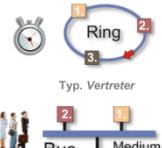
Der Media Access Control Layer (MAC-Layer) in LANs



- Der **MAC-Layer** stellt **je nach Topologie** eines **Netzes** ganz **unterschiedliche Arten (Klassen)** von **Medienzugriffsverfahren (MAC-Protokolle)** bereit.

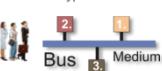
- **Deterministische Zugriffsverfahren**

- ↳ Sendezeitpunkt liegt in einem **irgendwie** bestimmbaren Zeitintervall
- ✗ **Token-Passing** (**Token-Ring**, **FDDI**, **ArcNet**-**TokenBus**), **Demand-Priority** (**Anyan**)



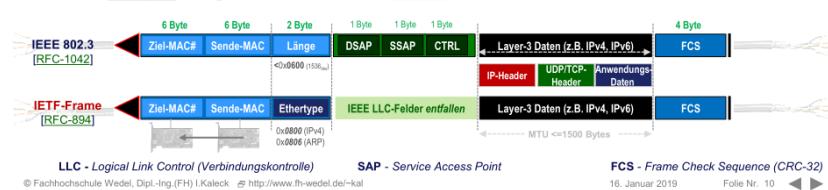
- **Stochastische Zugriffsverfahren**

- ↳ Sendezeitpunkt ist **nicht exakt** oder **gar nicht** bestimbar (berechenbar)
- ✗ **CSMA/CD** (**Ethernet**), **CSMA/CA** (**Wireless LANs** im **DCF-Betrieb**)



- **Speicherung notwendiger Zusatzinformationen im MAC-Header**

- ↳ Unterschiedliche MAC-Headerstrukturen je nach **Zugriffsverfahren!**
- ✗ **Beispiel: Mögliche Ethernet MAC-Frames** (Maximale Länge <= 1518 Bytes)



Die MAC ist die zweitunterste Schicht und umfasst Netzwerkprotokolle und Bauteile, die regeln, wie sich mehrere Rechner das gemeinsam genutzte physische Übertragungsmedium teilen. Sie wird benötigt, weil ein gemeinsames Medium nicht gleichzeitig von mehreren Rechnern verwendet werden kann, ohne dass es zu Datenkollisionen und damit zu Kommunikationsstörungen oder Datenverlust kommt.

Die Modellstruktur „Lokaler Netze“



- Das **IEEE 802 LAN-Modell** erweitert den **OSI Data-Link Layer** (-2) um eine **zusätzliche Zwischenschicht** auf dann **zwei Sublayer** (2a,2b)

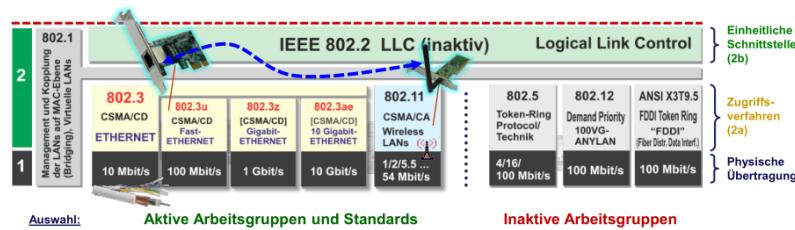


- Realisiert so einheitliche Schnittstelle zu den Netzwerkprotokollen

- **LLC** – **Logical Link Control Sublayer** (2b)
- **MAC** – **Media Access Control Sublayer** (2a)
- **PHY** – **Physical Control Layer** (1)

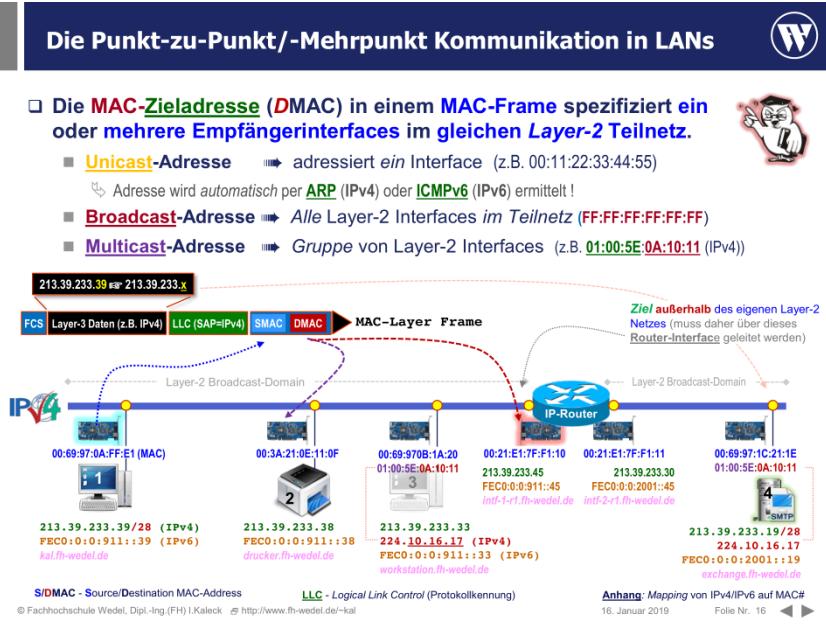
- ✗ Kennzeichnung spezifischer IEEE 802.x **Projektgruppen** (Task-Forces) innerhalb der IEEE 802.x Workgroup (WG) durch **Suffix-Buchstaben** (z.B. IEEE 802.3y).

Übersicht z.B. unter "IEEE 802.3 Ethernet Working Group"



Wozu wird eine MAC-Adresse denn überhaupt benötigt, wenn ein System (Interface) im LAN doch bereits über eine IPv4-Adresse verfügt? Wofür steht hier der Begriff **MAC**? „missing IDENTIFIER“

Die MAC-Adresse spezifiziert die Kommunikation auf Layer-2 eine IP-Adresse arbeitet auf Layer-3 (und aufwärts)



MAC: Media Access Control

2.3 WS15

Aufg1

Skizzieren Sie grob die Struktur bzw. Aufteilung des IEEE-802 LAN Schichtenmodells. Welche der OSI-Funktionsschichten umfasst diese Struktur?

Die Modellstruktur „Lokaler Netze“

- Das **IEEE 802 LAN-Modell** erweitert den OSI **Data-Link Layer** (-2) um eine zusätzliche Zwischenschicht auf dann **zwei Sublayer** (2a,2b)

- Realisiert so einheitliche Schnittstelle zu den Netzwerkprotokollen

- **LLC** – Logical Link Control Sublayer (2b)
- **MAC** – Media Access Control Sublayer (2a)
- **PHY** – Physical Control Layer (1)

- X Kennzeichnung spezifischer IEEE 802.x **Projektgruppen** (Task-Forces) innerhalb der IEEE 802.x Workgroup (WG) durch Suffix-Buchstaben (z.B. IEEE 802.3y)..

Übersicht z.B. unter "[IEEE 802.3 Ethernet Working Group](#)"

2	Management und Konfiguration auf der LAN-Ebene (Bridging), Virtuelle LANs	802.1
1	Auswahl:	802.2
	Aktive Arbeitsgruppen und Standards	IEEE 802.2 LLC (aktiv)
	Inaktive Arbeitsgruppen	Logical Link Control
		Einheitliche Schnittstelle (2b)
		Zugriffsverfahren (2a)
		Physische Übertragung

802.1 Management und Konfiguration auf der LAN-Ebene (Bridging), Virtuelle LANs

802.2 IEEE 802.2 LLC (aktiv)

802.3 802.3 CSMACD ETHERNET

802.3u 802.3u CSMACD Fast-ETHERNET

802.3z 802.3z [CSMA/CD] Gigabit-ETHERNET

802.3ae 802.3ae [CSMA/CD] 10 Gigabit-ETHERNET

802.11 802.11 CSMA/CA Wireless LANs

802.5 802.5 Token-Ring Protokoll

802.12 802.12 Demand 100VG- ANYLAN

FDDI 802.12 FDDI "Fiber-Duo Data Interf."

ANSI X3T9.5

10 Mbit/s

100 Mbit/s

1 Gbit/s

10 Gbit/s

1/2/5.5 / 54 Mbit/s

4/16 / 100 Mbit/s

100 Mbit/s

100 Mbit/s

Aktive Arbeitsgruppen und Standards

Inaktive Arbeitsgruppen

© Fachhochschule Wedel, Dipl.-Ing.(FH) I.Kaleck <http://www.fh-wedel.de/~kaleck>

16. Januar 2019

Folie Nr. 7

2.4 WS16

Aufg1

Welche konkrete Aufgabe hat in den IEEE 802 LANs speziell der MAC-Layer?
Ist dieser generell einheitlich?

In eigenen Worten:-Zweit unterste Schicht vom OSI-Modell (unterste Schicht der aufgeteilten Sicherungsschicht)- Umfasst Netzwerkprotokolle, regelt wie sich mehrere Rechner das gemeinsam genutzte physische Übertragungsmedium teilen.- Je nachdem ob Zugriff *kontrolliert* oder *konkurrierend* stattfinden soll wird ein entsprechendes Verfahren genutzt (kontrolliert Beispiel Schule - Siehe nächster Absatz; konkurrierend z.B. CSMA/CD)

- Kontrollierter Zugriff
 - Token-Ring
 - Token-Bus
 - CSMA/CA
- Konkurrierender Zugriff
 - ALOHA
 - CSMA/CD
 - CSMA/CR

Wikipedia:Media Access Control [midja kses kntl] oder Medium Access Control [midjm] (MAC, engl. „Medienzugriffssteuerung“) ist eine vom Institute of Electrical and Electronics Engineers (IEEE) entworfene Erweiterung des OSI-Modells. Das IEEE unterteilte die Sicherungsschicht (Schicht 2) des OSI-Modells in die Unterschichten Media Access Control (2a) und Logical Link Control (2b), wobei die MAC die untere der beiden ist.Das OSI-Modell ordnet die in einem Rechnernetz benötigten Hardware- und Softwareteile in insgesamt sieben Schichten ansteigender Komplexität an. Je höher eine Schicht liegt, desto weniger interessant ist sie für den technischen Ablauf der Datenübertragung und umso mehr ist sie mit dem eigentlichen Inhalt der Daten beschäftigt. Die MAC ist die zweitunterste Schicht und umfasst Netzwerkprotokolle und Bauteile, die regeln, wie sich mehrere Rechner das gemeinsam genutzte physische Übertragungsmedium teilen. Sie wird benötigt, weil ein gemeinsames Medium nicht gleichzeitig von mehreren Rechnern verwendet werden kann, ohne dass es zu Datenkollisionen und damit zu Kommunikationsstörungen oder Datenverlust kommt. Im ursprünglichen OSI-Modell war eine solche Konkurrenz um das Kommunikationsmedium nicht vorgesehen, weshalb die MAC dort nicht enthalten ist.

IEEE 802.2 – Logical Link Control Sublayer (LLC)

Die einheitliche LLC-Zwischenschicht dient zur Realisierung der Unabhängigkeit von spezifischen MAC-Zugriffsverfahren.

- Zugriff über einheitlichen Dienstzugangspunkt (Service Access Point)
- Repräsentiert ursprüngliche Sicherungsfunktion des Data-Link Layer
 - X IEEE-LANs erlauben per LLC (Typ-1) nur eine Fehlererkennung !!
- LLC-Daten speichern im Frame nur 1-Byte Protokoll-Kennung (z.B. IPv4, OSI, ...)
- X In Ethernet-LANs wird LLC meist durch 16-Bit Protokollfeld (Ethertype) ersetzt.

Netzwerkprotokolle
SAP

IEEE Specification

* IPv6 hat keinen 1-Byte SAP-Wert => erweitertes SNAP-Rahmenformat notwendig

MAC – Media Access Control

16. Januar 2019 Folie Nr. 9

Der Media Access Control Layer (MAC-Layer) in LANs

Der MAC-Layer stellt je nach Topologie eines Netzes ganz unterschiedliche Arten (Klassen) von Medienzugriffsverfahren (MAC-Protokolle) bereit.

- Deterministische Zugriffsverfahren
 - Sendezeitpunkt liegt in einem irgendwie bestimmbarer Zeitintervall
 - X Token-Passing (Token-Ring, FDDI, ArcNet-TokenBus), Demand-Priority (Anylan)
- Stochastische Zugriffsverfahren
 - Sendezeitpunkt ist nicht exakt oder gar nicht bestimmbar (berechenbar)
 - X CSMA/CD (Ethernet), CSMA/CA (Wireless LANs im DCF-Betrieb)
- Speicherung notwendiger Zusatzinformationen im MAC-Header
 - Unterschiedliche MAC-Headerstrukturen je nach Zugriffsverfahren!
 - X Beispiel: Mögliche Ethernet MAC-Frames (Maximale Länge <= 1518 Bytes)

IEEE 802.3 [RFC-1042]

IETF-Frame [RFC-894]

LLC - Logical Link Control (Verbindungssteuerung)

SAP - Service Access Point

FCS - Frame Check Sequence (CRC-32)

16. Januar 2019 Folie Nr. 10