Kommunikationssysteme Selbstlernfragen und Antworten

Sven Bergmann

31. Mai 2022

Inhaltsverzeichnis

Vorlesung 1 - Schichtenmodelle

Was ist der Unterschied zwischen Client-Server und Peer-to-Peer Netzwerken?

- Client-Server
  - Server-Prozess: Langlebige Anwendung, die kontinuierlich auf Anfragen wartet, diese verarbeitet und beantwortet
  - Client-Prozess: Zumeist kurzlebige Anwendung die Anfragen an den Server-Prozess stellt und auf die Antwort wartet. Die Rolle ist damit zumeist beendet
- Peer-to-Peer
  - Gleichrangige Kommunikationspartner
  - Oft bessere Leistung als Client-Server
  - Übergreifender Datenbestand

Welche Arten Proxies existieren in Rechnernetzen, und welche Aufgaben haben sie typischerweise?

- Forward Proxy
- Reverse Proxy
- Aufgaben:
  - Proxy zum Zwischenspeichern/Anonymisieren
  - Proxy zum Lastbalancieren von Webseiten

Wie unterscheiden sich Point-to-Point und Multi-Access-Netzwerke?

- Point-to-Point (Punkt-zu-Punkt)
  - Ein Paar von Rechnern ist durch eine direkte Leitung verbunden
  - kein anderer Rechner kann diese Leitung nutzen
  - Full-Duplex: Senden und Empfangen gleichzeitig möglich
  - Half-Duplex: Nur eines von beiden gleichzeitig möglich
  - Simplex: Daten können nur in eine Richtung fließen
- Multi-Access-Netze
  - Mehrere angeschlossenen Rechner teilen sich einen Übertragungskanal
  - Damit Daten trotzdem an den richtigen Empfänger gesendet werden, müssen sie mit einer Zieladresse versehen werden
  - Daten werden in Übertragungseinheiten (Frames) eingeteilt und mit der Adresse des Empfängers ausgewiesen
  - „Rechner“ prüfen, ob die Nachricht für sie ist (aktiver Vorgang!)
  - Sollen alle Stationen gleichzeitig eine Nachricht erhalten, so werden Broadcast-Adressen (spezielle Adressen zur Adressierung aller Stationen) verwendet

Welche Konsequenzen entstehen für die Datenkommunikation im Falle von Multi-Access-Netzwerken?

- Mehrere angeschlossenen Rechner teilen sich einen Übertragungskanal
- Damit Daten trotzdem an den richtigen Empfänger gesendet werden, müssen sie mit einer Zieladresse versehen werden
- Daten werden in Übertragungseinheiten (Frames) eingeteilt und mit der Adresse des Empfängers ausgewiesen
- „Rechner“ prüfen, ob die Nachricht für sie ist (aktiver Vorgang!)
- Sollen alle Stationen gleichzeitig eine Nachricht erhalten, so werden Broadcast-Adressen (spezielle Adressen zur Adressierung aller Stationen) verwendet

Wie unterscheiden sich statische und dynamische Netzwerke?

- Statische Netze:
  - fest verdrahtete Punkt-zu-Punkt Verbindungen oder Multi-Access-Netze
  - jeder Knoten besitzt eine feste Anzahl von Nachbarn oder einen Zugang zu einem Multi-Access-Netze
  - besitzen keine inhärent im Netz verankerte Vermittlungsfunktion
  - Vermittlung über Netzgrenzen hinweg jedoch durch Weiterleiten möglich (Store-and-Forward)
- Dynamische Netze:
  - Verbindungen enthalten konfigurierbare Schaltelemente
  - diese können dynamisch vermitteln (Weg wird geschaltet)
  - ein- oder mehrstufiger Aufbau möglich
  - Mit Aufwand blockadefreie Schaltungen ohne Crossbar

Ordnen Sie die Begriffe Paketvermittlung und Leitungsvermittlung zu!

- Die Leitungsvermittlung (circuit switching) stellt zwischen zwei oder mehr Teilnehmern einen Übertragungskanal über mehrere Vermittlungsstellen für die Dauer der Übertragung her. Die Leitungsvermittlung eignet sich in der Regel für zeitkritische Anwendungen bzw. der Übertragung von Daten in Echtzeit.
- Bei der Paketvermittlung (store and forward) werden die Daten oder Informationen in Pakete aufgeteilt. Der Dienst bzw. die Anwendung übergibt die einzelnen Pakete an das Kommunikationssystem und versieht sie mit der Zieladresse und weiteren Vermittlungsinformationen. Das Kommunikationssystem vermittelt die Datenpakete vom Sender zum Empfänger. Die Pakete können dabei unterschiedliche Wege zu ihrem Ziel nehmen. Beim Empfänger werden die Datenpakete dann wieder zusammengesetzt. Die Paketvermittlung eignet sich für zeitunkritische Übertragungen.

Was versteht man unter dem Store-and-Forward-Verfahren, und wo wird es eingesetzt?

- Im Netz findet ein Store-and-Forward statt. An der Grenze zwischen zwei Netzen sorgen Router für die Weiterleitung der Daten. Nach dem Empfang findet die Entscheidung über den nächsten Router konzeptionell anhand der Zieladresse statt.
- Wird in der Internet-Schicht eingesetzt (entspricht ISO/OSI 3) bei statischen Netzen

Welche Metriken kennen Sie, um Topologien von Rechnernetzen zu charakterisieren?

- Durchmesser (Diameter)
  - Maximaler Abstand zweier Knoten, d. h. die Anzahl von Kanten
  - → Ziel: Möglichst klein (Zeitbedarf für Übertragung)
- Bisektionsbreite (Connectivity)
  - Minimale Anzahl von Kanten die man entfernen muss, um das Netzwerk in zwei Hälften zu teilen
  - → Ziel: Möglichst groß zur Verbesserung der Fehlertoleranz
- Knotengrad
  - Anzahl von Verbindungen eines Knotens zu seinen Nachbarn. Ist die Anzahl nicht konstant, so wird das Maximum aller Knoten genommen.
  - → Ziel: Möglichst klein, da die Kosten so mit diesem Grad steigen

Welche räumliche Ausdehnung besitzen typischerweise LANs?
10 m – wenige km

Was versteht man unter einem Protokoll im Kontext der Datenkommunikation?
Ein Protokoll ist die Gesamtheit aller Vereinbarungen zwischen Computeranwendungen zum Zweck einer gemeinsamen Kommunikation

Nennen Sie 3–4 Problemdomänen, die für eine erfolgreiche Datenkommunikation zu lösen sind!

- Kodierungsregeln und Semantiken der Nutzdaten
- Regelung der Übertragungsrichtung (wer redet, wer hört zu?)
- Adressierung des Zielsystems für die Datenübertragung
- Wegefindung der Daten in komplexen, hierarchischen Netzen
- Erkennung und Korrektur von Übertragungsfehlern
- Regelung des Zugriffs auf das Übertragungsmedium
- Darstellung der Nutzdaten als physikalisches Signal

Welche Vorteile (und ggf. auch Nachteile) haben Schichten-Architekturen?

- Vorteile:
  - Einzelne Schichten sind leicht veränderbar, bei der Einhaltung der Schnittstellen/Interfaces
  - Bei Veränderung der Schnittstellen/Interfaces sind nur die beiden angrenzenden Schichten betroffen
  - Schichtenarchitekturen kapseln Maschinenabhängigkeiten, daher leicht portierbar. Nur die innerste Schicht muss neu implementiert werden
- Nachteile:
  - Es ist schwierig Systeme sauber in Schichten zu strukturieren. Wenn äußere Schichte Dienste der inneren Schichten benötigen, wird leicht die einfache Abhängigkeit von der nächst unteren Schicht zerstört
  - Es kann Performanz-Probleme geben, weil mit dem Zugriff auf die Dienste eine Schicht immer eine gewisser Overhead verbunden ist

Wie heißen die sieben Schichten des ISO/OSI-Modells, und welche grobe Aufgabe haben sie jeweils?

- Schicht 7: Anwendungsschicht (Application Layer)
  - In dieser Ebene werden (Standard-)Schnittstellen zur Verfügung gestellt, die bestimmten Anwendungstypen ganze Kommunikationsdienste bereitstellen
  - Ein Beispiel hierfür ein allgemeingültiges Protokoll zur Übertragung von Webseiten samt fest definierter Schnittstelle (GET, POST, DELETE, ...) sein. Wer einen Webbrowser oder einen Webserver implementieren will, könnte dann diese Schnittstelle zur Kommunikation mit den Produkten anderer verwenden
  - **Merke:** Das Internet realisiert das anders.
- Schicht 6: Darstellungsschicht (Presentation Layer)
  - Beschäftigt sich damit, die zu übertragenden Daten so darzustellen, dass sie von vielen unterschiedlichen Systemen gehandhabt werden können
  - Beispielsweise codieren manche Rechner einen String mit ASCII-Zeichen, andere benutzen Unicode, manche benutzen bei Integern das 1-, andere das 2-Komplement. Problematisch ist auch die Byteordnung des Prozessors (Big/Little-Endian)
  - Formal wird hier das verwendete Format beschrieben
    - Anstatt für jede Anwendung eine eigene Übertragungssyntax und semantik zu definieren, stellt man hier eine allgemeingültige Lösung bereit
    - Die spezifischen Daten eines Rechners werden hier eindeutig beschrieben
- Schicht 5: Sitzungsschicht (Session Layer)

  - Dialogkontrolle, d. h. es kann festgelegt werden, welcher Kommunikationspartner wann übertragen darf (wer redet, wer hört zu?). Da wir bei ISO/OSI eigentlich eine Steuerung über einen Header benötigen könnte hierzu ein Token verwendet werden. Bei bestimmten Operationen darf dann nur der Kommunikationspartner, der im Besitz des Tokens ist, diese Operation durchführen
  - Wichtiger Ansatz wäre auch die Bereitstellung von Wiederaufsetzpunkten. Wurde beispielsweise eine 2-stündige Dateiübertragung mittendrin durch einen Ausfall unterbrochen, so braucht nicht die gesamte Übertragung wiederholt werden, sondern man geht nur bis zum letzten Aufsetzpunkt zurück

- Schicht 4: Transportschicht (Transport Layer)
  - Ermöglicht die Kommunikation zwischen Anwendungen der Endsysteme
    * Segmentierung von Datenströmen zur Übertragung der Daten in Einheiten: Datagramme (Paketen)
    * Verbergen wesentlicher Charakteristika der Netzinfrastruktur
  - Aufgabe: Transport der Daten zwischen den Kommunikationspartnern mit bestimmten (aushandelbaren) Dienstmerkmalen
    * Adressierung von Anwendungsprozessen
    * Eventuell Regeln zur Behandlung von Fehlern
    * Eventuell Flusskontrolle/Staukontrolle zur Anpassung der Datenrate an die Fähigkeiten des Netzes und des Empfängers

- Schicht 3: Vermittlungsschicht (Network Layer)
  - Übertragung der Daten zwischen Rechnern in einem Netz aus Netzen
  - Hauptaufgabe ist dabei, eine geeignete Wegewahl (Routing) zu treffen
  - Eine notwendige Voraussetzung sind dazu u. a. ein gemeinsamer Adressraum für Rechner und eine Einigung auf eine maximale PDU-Größe (Datagramm-Größe)
  - Statisches Netzkonzept: Zwischenknoten speichern ankommende Nachrichten zwischen und ermitteln (über Tabellen) den Teilnehmer, der die Daten als nächstes erhält. Hierbei muss man mit diesem direkt kommunizieren können.
  - Weiterhin: Multiplexing mehrerer logischer Verbindungen über eine physikalische Verbindung

- Schicht 2: Sicherungsschicht (Data Link Layer)
  - Kommunikation zwischen Rechnern in einem einzelnen Netz
  - Logical Link Control (LLC):
    * Liefert der Vermittlungsschicht eine fehlerfreie Übertragung der Daten zwischen zwei Rechnern (z. B. innerhalb eines lokalen Netzes)

        * Dazu werden die ankommenden Daten in sog. Rahmen unterteilt, die einzeln übertragen werden
        * Der Empfänger überprüft, ob die Übertragung korrekt war (z. B. mittels einer Prüfsumme). Im Fehlerfall wird der entsprechende Rahmen neu angefordert
        * Weiterhin wird versucht, eventuell auftretende Staus durch Flusskontrolle zu vermeiden, z. B. wenn der Empfänger überlastet ist.
    - Medium Access Control:
        * Bei lokalen Netzen wird außerdem der konfliktfreie Zugriff auf das Netz geregelt, es können ja ggf. nicht mehrere Teilnehmer gleichzeitig senden

- Schicht 1: Bitübertragungsschicht (Physical Layer)
    - Transportiert die einzelnen Bits über eine bestimmte physikalische Leitung (Medium)
    - D. h. es muss festgelegt werden, welchen Leitungstyp man benutzt und wie eine "1" bzw. eine "0" auf der Leitung kodiert werden
        * Dazu legt man z. B. bei Verwendung von Kupferkabel als Leitung fest, dass Bits als Spannungspulse übertragen werden (z. B. „Übertrage für eine Millisekunde +1 Volt, um eine 1 zu transportieren")
    - Weiterhin wird definiert:
        * Stecker (Pinbelegungen),
        * Übertragungsrichtung (uni-/bidirektional),
        * ...

Wie überträgt jede Schicht die für sie relevanten Informationen?
Schicht n versieht ihre Nachricht mit Kontrollinformationen (z. B. in Form eines Headers) und versendet alles zusammen (oftmals Protocol Data Unit (PDU) genannt). Dazu nutzt sie die Dienste der nächsttieferen Schicht (n-1).

Welche Unterschiede existieren zwischen dem ISO/OSI-Modell und dem Internet-Referenzmodell?

	ISO/OSI-Modell	Internet-Referenzmodell
Alias	Open Systems Interconnection	Transmission Control Protocol (TCP)
# Schichten	7	4
Zuverlässigkeit		zuverlässiger als ISO/OSI
Grenzen	streng	nicht sehr streng
Ansatz	vertikal	horizontal
–	verwendet verschiedene Session- und Präsentationsschichten	verwendet in der Anwendungsschicht sowohl die Session- als auch die Präsentationsschicht
Kommunikation	Unterstützt auf der Netzwerkebene sowohl verbindungslose als auch verbindungsorientierte Kommunikation	bietet Unterstützung für die verbindungslose Kommunikation innerhalb der Netzwerkschicht
Abhängigkeit	protokollunabhängig	protokollabhängig

Zu welcher Schicht gehören die Protokolle TCP und UDP, und wie unterscheiden sie sich?
Beide Protokolle gehören zur Schicht 4, der Transport-Schicht.

	TCP	UDP
Zuverlässigkeit	hoch	niedriger
Geschwindigkeit	niedriger	hoch
Transfermethode	Pakete werden nacheinander zugestellt	Pakete werden im Datenstrom zugestellt
Fehlererkennung und – behebung	ja	nein
Congestion control	ja	nein
Empfangsbestätigung	ja	nur die Prüfsumme

Welche Vorteile hat es (bzw. warum ist es notwendig), die Host-to-Network-Schicht komplett in Hardware zu realisieren?
Idee: Die faktische Datenübertragung wird von der Netzwerkkarte des Rechners erledigt

- Vorteil bei Multi-Access-Netzen: Die Netzwerkkarte kann selber entscheiden, ob die Daten für den eigenen Rechner sind → Entlastung des Betriebssystems (da kein Interrupt notwendig)
- Starke Entkopplung vom Betriebssystem: IP teilt dem Treiber der Netzwerkkarte mit, dass diese Daten (zuverlässig) an eine gegebene Zieladresse (MAC-Adresse) übertragen soll
- Übertrage das IP-Datagramm der Länge 1500 Byte an die MACAdresse

- Direkte Anbindung des Zielrechners erforderlich

Vorlesung 2 - Sockets und Darstellungsschicht

Wer kommuniziert beim Internet-Referenzmodell letztendlich miteinander?
Die Schichten untereinander und die Schicht 1 mit der Schicht 1

Welche 3 Arten von 'Adressen' werden im Internet-Referenzmodell für die Kommunikation benötigt?

- Portnummern
- IP-Adressen
- MAC-Adressen

Was abstrahiert aus Programmiersicht ein sog. 'Socket'?
Einen TCP Clienten

Warum haben Client- und Serversockets eine unterschiedliche Anzahl von Konstruktorparametern?
Der Clientsocket muss den Zielrechner und den eigenen Port mitgeben, um Daten senden und empfangen zu können, während der Serversocket nur den Port mitgeben muss, um Verbindungen zu akzeptieren.

Was bewirkt auf Serverseite der Aufruf von accept()?
Damit wartet der Server auf eingehende Verbindungswünsche.

Was ist bei der Programmierung von Servern zu beachten, wenn eine hohe Zahl an Anfragen erwartet wird?
Jeden Clienten in einem eigenen Thread bearbeiten.

Wodurch unterscheiden sich Little- und Big-Endian-CPUs, und warum kann das zu Problemen bei der Datenkommunikation führen?

- Bei **Big-Endian** wird das „große Ende“ (also der signifikanteste Wert in der Sequenz) zuerst abgelegt (also in niedrigsten Speicheradresse)
- Bei **Little-Endian** wird das „kleinste Ende“ (also der am wenigsten signifikante Wert) zuerst gespeichert

Definieren Sie die Begriffe “Abstrakte Syntax“ und “Transfersyntax“

- Abstrakte Syntax
  - Übertragung der grundsätzlichen Struktur der Daten

$$Serialisierung - Deserialisierung$$

- Transfersyntax
  - Übertragung des konkreten Datenstroms mit einer vereinbarten Kodierung

$$Marshalling - Unmarshalling$$

Was versteht man unter (De-) Serialisierung?
Deserialisierung ist die Wiederherstellung eines Objektes ohne Vorwissen über die Typen der Objekte

Nennen Sie 3 Technologien oder APIs, die das Übertragen von abstrakten/strukturierten Daten über ein Rechnernetz ermöglichen!

- ISO:
  - ASN.1 (Abstract Syntax Notation)
- Sun ONC (Open Network Computing)-RPC:
  - XDR (eXternal Data Representation)
- OSF (Open System Foundation)-RPC:
  - IDL (Interface Definition Language)
- Corba:
  - IDL und CDR (Common Data Representation):
  - CDR bildet IDL-Datentypen in Bytefolgen ab.
- W3C:
  - XML/SOAP
  - Darstellung aller Datentypen als (Maschinen-)lesbarer Text. Zu klären: Zeichenkodierung
- Java:
  - Objektserialisierung, d. h. Abflachung eines (oder mehrerer) Objektes zu einem seriellen Format inkl. Informationen über die Klassen. Deserialisierung ist die Wiederherstellung eines Objektes ohne Vorwissen über die Typen der Objekte
- JavaScript:
  - JSON (JavaScript Object Notation)

Erklären Sie den Aufbau und die syntaktischen Elemente eines XML-Dokumentes!

- XML-Dokumente: Zeichendaten und Auszeichnungen
  - XML- und Dokumenttyp-Deklarationen

```
<?xml version=``1.0`` encoding=``UTF-8``?>
```

  - Elemente mit möglichem Inhalt

```
<name>Volker Sander</name>
```

  - Attributen in Elementen

```
<name attribute=``Wert``>
```

- Entity-Referenzen (< statt <)
- Kommentare
  <!– Das ist ein Kommentar –>
- Processing Instructions – werden an die aufrufende Instanz weitergeleitet
  <?name pidata?>
- Jedes Dokument entspricht einer Baumstruktur (DOM – Document Object Model)
- Die Baumknoten werden Elemente genannt
- Es kann nur ein Element an der Wurzel geben
- Syntaxregeln müssen strikt eingehalten werden
  * Jedes Starttag muss ein Endtag haben

    <BOOK>...</BOOK>
    <BOOK />

  * Verschachtelung nur mit vollständigen Tags möglich:

    <BOOK> <LINE> This is OK </LINE> </BOOK>

    <LINE> <BOOK> This is </LINE> definitely NOT </BOOK> OK

  * Attributwerte müssen mit ‘ oder “ abgegrenzt werden

Was ist der Unterschied zwischen Wohlgeformtheit und Validität bei einem XML-Dokument?

- Wohlgeformtheit:
  - Dokument entspricht den syntaktischen Regeln
    * Genau ein Dokument-Element
    * Jedes öffnende Tag hat ein schließendes Tag.
    * Die Verschachtelung ist balanciert.
- Validät:
  - Dokument ist:
    * wohlgeformt
    * konform zu einer fest vorgegebenen Dokumentenstruktur
    * Document Type Description (DTD)
    * XML Schema Definition (XSD)

Wozu dient ein XML-Schema?
Ein XML Schema enthält in XML notierte Regeln, die erlaubte Elementbezeichner, Reihenfolgen, Inhalte und Attribute mit Wertebereichen aufzählen

Nennen Sie 3 Kompositoren (und deren Ergänzungen), die in XML-Schemas verwendet werden können!

- ```
  <xsd:sequence>
      [Inhalt 1]
      ...
      [Inhalt n]
  </xsd:sequence>

  <xsd:all>
      [Elementdeklarationen]
  </xsd:all>
  ```

- ```
  <xsd:choice>
      [Inhalt a]
      ...
      [Inhalt x]
  </xsd:choice>
  ```

Wozu dient das SOAP-Protokoll, und wie ist es grundlegend aufgebaut?

- SOAP (ursprünglich für Simple Object Access Protocol) ist ein Netzwerkprotokoll, mit dessen Hilfe Daten zwischen Systemen ausgetauscht und Remote Procedure Calls durchgeführt werden können.
- SOAP regelt, wie Daten in der Nachricht abzubilden und zu interpretieren sind
- SOAP stellt so eine Konvention für entfernte Prozedur-/Methodenaufrufe dar
- Eine SOAP-Nachricht besteht zunächst auf der obersten Ebene aus einem Envelope
- Der Envelope enthält einen optionalen Header sowie die eigentliche Nachricht im SOAP Body

Wie ist eine JSON-Datei grundsätzlich aufgebaut?
Beispiel:

```
{
    "id" : 564146,
    "Name" : "Mustermann",
    "Vorname" : "Max"
}
```

Vorlesung 3 - Internet, IP Adressen und CIDR

Was ist ein sog. Autonomes System (AS) im Internet?
In IP-Netzen sind autonome Systeme (AS) ein Verbund von Routern und Netzwerken, die einer einzigen administrativen Instanz unterstehen, einer Organisation oder einem Unternehmen. Das bedeutet, dass sie alle zu einer Organisation oder zu einem Unternehmen gehören.

Wodurch sind Tier 1–3 ISPs charakterisiert?

- Tier 1 Internet Service Provider (ISPs) (bieten die Basis des Internets)
  - Treten gleichberechtigt auf
  - Anbindungen an bestimmten Orten
- Tier 2 ISPs: kleinerer (oft nur regional tätiger) ISP
  - Anbindung an einen oder mehrerer Tier-1 ISPs
  - Ggf. Anbindung an weitere Tier-2 ISPs
- Tier 3 ISPs und lokale ISPs
  - Binden die Kunden an ("access network", z. B. über DSL)
  - Dienst nahe den Endsystemen

Beschreiben Sie mit eigenen Worten, was ein Router nach dem Empfang eines Paketes mit der IP-Zieladresse X zu tun hat! Welche Informationen werden dabei benötigt?

- Informationen zu extrahieren:
  - In welches Netz muss das Paket ausgeliefert werden?
  - Falls Router das Zielsystem direkt erreichen kann (also eine direkte Verbindung zum Zielnetz besitzt): An welchen Rechner muss das Paket ausgeliefert werden?
- Die Adresse muss also Informationen über das Ziel-**Netz** und den Ziel-**Rechner** enthalten! (vgl.: Vorwahl/Durchwahl beim Telefonieren)

Wie kann im (alten) klassenbasierten System von IP-Adressen erkannt werden, um was für eine Klasse es sich im konkreten Fall handelt?
Über die ersten Bits (Class A: 0, Class B: 10, Class C: 110, Class D: 1110, Class E: 1111)

Wie viele Knoten (Hosts) können maximal an ein Class-B Netz angeschlossen werden?
IP-Adressklassen:

1. Class A für Netze mit bis zu 16 Mio. Knoten (0-127)
2. Class B für Netze mit bis zu 65.536 Knoten (128-191)
3. Class C für Netze mit bis zu 256 Knoten (192-223)

4. Class D für Gruppenkommunikation (Multicast) (224)
5. Class E, noch reserviert für zukünftige Anwendungen

Class	Start	Ende	Anzahl Netze	Rechner / Netz
A	1.0.0.0	127.255.255.255	127	16.777.214
B	128.0.0.0	191.255.255.255	16384	65534
C	192.0.0.0	223.255.255.255	2.097.152	254
D	224.0.0.0	239.255.255.255	Multicast	
E	240.0.0.0	255.255.255.254	Reserved	

Welche speziellen Werte existieren für den Host-Anteil in einer IP-Adresse, und was bedeuten sie?

- Die 0 darf nicht vergeben werden, da der Rechner sonst die selbe IP-Adresse wie die Netzwerkkennung hätte.
- Die 255 darf nicht vergeben werden, da dies die sogenannte Broadcast Adresse darstellt.

Was sind sog. private IP Adressen und Netzwerke?

Private IP-Adressen (abgekürzt Private IP) sind IP-Adressen, die von der IANA nicht im Internet vergeben sind. Sie wurden für die private Nutzung aus dem öffentlichen Adressraum ausgespart, damit sie ohne administrativen Mehraufwand (Registrierung der IP-Adressen) in lokalen Netzwerken genutzt werden können.

Was ist eine Subnetzmaske (häufig auch einfach nur Netzmaske genannt) und wie ist sie aufgebaut?

Subnetzmasken kennzeichnen den Bereich der IP-Adresse, der das Netzwerk und das Subnetzwerk beschreibt. Dieser Bereich wird dabei durch Einsen („1“) in der binären Form der Subnetzmaske festgestellt.

Beispiel	140.	201.	10.	100
	255.	255.	255.	0
Netzwerk:	140.	201.		
Subnetz:			10.	
Endsystem:				100

Wie kann man aus einer Ziel-IP und einer Netzmaske die Adresse des Ziel-Netzes berechnen?

Indem man beide Adressen mit AND verknüpft

Welche Vorteile hat CIDR gegenüber dem alten Ansatz der klassenbasierten IP-Adressen?

- Trennung von starrer Klasseneinteilung durch Ersetzen der festen Klassen durch Netzwerk-Präfixe variabler Länge
- Die Längenangabe sagt aus, wie viele Bit als Netzteil der Adresse verwendet werden sollen (Länge der 1-Folge)

- Router merken sich in ihrer Routing-Tabelle zusätzlich zu den IP-Adressen die Präfixlänge, z. B. 194.142.0.x/17 = betrachte die ersten 17 Bit als Netzadresse
- Sehr flexible Gestaltung von Routing-Tabellen möglich

Was muss ein Router bei Verwendung von CIDR für jeden Eintrag in der Routing-Tabelle speichern?
Router merken sich in ihrer Routing-Tabelle zusätzlich zu den IP-Adressen die Präfixlänge, z. B. 194.142.0.x/17 = betrachte die ersten 17 Bit als Netzadresse

Erklären Sie das Logest-Prefix-Match Verfahren!
Suche nach dem Routing-Eintrag mit der größten Überdeckung der Zieladresse

Ziel	11.1.2.5	= 00001011.0000001.00000010.00000101
Route #1	11.1.2.0/24	= 00001011.0000001.00000010.00000000
Route #2	11.1.0.0/16	= 00001011.0000001.00000000.00000000
Route #3	11.0.0.0/8	= 00001011.0000000.00000000.00000000

Es wird der Weg ermittelt, welcher am genausten spezifiziert wird (most specific)

Unter welchen Voraussetzungen können bei CIDR Einträge in einer Routing-Tabelle zusammengefasst werden?
- Der Longest Prefix Match Algorithmus erlaubt das Zusammenfassen von Routen
  - Es reicht, wenn die genaue Adresse erst nahe am Ziel bekannt ist
  - Signifikanter Beitrag zur Reduktion der Größe der Routing-Tabellen im Internet
- **Vorsicht:** Durch das Zusammenfassen von Routing-Einträgen dürfen keine fehlerhaften Regeln entstehen
  1. Ein Zusammenfassen in nur möglich, wenn gleiche Ziele (Next Hop) verwendet werden
  2. Die relaxierte Interpretation der Netzwerkadresse kann ggf. andere, nicht gewollte Einträge umfassen. Hier hilft aber ggf. die Longest Match Regel. Hierzu muss aber der Präfix der überschriebenen Regel länger sein.
  3. 0.0.0.0/0 ist ein Default-Route

Wozu dient der default-Route Eintrag in einer Routingtabelle?
Die Default-Route wird gewählt, wenn keine Route bevorzugt wird.

Vorlesung 3 - Beispielaufgaben

Übungsaufgabe 1:
Gehen Sie von der folgenden (vereinfacht dargestellten) Routing-Tabelle aus:

Zieleintrag	Zu nehmender Router
139.179.200.0/21	R1
139.179.128.0/18	R2
139.179.112.0/20	R3
139.179.192.0/20	R4
139.179.0.0/16	R5

An welchen Router werden die folgenden Ziel-IP-Adressen verschickt?

(a) 139.179.60.10

(b) 139.179.210.40

(c) 139.179.197.55

(d) 139.179.205.180

Begründen Sie Ihre Antwort!

Übungsaufgabe 2: Gegeben sei die vereinfacht dargestellte Routing-Tabelle:

Zielnetz (CIDR)	Router
128.128.0.0/9	R1
128.160.0.0/11	R2
128.176.0.0/12	R1
128.192.0.0/10	R1
default	R3

Können Sie hier Routing-Einträge zusammenfassen? Falls ja, welche, und wie sehen die zusammengefassten Einträge aus? Zusatzfrage: Kann weiter vereinfacht werden, wenn die Präfixe in der Tabelle geändert werden dürfen?

Vorlesung 3 - Lösungen

Übungsaufgabe 1:
Um diese Aufgabe zu lösen, muss der sog. longest prefix match verwendet werden. Dazu müssen die Routing-Tabellen-Einträge in eine binäre Darstellung überführt werden (die Netzwerk-Bits sind hier unterstrichen dargestellt):

Zieleintrag (CIDR)	Binärdarstellung	Zu nehmender Router
139.179.200.0/21	10001011.10110011.11001000.00000000	R1
139.179.128.0/18	10001011.10110011.10000000.00000000	R2
139.179.112.0/20	10001011.10110011.01110000.00000000	R3
139.179.192.0/20	10001011.10110011.11000000.00000000	R4
139.179.0.0/16	10001011.10110011.00000000.00000000	R5

Die IP-Adressen werden ebenfalls in eine Binärdarstellung gewandelt:

(a) 139.179.60.10 → 10001011.10110011.00111100.00001010

(b) 139.179.210.40 → 10001011.10110011.11010010.00101000

(c) 139.179.197.55 → 10001011.10110011.11000101.00110111

(d) 139.179.205.180 → 10001011.10110011.11001101.10110100

Bei scharfem Hinschauen sieht man, dass die ersten 2 Bytes in allen Routing-Einträgen gleich sind und dass die Netzwerkbits immer mindestens 16 Bit lang sind. Daher kann man sich ganz auf das 3. (und ggf. 4) Byte in den Adressen konzentrieren.

(a) Die ersten 4 Einträge passen alle nicht → R5 wird genommen

(b) Die ersten 4 Einträge passen alle nicht → R5 wird genommen

(c) Der 4. Eintrag passt → R4 wird genommen

(d) Der 1. und der 4. Eintrag passen. Weil der Netzanteil des ersten Eintrags länger ist, wird dieser verwendet!

Übungsaufgabe 2:
Zunächst schreiben wir die Tabelle in Binärform (Netzwerk Bits sind unterstrichen):

Zieleintrag (CIDR)	Binärdarstellung	Next Hop
128.128.0.0/9	10000000.10000000.00000000.00000000	R1
128.160.0.0/11	10000000.10100000.00000000.00000000	R2
128.176.0.0/12	10000000.10110000.00000000.00000000	R1
128.192.0.0/10	10000000.11000000.00000000.00000000	R1
default		R3

Wir können nur Routing-Einträge zusammen fassen, die zu dem gleichen Ziel gehen! Eintrag 1 ist der allgemeinste Eintrag, und Einträge 4, 2 und 3 immer feinere Spezialisierungen des 1. Eintrages. Eintrag 4 ist eine Spezialisierung von Eintrag 1, und beide Einträge haben das gleiche Ziel. Da es keine weiteren Einträge gibt, die durch eine Zusammenlegung überschrieben würden, können diese Einträge zusammengefasst werden. Dazu kann der spezialisiertere Eintrag gelöscht werden, also:

128.128.0.0/9	R1
128.160.0.0/11	R2
128.176.0.0/12	R1
default	R3

Zusatzfrage: Eintrag 2 spezialisiert Eintrag 1 und leitet nach R2, wobei allerdings die weitere Spezialisierung im 3. Eintrag wieder nach R1 leitet. Diese Situation könnte man auch lösen, in dem man beim 2. Eintrag einen Präfix von 12 verwendet, und dadurch den 3. Eintrag überflüssig macht, weil nun Regel 1 die IPs, die vorher von Regel 3 erfasst wurden, auch nach R1 routet, also:

128.128.0.0/9	R1
128.160.0.0/12	R2
default	R3

Vorlesung 4 - Routingprotokolle und NAT

Erklären Sie den Unterschied zwischen Routing und Forwarding. Ordnen Sie den beiden Begriffen die Begriffe Control Plane und Data Plane zu.

- Das eigentliche Routing (die Control-Plane) ist verantwortlich für Wegewahl, mit der die Ende-zu-Ende-Kommunikation erreicht wird
- Das Weiterleiten (engl. forwarding) der Pakete (die Data-Plane) gemäß den Vorgaben der Control-Plane

Mit welchem Algorithmus kann ein optimaler Quelle-Senke Baum berechnet werden?
Mit dem Dijkstra Algorithmus

Welche 2 Arten von Routingverfahren kennen Sie, und welche Unterschiede existieren zwischen den Verfahren?

- Distanzvektoralgorithmen: ohne Kenntnis der gesamten Netztopologie
- Link-State Routing: mit Kenntnis der gesamten (zumindest im AS) vorhandenen Netztopologie

Erklären Sie den Bellmann-Ford Algorithmus mit eigenen Worten

- Definiere:
  - $c_x(v) :=$ Kosten zum Nachbarn v von x aus
  - $d_x(y) :=$ Kosten des günstigsten Weges von x nach y
- Gibt es einen Weg zwischen x und y und sind x und y nicht direkt verbunden, dann muss es einen Nachbarn v von x geben für den gilt:

  $$d_x(y) = \min\{c_x(v) + d_v(y)\}$$

  hierbei wird das Minimum über alle Nachbarn von x genommen. Die Kosten der direkten Verbindung wird als bekannt angenommen

Erklären Sie wie es zum sog. Count to Infinity-Problem kommen kann!

- Der Ausfall von Routen/Routern führt zum „Count-to-Infinity“ Problem:

  $$A - B - C$$

- Betrachte B: Router A fällt aus, bekommt aber von C gesagt, dass er einen Weg nach A kennt (der allerdings über B führt, was B nicht weiß ...) → Die Kosten zum Weg nach A schaukeln sich langsam auf ...

Wie funktioniert das Link-State Routing?

- Jeder Router führt die folgenden Schritte durch:
  1. Die Nachbarn und deren Netzadressen ermitteln
  2. Die Kosten zu jedem seiner Nachbarn festlegen
  3. Ein Paket zusammenstellen, in dem alles steht, was bisher gelernt wurde
  4. Dieses Paket an alle anderen Router senden und von allen anderen Routern derartige Pakete empfangen
  5. Den kürzesten Pfad zu allen anderen Routern berechnen
- Dadurch wird die gesamte Topologie in jedem Router abgebildet. Anwendung des Dijkstra-Algorithmus möglich!

Nennen Sie jeweils ein konkretes Routing-Protokoll, was das Distanzvektor-Verfahren bzw. das Link-State-Verfahren benutzt.

- RIP, RIP2: Intra-AS, Distance-Vector, veraltet
- IS-IS: Intra-AS, ursprünglich für DECnet, danach ISO Standard und Grundlage für OSPF, (Shortest Path First)
- OSPF: Intra-AS, Link-State, Unicast (Shortest Path First)
- BGP: Border Gateway Protokol Inter-AS, Distance-Vector

Warum werden Distanzvektor-Verfahren gerne zwischen autonomen Systemen eingesetzt?

- Leicht zu implementieren, einfache Berechnung
- Neue, bessere Routen werden im Netz schnell propagiert

Was sind "private" IP-Netze und -Adressen?

- Jeder Endkunde (jede kleinere Firma etc.) bekommt lediglich nur eine eindeutige öffentliche IPv4 Adresse vom ISP, d. h. es existiert auch nur ein Zugangspunkt (Gateway) zu diesem Netz
- Innerhalb des Hauses/der Firma wird ein “privates“ Netz betrieben, was die spezifizierten privaten IP-Adressblöcke benutzt:
  - 10.0.0.0 – 10.255.255.255
  - 172.16.0.0 – 172.31.255.255
  - 192.168.0.0 – 192.168.255.255

Wie werden solche Adressen im Zusammenhang mit NAT eingesetzt?
Der NAT-Router ersetzt die Source-IP (z. B. 10.0.0.3) mit der öffentlichen Adresse

Was passiert beim Verschicken eines IP-Paketes über einen NAT-Router?
Der NAT-Router ersetzt die Source-IP (z. B. 10.0.0.3) mit der öffentlichen Adresse

Was passiert anschließend beim Empfangen eines Antwortpaketes (von einem Server außerhalb des privaten Netzes)?
Der Server adressiert in seiner Antwort ein Ziel-Port, das der NAT-Router dann wieder in die interne IP und die interne Port-Nummer zurück übersetzt.

Warum verletzt das NAT-Verfahren die Schichtenarchitektur?
Layer 3 kennt Details des Layer 4, was eigentlich nicht sein darf.

Nennen Sie 2 Szenarien, wo der Einsatz von NAT zu Problemen führen würde. Begründen Sie jeweils ihre Antwort!

- Es wird nicht TCP/UDP verwendet
  - Begründung: Wenn TCP/UDP nicht verwendet wird, existiert ggf. das Konzept der Portnummern überhaupt nicht mehr. Diese Portnummern sind aber elementare Voraussetzung für die internen „Übersetzungen“ eines NAT-Routers.
- Übergeordnete Protokolle übertragen die IP als Payload (z. B. ftp)
  - Begründung: Wenn in den Payload-Daten eine IP übertragen wird, kann der NAT-Übersetzungsprozess nicht stattfinden. Ein Rechner in einem privaten Netz würde z. B. als Ziel IP 192.168.178.20 in die Payload-Daten kodieren, die auf Empfängerseite (bei einem entfernten Server) nicht verwendet werden kann (weil privat).
- Verschlüsselte Verbindungen werden genutzt
  - Begründung: Wenn der NAT-Router bereits verschlüsselte IP-Pakete erhält, kann er ggf. nicht mehr IP und Portnummer aus den Paketen lesen.

Was wird bei Port Restricted Cone NAT bei Antwortpaketen überprüft? Was muss sich der NAT-Router dazu merken?
Dieser Fall erweitert den restricted cone NAT in der Art, dass auch nur der entfernte Port mit dem internen Rechner kommunizieren kann. Der Router merkt sich Ziel-IP und Ziel-Port.

Vorlesung 5 - ARP, ICMP und IPv6

Welche unterschiedlichen Aufgaben und Eigenschaften hat eine IP- gegenüber einer MAC-Adresse?

- IP-Adresse: ‚Logische' Adressierung (Layer 3)
- MAC-Adresse: ‚Physikalische Adressierung' (Layer 2)

Wozu wird das ARP-Protokoll eingesetzt? In welchem 'Layer' wird dieses Protokoll implementiert?

ARP (Address Resolution Protocol) Layer-2 Protokoll:

- Ermöglicht das Herausfinden einer MAC-Adresse auf Basis einer versendeten IP-Adresse
- Funktioniert über Broadcast-Paket an MAC FF:FF:FF:FF:FF:FF
- Der Host mit der angefragten IP-Adresse antwortet mit seiner MAC-Adresse
- Der empfangende Knoten ‚cached' i. d. R. die MAC-Adressen

Wo befindet sich die ARP-Tabelle?

Das Address Resolution Protocol (ARP) arbeitet auf der Schicht 2, der Sicherungsschicht, des OSI-Schichtenmodells

Welche Vorteile hat das DHCP-Protokoll gegenüber dem älteren RARP-Protokoll?

- Probleme von RARP
  - Ethernet-Broadcasts sind auf Subnetze beschränkt. In einem LAN mit Subnetzen braucht man mehrere RARP-Server.
  - Durch RARP erfährt ein Rechner nur seine IP-Adresse! Zu einer vollständigen Konfiguration einer Netzwerkschnittstelle gehören noch mindestens Netzmaske und Default-Gateway.
  - DHCP hat RARP heute komplett abgelöst!
- DHCP (Dynamic Host Configuration Protokoll)
  - Basiert auf dem älteren BOOTP-Protokoll und ist zu diesem (eingeschränkt) kompatibel
  - Realisiert als Application Protokoll über UDP Port 67
  - Ermöglicht die Konfiguration über Subsystemgrenzen (DHCP Relay Agents) und mit Szenarien mit mehreren DHCP-Servern
  - Erlaubt das Konfigurieren aller wichtigen Parameter (IP/Mask/default Gateway/DNS Server)
  - Erlaubt das zeitlich u. A. beschränkte Vergeben von IPKonfigurationen (leases) und das Steuern der Vergabe
  - Sicherheitsprobleme: MAC-Spoofing, DHCP Starvation etc.

Erklären Sie die Funktion der Felder "Time to live" und "Fragment offset" im IPv4 Header!

- **TTL (Time-to-Live):** Mit TTL gibt der Sender die Lebensdauer des Pakets in Sekunden an. Jede Station, die ein IP-Paket weiterleiten muss, zieht von diesem Wert mindestens 1 ab. Hat der TTL-Wert 0 erreicht, wird das IP-Paket verworfen. Dieser Mechanismus verhindert, dass Pakete ewig Leben, wenn sie nicht zustellbar sind. TTL-Werte zwischen 30 und 64 sind typisch.
- **Fragment-Offset:** Enthält ein IP-Paket fragmentierte Nutzdaten, steht in diesem Feld die Position der Daten im ursprünglichen IP-Paket.

Warum werden IP-Pakete auf Ihrem Weg ggf. fragmentiert? Welche Rolle spielt dabei die MTU?

- IP-Pakete sind gegebenenfalls zu groß und werden daher fragmentiert.
- Die MTU (Maximum Transfer Unit) beschreibt die maximale Größe und liegt auf Layer 2.

Wie funktioniert das Verfahren der "Path MTU Discovery"?

- Das Quell-System schickt die Pakete mit der Flagge DF (don't fragment)
- Wenn ein Router eine zu kleine MTU erkennt, wird das Paket verworfen und eine ICMP-Nachricht zurück gesendet
- Das Quell-System kann jetzt kleinere Pakete erzeugen, die weiter geleitet werden können
- Der Prozess muss ggf. mehrmals wiederholt werden!

Welche Aufgaben hat das ICMP-Protokoll?

- Das Internet Control Message Protocol ist ein Steuerprotokoll der Schicht 3, welches auf IP aufbaut! Dieses Protokoll wird z. B. von Routern verwendet, wenn etwas Unerwartetes passiert.
- Aufgaben:
  - Mitteilung von Problemen beim Paketversand
  - Echo-Anfragen (existiert der Zielknoten?)
  - Unterstützung von höheren Protokollen und Anwendungen (z. B. Path MTU discovery, traceroute, ...)

Wie lang (in Bytes) ist eine IPv6-Adresse? Nennen Sie 4 Vorteile von IPv6 gegenüber IPv4!

- 128-Bit-Adressen (8 Gruppen zu je 4 Hexadezimal-Zahlen)
- Vorteile von IPv6 gegenüber IPv4:
  - längere Adressen und dadurch ein größerer Adressraum

– mehrere IPv6-Adressen pro Host mit unterschiedlichen Gültigkeitsbereichen
– Multicast durch spezielle Adressen
– schnelleres Routing

Vorlesung 5 - Beispielaufgaben

Übungsaufgabe 1:

Rechner **A** sei über einen Router **R** mit Rechner **B** verbunden. Für die Strecke von **A** zum Router gelte **MTU=2000**, für die Strecke vom Router **R** zu Rechner **B** sei die **MTU 1500**: Es soll ein Datenpaket der Länge **3600** Byte übertragen werden (ohne IP-Header!). Skizzieren Sie den Prozess der Fragmentierung, indem sie die folgenden Tabellen ausfüllen:

A → MTU 2000 → R

ID	MF	Total Length	Offset

R → MTU 1500 → B

ID	MF	Total Length	Offset

Vorlesung 5 - Lösungen

Übungsaufgabe 1:

Die IDs können frei gewählt werden, müssen sich nur unterscheiden:

A → MTU 2000 → R

ID	MF	Total Length	Offset
1	**1**	**1996**	**0**
2	**0**	**1644**	**247**

R → MTU 1500 → B

ID	MF	Total Length	Offset
11	**1**	**1500**	**0**
12	**1**	**516**	**185**
21	**1**	**1500**	**247**
22	**0**	**164**	**432**

Auf der ersten Strecke (A → R) wird das Paket in zwei Unterpakete mit einer Payload-Größe von 1976 + 1624 = 3600 Bytes zerlegt. 1976 muss dabei durch 8 teilbar sein! Auf der zweiten Strecke (R → B) werden diese zwei Pakete dann in Pakete mit Payload-Größe 1480 + 496 + 1480 + 144 = 3600 Bytes zerlegt. 1480 muss dabei durch 8 teilbar sein! Das letzte Paket muss das MF-Bit (**M**ore **F**ragments) auf 0 setzen!

Vorlesung 6 - Send and Wait, Sliding Window

Nennen Sie die 2 wichtige Transportprotokolle im Internet! Wie unterscheiden sie sich?

- Transmission Control Protocol (TCP) → zuverlässig
  - Kommunikationsprimitive, Sockets, Ports
  - Virtuelle Verbindungsorientierung: Modell zweier Streams die die Prozesse miteinander verbinden; 'Open'-'Close' der Streams sind die virtuellen Verbindungen
  - Flusskontrolle, Staukontrolle
- User Datagram Protocol (UDP) → unzuverlässig
  - Kommunikationsprimitive, Sockets, Ports
  - Postkartenmodell: Ein Empfangspunkt (Port) für alle Nachrichten, versenden ohne Absprache mit dem Empfänger

Was bedeutet eine 'virtuelle Verbindungsorientierung'?
Modell zweier Streams die die Prozesse miteinander verbinden; 'Open'-'Close' der Streams sind die virtuellen Verbindungen

Erklären Sie das ARQ-Protokoll und die Randbedingungen, unter denen dieses Protokoll eine sichere Datenübertragung gewährleistet! Wo und warum werden hier Timeouts eingesetzt?

- Segmentweises Vorgehen
- Timer zur Fehleridentifikation
  - Verschicke ein Segment und warte auf den Empfang des ACKs
  - Bei Empfang eines ACKs wird das nächste Segment verschickt, andernfalls wird die Übertragung wiederholt
  - Jeder Datenstrom wird in Segmente unterteilt, z. B. 1460 Bytes Nutzdaten
  - Nach jedem gesendeten Segment wird auf eine Bestätigung gewartet; während der Wartezeit werden keine weiteren Segmente übertragen

Wie ist der Nutzungsgrad einer Verbindung definiert? Warum gibt es bei Verbindungen mit hoher RTT hier Probleme?

- Nutzungsgrad: Verhältnis von genutzter Übertragungszeit zu gesamter Übertragungsdauer (inkl. der Wartezeit)
- $$\rho = \frac{\text{genutzte Übertragungszeit}}{\text{genutzte Übertragungszeit} + \text{Wartezeit}}$$

Was bedeutet 'Pipelining' im Kontext der Datenübertragung? Was bedeutet in diesem Zusammenhang 'Fensterbreite'? Welche Schwierigkeiten entstehen bei Fehlerfällen?

- Pipelining:
  - Senden ohne vorheriges ACK
  - Fensterbreite beim Sender: Anzahl der Segmente, die ohne Bestätigung gesendet werden
  - Fensterbreite beim Empfänger: Anzahl der Segmente, die auch bei Lücken oder Fehlern zwischengespeichert werden
- Probleme beim Empfänger:
  - Empfang eines out-of-order-Segments
    - Eigentlich wurde ein anderes Segment erwartet
    - Je nach Implementierung wird das nicht erwartete Segment einfach ignoriert, es wird dann verworfen
  - Empfang eines fehlerbehafteten Segments
    - Keine Reaktion (Der Sender wird irgendwann eine erneute Übertragung vornehmen, da ja keine Bestätigung verschickt wurde)
    - Falls unterstützt: Verschicken einer „negativen“ Bestätigung oder einer Nachricht, die dies kommuniziert (als Indiz für einen möglichen Paketverlust)
  - Probleme beim Sender:
    - Timeout → Worauf bezieht sich dieser?
    - Empfang einer nicht erwarteten Bestätigung (out-of-order) ACKs
    - Empfang einer negativen Bestätigung (falls es die gibt)

Wie löst das Go-Back-N Verfahren Übertragungsfehler?

- Der Empfänger sendet nach dem Fehler kein ACK mehr
- Der Sender läuft dadurch in ein Timeout und fängt wieder ein Segment nach dem letzten bestätigten Segment an
- Alle direkt nach dem Fehler versendeten Segmente werden verworfen

Wie groß ist die Fensterbreite beim Sender und Empfänger bei 'Go-Back-N'?

- Fensterbreite Sender: > 1
- Fensterbreite Empfänger: 1

Warum sollten sich bei 'Sliding-Window' Verfahren Sender und Empfänger bzgl. ihrer Fensterbreiten koordinieren?

Weil sonst nicht die volle Bandbreite der Verbindung genutzt wird, oder auf Empfängerseite Pakete verworfen werden müssen (s. u.).

Was passiert, wenn das Sendefenster größer als das Empfangsfenster ist?
Wenn das Sendefenster größer ist als das Empfangsfenster, muss der Empfänger Pakete verwerfen, die später erneut gesendet werden müssen.

Was passiert, wenn das Empfangsfenster größer als das Sendefenster ist?
Wenn das Sendefenster kleiner als das Empfangsfenster ist, wird nicht die maximal mögliche Bandbreite der Übertragung genutzt, d. h. der Empfänger könnte noch mehr Pakete zwischenspeichern, die der Sender aber nicht sendet.

Was passiert, wenn beide Fensterbreiten 1 sind?
Dann haben wir einen Rückfall auf das Stop-and-Wait-Verfahren, also im Extremfall ein Byte senden, auf Quittung warten (dauert die Hin- und Rücksendezeit), nächstes Byte schicken u.s.w.

Warum sind große Fensterbreiten häufig schwer zu realisieren?
Große Fensterbreiten setzten große Puffer im TCP/IP Stack voraus. Außerdem kann TCP standardmäßig nur max. 64 kB Fenstergröße realisieren. Daher wird häufig die sog. Window-Scale-Option von TCP verwendet.

Wie kann der Empfänger eine 'Flusskontrolle' bei der Datenübertragung realisieren?
Wenn z. B. die Daten auf der Empfängerseite von der Anwendungsschicht nicht abgeholt werden, teilt der Empfänger irgendwann eine Fenstergröße von 0 mit, wodurch der Sender aufhört zu senden. Dadurch kann eine Flusskontrolle realisiert werden.

Leiten Sie die Berechnung der benötigten Fensterbreite aus dem 'Bandwidth-Delay'-Produkt her!

$$\rho = \#seg \cdot \frac{\frac{L}{R}}{\frac{L}{R} + RTT}$$

$$R\rho = \#seg \cdot \frac{L}{\frac{L}{R} + RTT}$$

$$R\rho = erzielbare\ Bandbreite = B$$

$$\#seg \cdot L = Fensterbreite\ in\ bit = W$$

$$Es\ gilt\ \frac{L}{R} \ll RTT\ (siehe\ vorherige\ Beispiele)$$

$$B \leq \frac{W}{RTT}\ bzw.\ W \geq B \cdot RTT$$

Wie funktioniert das 'Selective Repeat' - Verfahren? Werden hier auf Empfängerseite Segmente verworfen im Fehlerfall?

- Mittelbare Kenntnis über etwaig bereits empfangene Segmente, Empfänger puffert nicht erwartete Segmente, sodass sich bei Neuübertragung der „Lücke“ das Fenster ruckartig verschiebt
- Sender und Empfänger haben eine Fensterbreite > 1. Wenn ein Paket beim Empfänger nicht ankommt, sendet der Empfänger ab dann keine ACKs mehr, wodurch

der Sender irgendwann in den Re-Transmission-Timeout läuft. Der Sender wiederholt dann das Versenden des fehlenden Paketes und aller folgenden Pakete (obwohl die ggf. schon vorher fehlerfrei beim Empfänger angekommen waren). Das Empfänger-Fenster kann nach Empfang des fehlenden Paketes einen 'Sprung' machen.

- Ja, es werden im Fehlerfall auf Empfängerseite Pakete verworfen (die oben erwähnten, doppelt gesendeten Pakete ...)

Wie funktioniert das 'Selective Reject' - Verfahren? Werden hier auf Empfängerseite Segmente verworfen im Fehlerfall?

- Unmittelbare Kenntnis über unerwartete Ereignisse und sofortige Reaktion zur Behebung
- Grundsätzlich so wie Selective Repeat, nur dass der Empfänger nicht aufhört ACKs zu senden, sondern nach jedem weiteren Paket immer der gleiche ACK n (n ist entsprechende Sequenznummer) gesendet wird. Wenn der Sender dann z. B. 3-mal den gleichen ACK n empfängt, wird das auf Senderseite als NACK interpretiert,und das Packet n noch einmal gesendet. Dadurch kann der Sender früher auf den Fehler reagieren, und muss i. d. R. weniger oder keine Pakete zweimal senden wie beim Selective Repeat. Daher: Nein, in der Regel werden auf Empfängerseite keine Pakete verworfen (siehe Folie KS_11 Seite 16).

Was bedeutet eine kumulative Bestätigung?

- Eine Bestätigung zeigt an, dass alle Daten bis zu der verwendeten Nummer/Byte Position korrekt empfangen wurden
- Kommt ein Out-of-Order-Segment an, so wird demnach eine Bestätigung verschickt, die schon einmal verschickt wurde ("ich warte immer noch auf x")
- Speichert der Empfänger außerhalb der Reihenfolge empfangene Segmente zwischen, dann bedeutet ein „Lückenschluss", dass dieser einen „Sprung" bei den Bestätigungen bedingt

Wie können mehrfache ACKs auch als NACK gewertet werden?

- Kommt ein Out-of-Order-Segment an, so wird demnach eine Bestätigung verschickt, die schon einmal verschickt wurde ("ich warte immer noch auf x")
- Wenn ein Segment verloren gegangen ist, dann werden alle weiteren empfangenen Segmente die gleiche Position anzeigen
- Duplicate Acknowledgments: Empfang einer Bestätigung, die eine schon versendetes Feeback erneut gibt: ("ich warte immer noch auf x")
- Segmente können sich überholen, deshalb ist das nicht sofort als NACK aufzufassen
- Aber: Triple Duplicate Acknowledgement wird als NACK aufgefasst!

Vorlesung 6 - Beispielaufgaben

Beispiel: FastEthernet im LAN:

$$R = 100\frac{Mbit}{s},\ L = 1460\ Byte,\ \frac{L}{R} = 116.8\mu s,\ RTT = 3ms$$

$$\rho = \frac{\frac{L}{R}}{\frac{L}{R} + RTT} = 0.03747 = 3.74\%$$

Beispiel: Kommunikation mit Kalifornien:

$$R = 100\frac{Mbit}{s},\ L = 1460\ Byte,\ \frac{L}{R} = 116.8\mu s,\ RTT = 200ms$$

$$\rho = \frac{\frac{L}{R}}{\frac{L}{R} + RTT} = 0.05837\%$$

Übungsaufgabe 1:
Wir streben eine Kommunikation mit einer Mondstation an und möchten eine TCP-Anwendung unterstützen, die eine Datenrate von 100Mbit/s erzielen soll. Die Round-Trip-Zeit sei 2,4 Sekunden.

Wir groß (in Bytes) sollte das Übertragungsfenster (Sliding Window) mindestens sein, um diese Rate überhaupt erzielen zu können? Welche Rate könnte maximal erreicht werden, wenn die Größe des Übertragungsfensters 64KByte wäre (65536 Byte)?

Vorlesung 6 - Lösungen

Übungsaufgabe 1:
Die minimale Fenstergröße ergibt sich aus dem Bandwidth-Delay-Produkt:

$$W \geq B * RTT$$
$$W \geq 100\frac{Mbit}{s} * 2,4s = 240Mbit = 30MByte$$

Antwort: Die minimale Fenstergröße auf Sender- und Empfängerseite müsste mindestens 30MB betragen. Bei W = 65536 Byte gilt:

$$B \leq \frac{W}{RTT} = \frac{65536 * 8Bit}{2,4s} = 218,45\frac{kbit}{s}$$

Antwort: Bei einer Fenstergröße von 65536 Byte wäre die maximale Übertragungsrate $218,45\frac{kbit}{s}$

Vorlesung 7 - TCP

Wie identifiziert TCP ein Segment bzw. ein ACK? In welcher Einheit wird 'gemessen'?

- Segmente werden durch ihren Byte-Offset im Stream identifiziert (Sequence Number), wobei die Startposition beim Verbindungsaufbau zufällig festgelegt wird. Der Offset selbst ist dabei ein 32-Bit Integer.
- TCP verwendet kumulative ACKs: ACK $n+1$ sagt aus, dass alle Daten von der vorigen logischen Position bis zur Position n korrekt empfangen wurden und nun das Segment $n+1$ erwartet wird

Wird bei jedem TCP-Paket ein ACK mitgesendet?
Nein, aber:

- Nach 500ms **muss** ein ACK gesendet werden
- Nach zwei vollständigen Segmenten **sollte** ein ACK gesendet werden

Warum muss der Empfänger seine aktuelle Fenstergröße ('advertised window') dem Sender mitteilen? Wie?

- Um den Puffer berechnen zu können
  - Bedingungen für den Sender:

$$\begin{aligned} \text{LastByteAcked} &\leq \text{LastByteSent} \\ \text{LastByteSent} &\leq \text{LastByteWritten} \end{aligned}$$

    Zwischenspeichern der Daten zwischen **LastByteAcked** und **LastByteWritten**

$$\text{LastByteSent} - \text{LastByteAcked} < \text{AdvertisedWindow}$$

    EffectiveWindow = AdvertisedWindow - (LastByteSent - LastByteAcked)
  - Bedingungen für den Empfänger:

$$\begin{aligned} \text{LastByteAcked} &< \text{NextByteExpected} \\ \text{NextByteExpected} &\leq \text{LastByteRcvd} + 1 \end{aligned}$$

    Zwischenspeichern der Daten zwischen **LastByteRead** und **LastByteRcvd**
    AdvertisedWindow = Empfangspuffer – ((NextByteExpected - 1) - LastByteRead)
- über den TCP-Header und damit die Window Scale Option

Erklären Sie auf Empfängerseite den Unterschied zwischen Empfangspuffer-Größe und aktueller Fenster-Größe!

- Die Empfangspuffer-Größe ist die Gesamtgröße des zur Verfügung stehenden Puffers auf Empfangsseite, unabhängig von dessen Füllungsgrad.
- Die aktuelle Fenstergröße gibt den freien Speicher in diesem Puffer an. Dieser Wert kann z. B. auf 0 abfallen, falls die Applikation auf Empfängerseite die Daten nicht abholt.

Unter welchen Bedingungen wird in TCP ein ACK versendet?
Liegen keine Daten an, werden Acks verzögert – irgendwann aber doch verschickt

- Annahme: Es kommen viele Segmente hintereinander
- Delayed Acknowledgments
- Nach 500ms **muss** ein ACK gesendet werden
- Nach zwei vollständigen Segmenten **sollte** ein ACK gesendet werden

Welche Strategien zur Fehlerbehebung verwendet TCP? (Go-Back-N? Selective Repeat? Selective Reject?)

- TCP verwendet heute i. d. R. Selective Reject, in dem 3 gleiche ACKs als NACK interpretiert werden.
- **Go-Back-N/Selective Repeat Protokoll:** TCP-Sender verwaltet lediglich einen Timer für das Segment, welches als nächstes bestätigt werden muss. Kommt es zu einem Time-Out, so wird, bedingt durch das Zwischenspeichern auf Empfängerseite, hier zu einem **Selective Repeat** durchgeführt.
- **Selective Reject:** Empfänger speichert nicht nur out-of-Order Segmente im Empfangspuffer. Die meisten Versionen von TCP **emulieren** NAK-Mechanismen mittels dreifachem ACK mit gleicher Sequenznummer

Wozu dient der Retransmission Timer? Wie wird seine Länge bestimmt?
Timer wird beim Senden eines Segmentes (auf Senderseite) gestartet.

- Bei Ablauf: Erneutes Versenden des Segmentes.
- Bei Empfang eines ACKs: Rücksetzen des Timers, bzw. Neustart mit beim Versenden des nächsten Segmentes.

Was ist ein 'Congestion Collapse'? Wie wird er hervorgerufen?
Verstärkung der Überlastsituation durch unnütze Übertragung. Durch viele Verbindungen können Router überlastet werden.

- Überlast/Verstopfung: engl.: Congestion
- Pakete werden verworfen, auf TCP-Ebene gehen keine Quittungen ein
- TCP wiederholt die Daten und belastet das Netz damit noch stärker

Welche Einflussgrößen steuern die Bandbreite des Senders bei TCP?
Neben der von Empfänger mitgeteilten Empfangsfenstergröße wird das Sendefenster auch vom sog. congestion-window gesteuert (siehe KS12, Seite 19). Das Minimum dieser beiden Fenstergrößen wird verwendet. Über das congestion-Window wird z. B. der slow-start realisiert und das Verhalten bei Paketverlusten durch z. B. Router-Überlastung.

Was versteht man bei TCP unter 'Slow Start'?
Congestion Window bestimmt insbesondere zu Beginn die Übertragungsrate (Slow Start)

Erklären Sie die unterschiedlichen Strategien zur Kontrolle der genutzten Bandbreite bei TCP Reno!

- Vorsichtiger Beginn (Slow-Start), aber nur bis zu einem Schwellwert
- Unterscheidung zwischen Time-Out und duplicate ACKs:
  - Bei Time-Out gleiches Verhalten wie TCP Thaoe
  - Bei dup-ACKs (selective Reject) → Halbierung des Congestion Window (fast recovery)

Wie funktioniert der Verbindungsaufbau bei TCP? Welcher Begriff wird zur Beschreibung des Verfahrens verwendet?
Three-Way-Handshake:

1. Der Server wartet auf eingehende Verbindungswünsche
2. Der Client führt unter Angabe von IP-Adresse, Portnummer und maximal akzeptabler Segment-Größe eine CONNECT-Operation aus
3. CONNECT sendet ein SYN
4. Ist der Destination Port der CONNECT Anfrage identisch zu der Portnummer, auf der der Server wartet, wird die Verbindung akzeptiert, andernfalls mit RST abgelehnt
5. Der Server schickt seinerseits das SYN zum Client und bestätigt zugleich den Erhalt des ersten SYN-Segments
6. Der Client schickt eine Bestätigung des SYNSegments des Servers. Damit ist die Verbindung aufgebaut

Wozu dient der Keepalive-Timer? Wann ist dieser Timer wichtig?
Relativ lange Wartezeit. Wird bei jeder Transaktion rückgesetzt. Nach Ablauf → Abbau der Verbindung

Welche Datenfelder enthält der TCP-Header? Wozu werden sie jeweils verwendet?

- Source Port: Identifiziert die Anwendung auf der Senderseite.
- Destination Port: Identifiziert die Anwendung auf der Empfängerseite.

- Sequence Number: TCP betrachtet die zu übertragenden Daten als nummerierten Byte-Strom. Die Sequence Number ist die Nummer des ersten im Segment enthaltenen Datenbytes.
- Acknowledgement Number: Dieses Feld bezieht sich auf einen Datenfluss in Gegenrichtung, d. h. hiermit werden Daten bestätigt, die die Station, die das Segment absendet, zuvor von der Zielstation empfangen hat.
- Data Offset: Da der Segment-Header Optionen enthalten kann, ist seine Länge nicht fix. Im Data Offset-Feld wird die Länge (d. h. der Beginn des Datenteils) in 32-Bit-Einheiten angegeben.
- Res.: Reserviert für zukünftige Nutzung.
- Code: Die Bits des Code-Feldes steuern besondere Funktionen des Segments.
  - URG: Urgent Pointer Field is valid
  - PSH: This segment requests a push
  - SYN: Synchronize sequence numbers
  - ACK: Acknowledgement Field is valid
  - RST: Reset the Connection
  - FIN: Sender has reached end of his byte stream
- Window: Spezifiziert die Anzahl der Datenbytes (beginnend mit der im Acknowledgement - Feld angegebenen Byte-Nummer), die der Sender des Segments als Empfänger eines Datenstromes in Gegenrichtung akzeptieren wird.
- Checksum: 16-Bit Längsparität über das gesamte Segment (Header + Daten).
- Urgent Pointer: Damit können Teile des zu übertragenden Byte-Stroms als dringend markiert werden.

Wozu dient der Persistence-Timer in TCP? Was passiert nach seinem Ablauf?
Timer wird nach Empfang einer Fenstergröße von 0 gestartet. Nach Ablauf Anfrage nach neuem Fenster (>0)

Wie funktioniert die (häufig eingesetzte) Window-Scale Option in TCP? Wann wird sie benötigt?

- Einführen einer Window-Scale-Erweiterung die ein Skalierungsfaktor für das 16-Bit Window-Feld darstellt
- Der Skalierungsfaktor wird als neue TCP-Option eingeführt: Window Scale ist 3 Byte lang – das letzte Byte gibt die Skalierung LOGARITHMISCH an (shift count: Das Fenster wird shift count bits nach links veschieben – hierbei ist der maximale Wert 14!)

- Die Option wird nur in einem SYN-Segment beim Verbindungsaufbau übertragen. Danach wird der Wert für die ganze Verbindung angenommen
- Beide Seiten müssen eine Window-Scale-Option verschicken Null bedeutet „keine Skalierung“
- Die neue maximale Fenstergröße in Bytes errechnet sich wie folgt:

$$65536 * 214 = 65535 * 16384 = 1.073.725.440$$

- TCP-intern wird die Fenstergröße jetzt als 32-Bit-Zahl verwaltet

Was versteht man unter dem 'Silly Window'-Syndrom? Wie kann es gelöst werden?

- Empfangsfenster ist „voll“, die empfangende Applikation liest die Zeichen aber nur einzeln aus
- → Sender würde für jedes einzelne Zeichen ein neues Paket senden
- Lösung (Clark): Empfänger darf neue Fenstergröße erst erneut senden, wenn in seinem Buffer mehr Platz ist (z. B. ein Segment)

Wozu dienen die PSH und URG-Flaggen im TCP Header?

- Problem: Sender will wichtige Daten ohne Pufferung an die empfangende Applikation weitergeben
- Lösung: PSH: Flagge im TCP Header: Daten auf Empfängerseite direkt zustellen (kein Puffern)
- Alternative: URG: Flagge im TCP Header: „Event“ auf Empfängerseite auslösen

Vorlesung 7 - Beispielaufgaben

Übungsaufgabe 1:
Beim TCP Verbindungsaufbau wird der 3-way-handshake benutzt.

1. Warum wird nicht ein 'einfacher' Handshake, also nur 2 Nachrichten, verwendet?
2. Wissen beiden Seiten nach der 3. Nachricht sicher, dass die Verbindung aufgebaut ist?
3. Warum ist der 3-way-handshake bei TCP trotzdem sicher?

Übungsaufgabe 2:
1. Erklären Sie das Silly-Window-Syndrom!
2. Was passiert, wenn eine bestehende TCP-Verbindung über Stunden nicht genutzt wird? Was passiert, wenn einer der beiden verbundenen Rechner abstürzt?

Übungsaufgabe 3:
Woher kennt TCP die Größe der übermittelten Nutzdaten (bzw. wie 'lang' ein übertragenes Segment ist) ?

Übungsaufgabe 4:
Sie möchten mit der West-Küste der USA eine TCP-basierte Kommunikation durchführen. Damit Ihre Anwendung vernünftig funktioniert benötigen Sie eine Bandbreite von mindestens 40 $\frac{Mbit}{s}$. Die Round-Trip-Zeit sei 100ms.

Was benötigen Sie im TCP-Protokoll, um dieses Ziel zu erreichen? Wie genau würde dies ablaufen?

Vorlesung 7 - Lösungen

Übungsaufgabe 1:

1. Es wird kein einfacher Handshake verwendet, weil dann nicht jede Nachricht mit Verbindungswunsch (SYN Pakete) quittiert wurde. Nach der 3. Nachricht ist jede der beiden SYN-Nachrichten quittiert worden!

2. Nein, nach der 3. Nachricht weiß der Initiator des Verbindungsaufbaus nicht, ob die 3. Nachricht nicht verloren gegangen ist (Stichwort: 2 army problem). Man geht aber davon aus, dass die 3. Nachricht genauso wie die 1. Nachricht (gleiche Richtung) erfolgreich zugestellt wurde.

3. Durch die bei TCP folgende Datenübertragung wird der Verbindungsaufbau indirekt mit bestätigt. Mit dem Verbindungsaufbau wird eine 'Bestätigungskette' über die ACKs aufgebaut, die am Anfang der Datenübertragung auch den Verbindungsaufbau bestätigt, also die 4. Nachricht die 3. Nachricht bestätigt, u. s. w.

Übungsaufgabe 2:

1. Das Silly-Window-Syndrom besteht, wenn TCP-Segmente/Pakete mit einer sehr geringen ('silly') Anzahl an Nutzdaten (z. B. nur einem Byte) gesendet werden. Man kann das Problem beheben, wenn man erst auf mehr Daten wartet, und dann ein größeres Datenpaket schickt. Manchmal muss man das Versenden der Daten erzwingen (Stichwort 'flush').

2. Durch den Keepalive-Mechanismus bleibt die Verbindung im Normalfall bestehen. Nach einer definierten Zeit würden Keep-Alive-Nachrichten ausgetauscht, die sicherstellen, dass die andere Seite noch 'lebt'. Wenn eine der beiden Seiten abstürzen würde, würde das die Gegenseite durch fehlende Quittierungen der Keep-Alive-Nachrichten mitbekommen, und die Verbindung abbauen.

Übungsaufgabe 3:

Im TCP-Header existiert kein Feld zur Längenangabe der übermittelten Nutzdaten. TCP muss hierzu auf das 'Total Length' Feld im IP Header zurückgreifen, und die Größe des IP- und TCP-Headers (ggf. mit Optionen) abziehen. Daraus ergibt sich dann die Größe der übermittelten Nutzdaten.

Übungsaufgabe 4:

Das erforderliche Sendefenster ergibt sich aus dem Bandwidth-Delay Produkt:

$$40.000.000 \ \frac{Bit}{s} * 0,1s = 4.000.000 \ Bit = 500.000 \ Byte$$

Diese Fenstergröße kann im Original-TCP Header nicht abgebildet werden (maximal 64 kB). Daher muss die Window-Scale Option eingesetzt werden. Damit die erforderliche Fensterbreite verwendet werden kann, muss der ursprüngliche Maximalwert (64 kB) mindestens mit Faktor 8 multipliziert werden (524288 Bytes). D. h. im 3. Byte der Window-Scale Option muss mindestens eine 3 stehen (2^3 = Faktor 8). Dadurch können

nun allerdings Fenstergrößen nur noch in Vielfachen von 8 Byte kommuniziert werden! Beim Verbindungsaufbau muss bei beiden SYN-Nachrichten die Window-Scale Option entsprechend mitgesendet werden, damit ein Voll-Duplex Betrieb mit 40 $\frac{MBit}{s}$ möglich ist. Eine nachträgliche Änderung der Fenster-Skalierung ist nach erfolgtem Verbindungsaufbau nicht mehr möglich!

Vorlesung 8 - UDP und DNS

Warum hat UDP neben TCP eine Daseinsberechtigung? Wann kann dieses Protokoll sinnvoll eingesetzt werden? Nennen Sie Beispiele für den konkreten Einsatz!

- UDP stellt eine „direkte“ Schnittstelle zur Nutzung von IP dar: Anwendungen können Nachrichten direkt verschicken, ohne Verbindungsaufbau
- Unzuverlässig, verbindungslos
- einfacher und schneller als TCP
- Optionale Prüfsumme
- Sehr viele Multimedia-Anwendungen verwenden UDP, da dort keine zuverlässige Verbindung benötigt wird

Einsatzgebiete:

- Multimedia: Die digitale Übertragung von Audio- und Videodaten besitzt spezifische Anforderungen:
  - Geringe Verlustraten stören nicht
  - Isochrones Abspielen → schwierig mit TCP ...
  - Latenzzeiten müssen insbesondere bei interaktiven Anwendungen gering sein (Telefonie erfordern eine maximale Latenz von 150ms)
  - Jitter: Die Variation der Laufzeit sollte ebenso beschränkt sein
- RFC: Remote Procedure Calls
- NFS: Network File System
- RTP: Real-Time Transport Protocol
- DNS: Domain Name System

Welche Felder enthält der UDP-Header?

- Source Port: Identifiziert den sendenden Prozess, also den Prozess, an den gegebenenfalls Rückmeldungen zu senden sind. Die Angabe ist optional; das Feld soll den Wert null haben, wenn die Option nicht genutzt wird.
- Destination Port: Identifiziert den Prozess im Zielsystem, an den die Daten abzuliefern sind.
- Length: Gibt die Gesamtlänge des UDP-Datagramms in Bytes an; die Mindestlänge beträgt somit 8 (= Header-Länge)

- Checksum: Die Angabe ist optional (0 bedeutet: keine Angabe). Für die Berechnung der Längsparität wird dem UDP-Datagramm ein (nicht mitübertragener) Pseudo-Header von 12 Bytes Länge vorangestellt, der im wesentlichen IP-Source Address, IP-Destination Address und die im IP-Datagramm angegebene Protokoll-Nr. für UDP (17) enthält. Da der Datenteil eines IP-Datagramms nicht durch die IP Header Checksum geschützt ist, bedeutet ein Verzicht auf die UDP-Checksum, dass der Inhalt des UDP-Datagramms (Header und Daten) nicht durch eine Prüfsumme gesichert ist.

Welche Schritte sind notwendig, um ein analoges Signal in ein digitales zu wandeln?

- Abtasten
- Halten
- Quantisieren
- Kodieren

Was besagt das Nyquist-Theorem?
Sampling-Frequenz $\geq 2\cdot$ maximale Frequenz des Signals

Nennen Sie unterschiedliche Kategorien von Multimedia-Anwendungen!

- Streaming gespeicherter Audio- und Videodaten
- Streaming von live Audio und Video
- Interaktive Audio und Video Nutzung

Warum ist beim Streaming von Live-Daten immer eine Pufferung auf Empfängerseite notwendig?
Wegen der Unterschiede in der Netzwerk- und der Wiedergabe-Latenz

Welches Anwendungsprotokoll unterstützt die Versendung von Echtzeitdaten über UDP?
Das RTP-Protokoll

Wozu dient das Domain Name System (DNS) hauptsächlich?
DNS handhabt die Abbildung von Rechnernamen auf Adressen (und weitere Dienste).

Wie ist ein lesbarer Domänen-Namen aufgebaut? Welche Beschränkungen existieren?

- der Name einer Domäne besteht aus der Folge von Labeln (getrennt durch ”.”) beginnend beim ‚Blatt‘ der Domäne und aufsteigend bis zur Wurzel des Gesamtbaums
- In den Blattknoten sind die IP-Adressen der durch die Labelsequenz gegebenen Namen gespeichert
- Eine Darstellung de.fh-aachen.agnm05.www wäre logischer, aber weniger lesbar
- Daher: Auflösung des Namens von hinten!

Was ist eine sog. Top-Level Domäne? Welche Kategorien existieren hier?
Ein direktes Blatt des DNS. Kategorien:

Domain	Intended use	Start Date	Restricted?
com	Commercial	1985	No
edu	Educational institutions	1985	Yes
gov	Government	1985	Yes
int	International organizations	1988	Yes
mil	Military	1985	Yes
net	Network providers	1985	No
org	Non-profit organizations	1985	No
aero	Air transport	2001	Yes
biz	Business	2001	No
coop	Cooperatives	2001	Yes
info	Informational	2002	No
museum	Museums	2002	Yes
name	People	2002	No
pro	Professionals	2002	Yes
cat	Catalan	2005	Yes

Welche Möglichkeiten hat der Resolver auf einem Rechner, einen Domänen-Namen aufzulösen?

- Rekursive Anfragen: Server schickt Anfrage zum nächsten Server weiter (oder Fehlermeldung). → Client-Server-Anfragen
- Iterative Anfragen: Server antwortet dem Fragenden direkt mit IP-Adresse des nächsten Servers. → Server-Server-Anfragen

Woher kennt ein Rechner typischerweise die IPs seines zugehörigen DNS-Servers?
In den Blattknoten sind die IP-Adressen der durch die Labelsequenz gegebenen Namen gespeichert

Was ist der Unterschied zwischen einer (Sub-) Domäne und einer Zone?
Zonen sind (außer in den ‚tieferen' Bereichen des Baumes) meistens nur für ein Namenselement einer Domänen zuständig (dann müssen vom Name Server weniger Informationen verwaltet werden)

Was versteht man unter einem Zonen-Transfer?
Zonentransfer bezeichnet beim Domain Name System (DNS) die Übertragung von Zonen auf einen anderen Server. Dieses Verfahren wird AXFR (Asynchronous Full Transfer Zone oder Asynchronous Xfer Full Range) abgekürzt. Da ein DNS-Ausfall für ein Unternehmen meist gravierende Folgen hat, werden die DNS-Daten – also die Zonendateien – fast ausnahmslos identisch auf mehreren Nameservern gehalten. Bei Änderungen muss sichergestellt sein, dass alle Server den gleichen Datenbestand besitzen. Die Synchronisation zwischen den beteiligten Servern wird durch den Zonentransfer realisiert. Der Zonentransfer beinhaltet nicht nur das bloße Übertragen von Dateien

oder Sätzen, sondern auch das Erkennen von Abweichungen in den Datenbeständen der beteiligten Server.

Löst ein DNS-Server eine Anfrage rekursiv oder iterativ auf? Warum?
Normalerweise arbeiten Nameserver rekursiv, da einige Resolver mit einer iterativen Antwort nichts anfangen können.

Woher kennt ein DNS-Server den 'Startpunkt' seiner Suche?
Ein DNS-Server kann natürlich nicht den Startpunkt deiner Suche in Form eines Domain-Namens auflösen (das wäre ein Henne-Ei-Problem). Es existieren well-known IPs (siehe KS_14, Seite 15), die als feste IPs zum Ansprechen des Root-Nameservers verwendet werden.

Welche Verfahren nutzt ein DNS-Server zur Lastreduktion (bzw. zum Vermeiden von erneuten Anfragen)?
Jeder DNS-Server besitzt auch einen Cache. Dieser hält vor kurzem aufgelöste Anfragen vor. Den Zeitraum liefert der Server, der diese Adresse ursprünglich einmal aufgelöst hat

Was ist ein MX-Record?
Hier wird bestimmt, an welchen (Mail-)Server E-Mails geschickt werden. In der Regel haben Mail-Server bestimmte Domains, unter denen sie erreichbar sind. Jeder Anbieter eines Mail-Systems kommuniziert seine MX-Records klar für seine Nutzer.

Wichtig: Damit jede Mail auch am richtigen Mail-Server ankommt, müssen die MX-Records eindeutig sein!

Warum ist das DNS ein kritischer Dienst im Internet, und Ziel von Hacking-Attacken?
Da er nur UDP verwendet, ist er häufig Angriffsziel:

- DNS ID Hacking: Anfragen werden über IDs geschützt, d. h. der Client erwartet nicht nur die Auflösung, sondern auch noch eine spezielle ID. Wenn diese nicht vom Netz abgegriffen werden kann, so muss man sie erraten
- DNS spoofing: Hier beantwortet ein falscher DNS-Server die Anfrage. Hier muss die ID verwendet werden. Auch wird die falsche IP, also die des eigentlich richtigen Servers angegeben (was von den Providern zu unterbinden ist)
- DNS Cache Poisoning: Hier wird versucht, einen eigentlich korrekten DNS-Server zu „verseuchen“. Idee ist, den Cache falsch zu füllen.

Vorlesung 9 - Anwendungsprotokolle

Was bedeuten die Abkürzungen HTTP und HTML? Was ist ein 'HT' ?

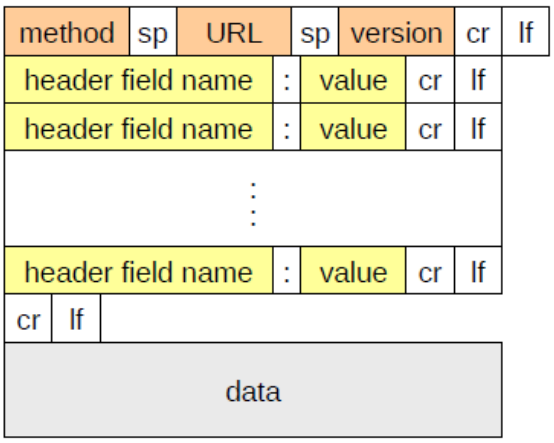
- HTML: Hypertext Markup Language
- HTTP: Hypertext Transfer Protocol
- 'HT': Hypertext

Erklären Sie den Zusammenhang zwischen URI, URL und URN!

- **URL:** Spezifikation von Ort und Zugriffsmodalitäten
- **URL:** (**U**niform **R**esource **L**ocator) Adressierung von Informationsobjekten mit Festlegung des Zugangs-Protokolls (Ort der Ressource). RFC2141
- **URN:** (**U**niform **R**esource **N**ame) Adressierung von Objekten ohne ein Protokoll festzulegen (Eindeutige und gleichbleibende Referenz – Name der Ressource). RFC1738
- **URI = URL ∪ URN**

Wie ist ein HTTP-Request-Header aufgebaut? Wie wird der Header von den Daten getrennt, und woher weiß man die Länge der Daten?

- Aufbau:



- Trennung: Leerzeile
- Länge: Als Attribut im Header (content-length)

Welche Gruppen von HTTP Status-Codes kennen Sie?

- 1xx – Informationen
- 2xx – Erfolgreiche Operation
- 3xx – Umleitung

- 4xx – Client-Fehler
- 5xx – Server-Fehler
- 9xx – Proprietäre Fehler

Welche HTTP-Methoden existieren neben 'GET'?

- **HEAD**
- **POST**
- **PUT**
- **DELETE**

Was ist MIME? Welche Attribute (mind. 3) im Header werden dazu verwendet, und was bedeuten (bzw. definieren) sie jeweils?

- **MIME** = **M**ultipurpose **I**nternet **M**ail **E**xtensions
- Attribute:
  - Content-Type: **IMAGE/JPEG**; name="picture.jpg"
  - Content-Transfer-Encoding: **BASE64**
  - Content-ID: <PINE.LNX.3.91.960212212235.325B@localhost>

Erklären Sie das Konzept von 'Virtual Hosts' bei HTTP!

- Auf einem Rechner sollen verschiedene Domains und Web-Server zur Verfügung stehen → Jeder Server hat die gleiche IP, aber ggf. unterschiedliche DNS-Namen!
- Ein oder mehrere Webserver (Software) sollen die Anfragen, für die auf dem Rechner vorhandenen Domains, beantworten
- Typische Anwendung: Web-Hosting (Provider)

Wo ist der SSL-Layer im ISO/OSI oder Internet-Schichtenmodell angesiedelt?
In der Darstellungsschicht (Schicht 6)

Erklären Sie die Unterschiede/Vorteile/Nachteile von symmetrischer und asymmetrischer Verschlüsselung!

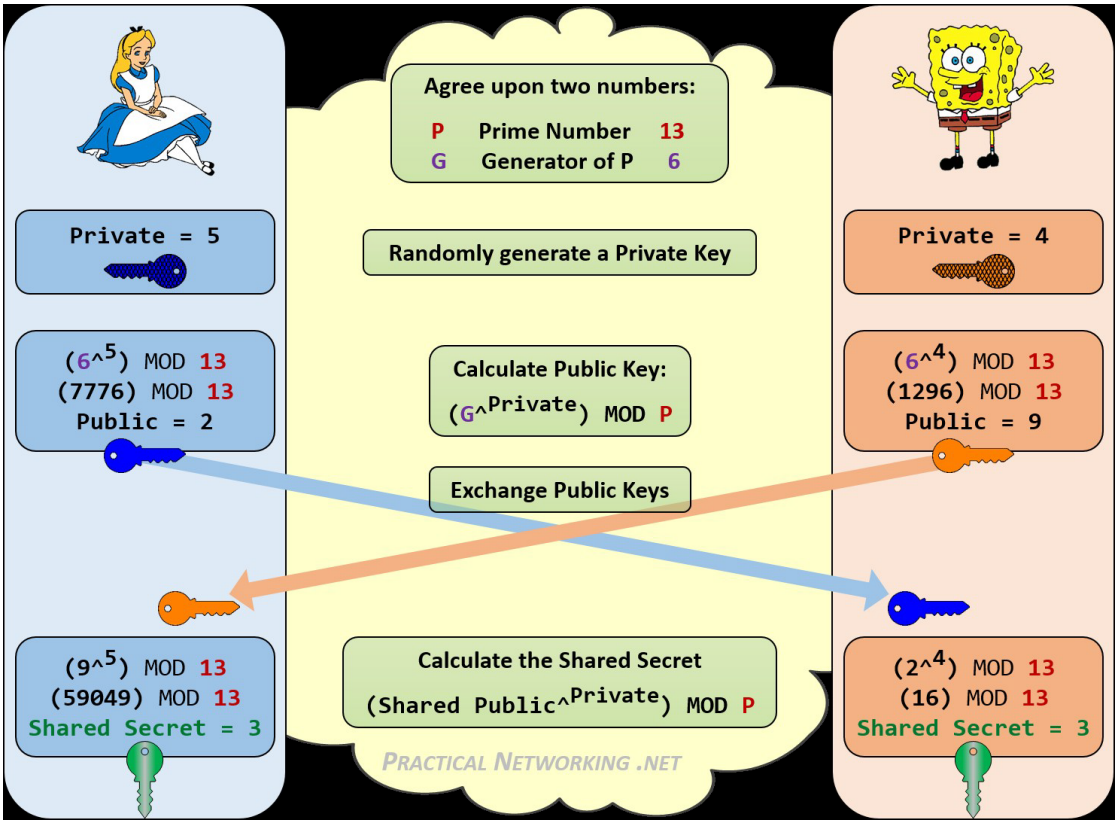
- Symmetrische Verschlüsselung:
  - schneller
  - braucht weniger Rechenleistung
  - Schlüssel muss allerdings an jeden verteilt werden, der die Daten entschlüsseln muss
- Asymmetrische Verschlüsselung:
  - sicherer
  - langsamer, da mehr Rechenleistung zum Entschlüsseln gebraucht wird
  - Schlüssel müssen nicht an alle verteilt werden (private und public Key)

Was ist ein Zertifikat? Wer stellt es aus, und welche Informationen enthält es?
Ein digitales Zertifikat ist ein digitaler Datensatz, der bestimmte Eigenschaften von Personen oder Objekten bestätigt und dessen Authentizität und Integrität durch kryptografische Verfahren geprüft werden kann. Das digitale Zertifikat enthält insbesondere die zu seiner Prüfung erforderlichen Daten. Die Ausstellung des Zertifikats erfolgt durch eine offizielle Zertifizierungsstelle, die Certification Authority (CA).

Welche Eigenschaften hat eine Hash-Funktion? Wo wird Sie im Kontext der Verschlüsselung eingesetzt?

- Surjektivität – Kein Ergebniswert (Hashwert) soll unmöglich sein, jedes Ergebnis (jeder Hashwert im definierten Wertebereich) soll tatsächlich vorkommen können.
- Effizienz – Die Funktion muss schnell berechenbar sein, ohne großen Speicherverbrauch auskommen (der Speicherbedarf des Hashwertes soll deutlich kleiner sein als jener des Schlüssels / Eingabewertes) und sollte die Quelldaten (Eingabewerte) möglichst nur einmal lesen müssen.
- Hash-Funktion wird verwendet, um die private Keys zu verschlüsseln

Wie kann man bei 2 Kommunikationspartnern ein 'Geheimnis' (z.B. einen Schlüssel zur symmetrischen Verschlüsselung) erzeugen, ohne dieses Geheimnis über das Netzwerk oder einen anderen Kanal auszutauschen?



Welche Aufgaben hat das SSL Handshake Protokoll und das SSL Record Protokoll?

- SSL Handshake Protokoll:
  - Den stärksten gemeinsam unterstützten Algorithmus ermitteln
  - Authentifikation der Kommunikationspartner (Client optional)
  - Ermitteln eines Session Keys zur symmetrischen Verschlüsselung (optional)
- SSL Record Layer:
  - Vollständig getrennt vom Handshake Protokoll
  - Verschickt Daten symmetrisch mit dem im Handshake ausgehandelten Verschlüsselungsalgorithmen und Session Keys
  - Bildet zu jedem Datenblock einen Message Digest zur Sicherung der Integrität

Warum sollte 'einfaches' FTP heute nicht mehr verwendet werden?
Zu unsicher, Übertragung der Login-Daten als Klartext ...

Warum gibt es in einem typischen Heimnetzwerk Probleme mit dem FTP 'Active' Mode?
In Heimnetzen wird typischerweise NAT verwendet, und beim 'Active' Mode horcht der Client für die Datenverbindung auf einem zufälligen Port und teilt diesen dem Server über die Kontrollverbindung mit. Diese Daten (IP in einem privaten Netz und Portnummer) sind aber für den NAT-Router nicht sichtbar (weil auf Anwendungsebene übertragen), und können daher vom NAT-Router nicht 'übersetzt' werden.

Informieren Sie sich über die Entstehungsgeschichte und Funktionalität von SSL und SSH!

- `https://de.wikipedia.org/wiki/Secure_Shell`
- `https://de.wikipedia.org/wiki/Transport_Layer_Security`
- `https://www.kreitiv.de/ssl-tls-und-ssh-verschluesselungsprotokolle/`

Wie funktionieren SFTP und TFTP?

- SFTP: FTP über SSH Session
- TFTP:
  - sehr einfaches Protokoll für den File-Transfer
  - die Kommunikation läuft über Port 69 und benutzt UDP, nicht TCP
  - hat keine Authentifizierung
  - benutzt immer 512-Byte-Blöcke

Welches Protokoll wird zum Versenden von Emails verwendet? Was passiert konkret bei Versenden, und wie ist das DNS beteiligt?

- Simple Mail Transfer Protokoll (SMTP)
- Email-Übertragung:
  1. User Agent erstellt E-Mail
  2. Aufteilen der E-Mail in Header und Body
  3. Überprüfen und Zwischenspeichern der E-Mail vom Message Transfer Agent
  4. MTA sucht Mailserver des Empfängers im DNS
  5. Mail wird an Mailserver verschickt
  6. Mail wird vom Ziel-MTA überprüft
  7. Mail wird vom Empfänger Mailserver gespeichert

Welche Protokolle werden zum Abrufen von Emails verwendet, und wie unterscheiden sie sich?

- Simple Mail Transfer Protocol (SMTP):
  - Versenden von E-Mails über TCP-Verbindung (Port 25)
  - SMTP ist ein einfaches ASCII-Protokoll
  - Ohne Prüfsummen, ohne Verschlüsselung
  - Ist der Server zum Empfangen bereit, signalisiert er dies dem Client. Dieser sendet die Information, von wem die E-Mail kommt und wer der Empfänger ist. Ist der Empfänger dem Server bekannt, sendet der Client die Nachricht, der Server bestätigt den Empfang.
- Post Office Protocol Version 3 (POP3):
  - Abholen der eMails beim Server über eine TCP-Verbindung, Port 110
  - Befehle zum An- und Abmelden, Nachrichten herunterladen, Nachrichten auf dem Server löschen oder liegen lassen, Nachrichten ohne vorherige Übertragung vom Server direkt löschen
- IMAP (Interactive Mail Access Protocol):
  - Hier werden die eMails nicht abgerufen und lokal gespeichert, sondern bleiben auf dem Server liegen!

Warum ist einfaches SMTP unsicher?

- Unverschlüsseltes, ASCII-basiertes Protokoll, Passwörter im Klartext.
- Einfache Möglichkeit zur Manipulation von E-Mails

Wozu dient das (veraltete) TELNET-Protokoll? Wozu kann es (z.B. im Praktikum) sinnvoll eingesetzt werden?

- TCP ermöglicht den transparenten, interaktiven Gebrauch von „entfernten“ Maschinen
- verbreitetes Protokoll: TELNET, welches auf einer Client/Server-Kommunikation basiert
- Ein „Pseudo-Terminal“ des Servers interpretiert Zeichen, als kämen sie von der eigenen Tastatur
- bei Antwort des Servers umgekehrter Weg (Pseudo-Terminal fängt Antwort ab, leitet sie über TCP an den Client weiter, der die Ausgabe am Bildschirm macht
- **Benutzername und Passwort werden unverschlüsselt übertragen**

Welches Protokoll sollte heute zum Login auf entfernten Rechnern verwendet werden?

- ssh adressiert die Sicherheitsprobleme von telnet und rlogin. Es ist ein Protokoll zur Erstellung einer sicheren Verbindung zwischen zwei Systemen. Alle während der Verbindung gesendeten und empfangenen Daten werden mit einer 128 Bit-Verschlüsselung verschlüsselt.
- ssh unterstützt verschiedene Authentisierungsarten:
  - Bei der sogenannten hostbased-Authentifizierung akzeptiert ein Rechner ohne eigene account-spezifische Tests die Vorgaben eines fremden Rechners. Es wird höchstens die Identität des fremden Rechners überprüft.
  - Die Authentifikation mit einem Passwort ist derzeit die 'übliche' Methode, um sich an einem Rechner anzumelden. Die Sicherheit dieses Mechanismus beruht auf der Geheimhaltung des Passwortes, dessen Übertragung allerdings verschlüsselt wird
  - Um auch das Übertragen eines verschlüsselten Passwortes zu vermeiden, werden die sogenannten public-key-Verfahren eingesetzt

Wie kann mein einen sicheren 'Tunnel' zu/von einem beliebigen (TCP-) Port einrichten?

Mit SSH: Port-Forwarding:

- verschlüsselte Verbindung zwischen zwei beliebigen Ports
- kann auch ohne Shell genutzt werden
- lokaler Port führt direkt auf den Zielport, als wäre dieser lokal

Wozu wird SNMP verwendet? Welches Transportprotokoll verwendet es? Was ist ein SNMP-Agent und eine MIB?

- Transportprotokoll: UDP
- SNMP: Protokoll, das festlegt, wie Management-Information kommuniziert wird (Formate und Bedeutung von SNMP-Nachrichten)
- MIB (Management Information Base): Die MIB spezifiziert die Informationseinheiten (items), die vorgehalten werden müssen, und welche Operationen darauf erlaubt sind.
- SNMP wird zum Management von Geräten im Netz verwendet (Fehlerstatus etc.)

Vorlesung 10 - Sicherungsschicht

In welche zwei Sublayer kann der Data-Link Layer (Schicht 2 in ISO/OSI) unterteilt werden? Was sind grob die Aufgaben dieser zwei Sublayer?

- LLC Sublayer: Das Protokoll LLC fügt einem gegebenen Datenpaket aus einer übergeordneten Schicht (meist der OSI-Schicht 3 „Vermittlungsschicht“) drei Felder hinzu:
  - zwei jeweils 8 Bit bzw. 1 Byte große Kennzeichen:
    - DSAP (Destination Service Access Point: Einsprungadresse des Empfängers)
    - SSAP (Source Service Access Point: Einsprungadresse des Absenders)
  - ein 1 oder 2 Byte großes Feld Control mit Steuerinformationen für Hilfsfunktionen wie z. B. die Datenflusssteuerung
- MAC Sublayer:
  - Das **Kanalzugriffsprotokoll** beschreibt, nach welchen Regeln auf ein Übertragungsmedium zugegriffen werden darf, d. h. ein Rahmen auf der Verbindungsleitung übertragen werden darf
  - Bei Punkt-zu-Punkt-Verbindungen ist das Leitungszugriffsprotokoll einfach.
  - Der Sender kann einen Rahmen senden, wann immer die Verbindungsleitung frei ist (bei vollduplex immer)
  - Bei Multi-Access-Netzen teilen sich mehrere Teilnehmer eine Verbindungsleitung, z. B. nach dem Bus-Prinzip.
  - Hier übernimmt der MAC Layer die Koordination der Leitungsnutzung
  - Der MAC-Layer liefert eine eindeutige Kennung für jedes Netzwerkgerät bzw. jede Netzwerk-Karte → MAC Adresse

Welche Übertragungsmedien (auf Schicht 1 in ISO/OSI) werden heute typischerweise eingesetzt?

- Kupferdoppelader (Twisted Pair)
- Koaxialkabel
- Funk
- Glasfaser

Welche physikalischen Größen werden dabei verwendet, und wie können diese moduliert werden?

- Spannung
- Elektromagnetische Wellen (Funk, Licht)

- Modellierung über:
  - Amplitude
  - Frequenz
  - Phase
- Die Veränderung dieser Eigenschaften im Rahmen der Datenübertragung nennt man Modulation
  - Amplitudenmodulation (AM)
  - Frequenzmodulation (FM)
  - Phasenmodulation (PM)

Welche unterschiedlichen Arten von 'twisted pair'-Kabeln kennen Sie?

- Unterscheidung nach Kategorie:
  - Kategorie 3 : Gemeinsame Umhüllung für vier Kupferdoppeladern
  - Kategorie 5 : Wie Kategorie 3, aber mehr Windungen/cm (weitere Reduktion der elektromagnetischen Interferenzen Umhüllung besteht aus Teflon (bessere Isolierung, Qualität der Signale bleibt auf längere Strecken akzeptabel)
  - Kategorie 6,7 : Die Paare sind zusätzlich einzeln mit Silberfolie umwickelt
- Unterscheidung nach Abschirmung:
  - UTP Kabel (Unshielded Twisted Pair) : Keine Abschirmung des Kabels STP Kabel (Shielded Twisted Pair) : Abschirmung des Kabels, dadurch günstigere Eigenschaften, trotzdem in der Praxis oft UTP
- Beispiele: S/UTP-Kabel (cat 5), S/STP-Kabel (cat 7)

Wie ist ein Glasfaserkabel prinzipiell aufgebaut? Wo findet die 'Übertragung' statt?

- Von innen nach außen:
  1. Faserkern / Kernglas (core)
  2. Mantelglas (cladding)
  3. Beschichtung (coating)
  4. Kunststoffummantelung (buffering)
  5. Schutzmantel
- Im Glaskern findet die Übertragung statt

Erklären Sie im Zusammenhang mit Glasfaserkabeln die Begriffe 'Moden' und 'Dispersion'!

- Dispersion
  - Begrenzt Übertragungsstrecke
  - Lichtpuls besteht aus mehreren Wellen (Strahlen) → Einfallswinkel dieser Strahlen unterschiedlich
  - Lichtstrahlen kommen im Medium unterschiedlich schnell vorwärts:
    - Wege (**Moden**) der Strahlen unterschiedlich lang (abhg. von Einfallswinkel)
    - Strahlen eines Impulses kommen zeitversetzt am Ende des Kabels an
    - Intensität der Impulse nimmt ab, benachbarte Impulse verschwimmen
  - (Weitere Faktoren können ebenso Dispersion verursachen)

Wie unterscheiden sich Monomode- und Multimode Glasfaserkabel? Welche Eigenschaften resultieren aus dem unterschiedlichen Aufbau?

- Monomode-Faser
  - Kerndurchmesser: 8–10 μm
  - Alle Strahlen können nur noch einen Weg nehmen
  - Keine Dispersion (homogene Signalverzögerung)
  - 50 $\frac{GBit}{s}$ über 100 km
  - Teuer wegen geringem Kerndurchmesser
- Multimode-Faser mit Stufenindex
  - Kerndurchmesser: 50 μm
  - Unterschiedliche Wege für Lichtwellen, je nach Einfallswinkel
  - Starke Dispersion
  - Bis zu 1 km
- Multimode-Faser mit Gradientenindex
  - Kerndurchmesser: 50 μm
  - Brechungsindex ändert sich fließend
  - Leicht unterschiedliche Wege für Lichtwellen
  - Geringe Dispersion
  - Bis zu 30 km

Bei welcher Netztopologie gibt es ein 'gemeinsames' Medium, auf das alle Teilnehmer zugreifen?
Multi-Access-Netz (gemeinsames Medium)

- Nur in lokalen Netzen verwendet
- Alle Stationen sind an ein einziges Medium angeschlossen
- Sendet eine Station Daten, werden sie an alle Stationen ausgeliefert
- Jeder Rechner kontrolliert jedes Paket, ob es für ihn bestimmt ist

Bei welchen Netztopologien gibt es ausschließlich Punkt-zu-Punkt-Verbindungen zwischen den Teilnehmern?

- Stern
- Ring
- Baum (mit Stern Verbindungen)

Vergleichen Sie Ring-, Bus- und Stern-Topologie bzgl. ihrer Vor- und Nachteile!

- Ring: Point-to-Point
  - Reihe von Punkt-zu-Punkt-Verbindungen
  - Aktive Knoten: fungieren als Repeater
  - Ausfall des gesamten Rings bei Unterbrechung einer Verbindung
  - Ausfall des gesamten Rings bei Ausfall eines Knotens (Bypass als Abhilfe)
  - Große Ausdehnung möglich (aufgrund der aktiven Knoten)
  - Einfaches Einfügen neuer Knoten
  - Variante: bidirektionaler Ring: Knoten sind durch zwei gegenläufige Ringe miteinander verbunden
- Bus: Multi-Access-Netz
  - \+ Einfach, preiswert, einfacher Anschluss neuer Knoten
  - \+ Passive Ankopplung der Stationen, der Ausfall eines Knotens ist kein Problem für die anderen Knoten
  - – Nur eine Station zu einem Zeitpunkt kann senden; alle anderen Stationen können nur empfangen
  - – Begrenzung der Zahl anschließbarer Stationen
  - – Passive Ankopplung der Stationen, daher begrenzte Ausdehnung des Busses (aber: Repeater zur Kopplung mehrerer Busse)
- Stern
  - Ausgezeichneter Knoten als zentrale Station

        * Nachricht von Station A wird durch die zentrale Station an Station B weitergeleitet
        * Punkt-zu-Punkt-Verbindungen (Switch), oder Broadcast (Hub)
        * Verwundbarkeit durch zentralen Knoten (Redundanz möglich)

Wie (und auf welcher Schicht) arbeitet ein Repeater?

- Verknüpfung von zwei Netzen zur Vergrößerung der Ausdehnung
- Arbeitet auf der Bitebene
  - Kann einkommende Signale als „0“ oder „1“ interpretieren
  - Empfang und Auffrischung des Signals – ein empfangenes Bit wird auf der anderen Seite neu als Stromimpuls codiert
  - Kein Verstehen von Adressen höherer Schichten, alle Daten werden weitergeleitet (das Netz bleibt z. B. ein Multi-Access-Netz)

Erklären Sie (im Kontext eines Netzes mit twisted-pair Kabeln) den Unterschied zwischen einem Hub und einem Switch!

- Hub = „Repeater mit mehr als zwei Anschlüssen“
  - Signalauffrischung wie beim Repeater
  - An einen Anschluss kann ein einzelner Rechner oder ein ganzer Bus angeschlossen werden
  - Multi-Access-Netz: der Hub gibt ein empfangenes Signal auf allen Anschlüssen wieder aus, praktisch wie ein ’Bus’ mit mehreren Anschlüssen:
  - Gemeinsamer Übertragungskanal, d. h. Stationen können nicht gleichzeitig senden und empfangen, nur eine Station auf einmal kann senden
  - Geringe Sicherheit, da alle Stationen mithören können
- Switch - Wie Hub, aber:
  - Punkt-zu-Punkt-Kommunikation zwischen zwei Stationen
    * Switch kann Layer-2-Adressen (MAC-Adressen) der angeschlossenen Stationen verstehen, lernt sie und kann Daten gezielt weiterleiten
    * Stationen können gleichzeitig senden und empfangen
    * Nur der adressierte Empfänger erhält die Daten, andere Stationen können nicht mithören
  - Vermeidung von Kollisionen (‚Mikrosegmentierung‘)
  - Puffer für jeden Port

Was ist ein 'Layer-3 Switch'?

- Ein Layer-3-Switch ist eine Kombination aus Router und Switch.
- Er beherrscht nicht nur Switching, sondern auch Routing.
- Da Router und Switche sehr ähnlich funktionieren – sie empfangen, speichern und leiten Datenpakete weiter – ist es nur logisch beide Geräte miteinander zu kombinieren, um daraus ein Multifunktionsgerät zu machen.

Warum gibt es in der Schicht 2 neben dem Header auch einen Trailer? Welche Felder enthält der Ethernet-Header?

- Trailer:
  - Frame Check Sequence (CRC Prüfsumme)
- Header:
  - MAC Empfänger
  - Absender
  - Ethernet Typ

Vorlesung 11 - Kanalzuteilung, Fehlerkorrektur

Welche Aufgabe hat der MAC Sublayer in der Schicht 2 (Wiederholungsfrage, siehe Vorlesung 10)?
Regelung des Zugriffs auf das Übertragungsmedium

Welche Eigenschaften hätte ein ideales Mehrfachzugriffsprotokoll?
Broadcast-Medium mit Maximalrate R bps

- Ein einzelner Knoten kann mit der Rate R übertragen
- M Knoten können mit einer mittleren Rate von $\frac{R}{M}$ übertragen
- Das Protokoll ist dezentral, d. h. es gibt keine Master-Knoten, die ausfallen und das ganze System zum Absturz bringen können
- Das Protokoll ist einfach und kann somit kostengünstig implementiert werden

Nennen Sie 3 grundsätzliche Strategien, wie der mehrfache Zugriff auf ein gemeinsames Medium gelöst werden kann!

- Kanalaufteilungsprotokolle (Multiplexing)
  - Aufteilung des Übertragungskanals in kleine Übertragungseinheiten (Zeitfenster, Frequenzen, Kodierung)
  - Exklusive Nutzung der Übertragungseinheiten für einzelne Knoten
- Zufallszugriffsprotokolle
  - Keine Unterteilung des Kanals, jeder überträgt mit der gesamten Leitungskapazität. Allerdings sind Kollisionen von Nachrichten möglich und müssen korrekt behandelt werden
- Rotationsprotokolle
  - Der Zeitpunkt, wann ein Knoten senden kann wird durch eine spezielle Koordinierung nach einem flexiblen Rotationsprinzip im Übertragungsmedium ausgetauscht.

Erklären Sie kurz die Funktionsweise von TDMA, FDMA und CDMA!

- TDMA: Time Division Multiple Access:
  - Aufteilung des Kanals in kleine Zeiteinheiten, die sich in Runden wiederholen
  - Jeder Knoten kann eine bestimmte Anzahl an Zeiteinheiten in jeder Runde nutzen
  - Ungenutzte Einheiten (slots) bleiben ungenutzt
  - Die Zeiteinheiten können meist auch gruppiert angefordert werden
  - Anforderung entspricht Konfiguration der NIC-Karte
- FDMA: Frequency Division Multiple Access

  - Aufteilung des Kanals in Frequenzbänder
  - Nach Nyquist kann ein rauschfreier Kanal mit einem Frequenzband der Breite x Hz binäre Signale nicht mit mehr als 2x Bps übertragen (Nyquist-Bandbreite)
  - Jede Station nutzt ein Frequenzband
  - Die Kapazität nicht genutzter Frequenzbänder geht verloren
- CDMA: Code Division Multiple Access
  - Keine Unterteilung in Zeitslots oder Frequenzen
  - Nutzung von ‚orthogonalen Codes' bei der (De-) Modulation, die sich im Medium überlagern/mischen, aber trotzdem auf Empfängerseite eindeutig wiederhergestellt werden können
  - Vorteil: Es gibt keine ungenutzten Resourcen wie bei TDMA/FDMA

Erklären Sie die Funktionsweise von CSMA/CD! Was bedeutet diese Abkürzung?

- Carrier Sense Multiple Access (CSMA)
  - höre vor der Übertragung das Medium ab
  - sende nur, falls das Medium frei ist
  - Analogie: Unterbreche keine Anderen
- Carrier Sense Multiple Access with Collision Detection (CSMA/CD)
  - wie CSMA, zusätzlich: höre während der Sendung das Medium weiter ab und breche die Übertragung ab, wenn eine Kollision auftritt
  - sende ein Jamming-Signal, damit jede Station weiß, dass eine Kollision aufgetreten ist und die Nachricht nutzlos geworden ist.
  - Wichtig: Man muss so lange senden, dass man ein Jamming-Signal während dessen auch mitbekommt

Erklären Sie, warum bei CSMA/CD ein Sender eine Mindestzeit senden muss (und parallel per 'CD' das Medium abhören muss)! Wie lässt sich diese Mindestzeit berechnen und ggf. in eine Mindest-Rahmengröße umrechnen?

Die maximale Zeit zur Entdeckung einer Kollision ist knapp zweimal so lang wie die Signallaufzeit auf dem Medium. Bei einer Signalgeschwindigkeit von ungefähr 100000 $\frac{km}{s}$ (10 $\frac{\mu s}{km}$) erhält man (unter Berücksichtigung der Zeit in 4 Repeatern) eine maximale Ende-zu-Ende-Signallaufzeit von 25 μs. Die maximale Konfliktdauer ist damit ca. 50 μs. Um einen Konflikt mit Sicherheit zu erkennen, muss die Station mindestens 50 μs auf dem Medium horchen und senden $\rightarrow$ bei 10 $\frac{MBit}{s}$ mindestens 500 Bit. Darauf basierend wurde für eine Senderate von 10 $\frac{MBit}{s}$ eine minimale Rahmenlänge (aufgerundet 64 Byte) definiert, um eine Kollisionserkennung auch im Worst-Case zu ermöglichen!

Wie funktioniert und wozu dient der 'Binary Exponential Backoff' - Algorithmus?
Um nach einer Kollision die gleichzeitige Wiederholung der kollidierten Sendungen zu vermeiden (Folgekollision), wird eine zufällige Wartezeit aus einem vorgegebenen Intervall gezogen. Das Intervall wird *klein* gehalten, um große Wartezeiten bis zur Wiederholung zu vermeiden. Dadurch ist allerdings das Risiko eines Folgekonflikts groß. Kommt es so zu einer weiteren Kollision, wird das Intervall vor dem nächsten Versuch vergrößert, um mehr Spielraum für alle sendenden Parteien zu schaffen.

Welche heute typischerweise eingesetzten Ethernet-Standards kennen Sie? Wie sind die Namen aufgebaut?
Basiert auf IEEE 802.3 „CSMA/CD“ 4 Klassen von Ethernet-Varianten:

- Standard Ethernet $\rightarrow 10\ \frac{Mb}{s}$
- Fast Ethernet $\rightarrow 100\ \frac{Mb}{s}$
- Gigabit Ethernet $\rightarrow 1000\ \frac{Mb}{s}$
- 10Gigabit-Ethernet $\rightarrow 10000\ \frac{Mb}{s}$

Warum wurde bei Gigabit-Ethernet die minimale Rahmenlänge von 64 auf 520 Bytes erhöht?
Damit die Segmentlänge nicht auf ca. 20 Meter verringert werden musste. Da Gigabit-Ethernet 10-mal schneller ist als Fast-Ethernet, musste (bei gleicher mindest-Sendedauer) die Rahmenlänge ca. verzehnfacht werden (64 Byte $\rightarrow$ 520 Byte).

Warum wurde bei Fast-Ethernet die Segmentlänge von 2500m (10MBit Ethernet) auf 200–250m verkleinert?
Die minimale Rahmenlänge zur Kollisionserkennung bei Ethernet beträgt 64 Byte. Bei 100 Mb/s wird der Rahmen aber ca. 10 Mal so schnell abgesendet, sodass eine Kollisionserkennung nicht mehr gewährleistet ist.

Wie ist die Rahmen-Struktur eines Ethernet-Paketes aufgebaut? Welche Daten (-Felder) werden im Header und Trailer auf Schicht 2 übertragen?
Ethernet-Rahmen:

- Präambel: kennzeichnet eine folgende Übertragung und synchronisiert den Empfänger mit dem Sender.
- Der Start-of-Frame-Delimiter: (bzw. die beiden aufeinanderfolgenden Einsen) zeigen an, dass endlich Daten folgen.
- Destination Address: das erste Bit kennzeichnet den Empfänger: entweder eine einzelne Station (1. Bit = 0) oder eine Gruppenadresse (1. Bit = 1; Broadcast ist auch hier durch $11 \ldots 1$ gegeben).
- Length/Type: Bei einem Wert bis 1500 wird die Angabe als Länge des Datenteils aufgefasst (dies ist der Fall beim sogenannten CSMA/CD), bei einem Wert ab

1536 wird hier angegeben, an welches Schicht-3-Protokoll die Daten weitergegeben werden sollen (verwendet bei Ethernet).

- FCS: Checksumme, 32-Bit CRC. Diese erstreckt sich über die Felder DA, SA, Length/Type, Data/Padding.

Felder in Schicht 2:

- MAC-Empfänger
- MAC-Absender
- 802.1Q-Tag (opt.)
- EtherType
- Nutzlast (1500 bytes)
- Frame Check Sequence

Erklären Sie die grundsätzliche Vorgehensweise des Medienzugriffes beim Token-Ring Netz!

- 'Token'-Verfahren, nur wer ein bestimmtes Token (= Bitfolge) besitzt, darf senden
- Die Rechner teilen sich einen Ring aus Punkt-zu-Punkt-Verbindungen
- Das Token wird zyklisch weitergegeben

Was ist ein Hamming-Abstand bei einem Code C mit den Wörtern c_1 bis c_n?

- Anzahl unterschiedlicher Bits zweier Codewörter c_1 und c_2, d. h. Anzahl der 1-Bits von c_1 XOR c_2.
- Beispiel: d(10001001, 10110001) = 3
- Hamming-Abstand D von vollständigem Code C :

$$D(c) \coloneqq \min\{d(c_1, c_2) \mid c_1, c_2 \,\epsilon\, C;\ c_1 \neq c_2\}$$

Was versteht man unter "Forward Error Correction"?

Das Erkennen UND Korrigieren von Bitfehlern bei der Datenübertragung

Wie groß muss der Hamming-Abstand mindestens sein, um e-Bitfehler zu erkennen bzw. zu beheben?

- erkennen von e-Bit-Fehlern: Hamming-Abstand e+1 notwendig
- beheben von e-Bit-Fehlern: Hamming-Abstand 2e+1 notwendig

Nennen Sie einen Code, der mit einer minimalen Anzahl von Prüfbits Einzelbitfehler korrigieren kann!

Hamming-Code (siehe KS_17, Seite 39 ff)

Was versteht man unter Modulo-2 Arithmetik? Wie werden Addition und Subtraktion durchgeführt?

- Die Rechenoperationen werden in der Modulo-2-Arithmetik einfacher, da hierbei keine Überträge zu berücksichtigen sind!
- Addition und Subtraktion führen so zu dem gleichen Ergebnis.
- Wir können einfach mit XOR arbeiten!
- Digitaltechnik, hier Halbaddierer: Eine Addition ist logisch ein XOR, das Carry ein UND
- Es gibt eine Bitkombination n, sodass gilt: $(D \cdot 2^r) XOR\ R = nG$
- D. h., R soll so gewählt werden, dass G in $D \cdot 2^r$ ohne Rest teilbar ist
- $D \cdot 2^r = nG\ XOR\ R$
- Damit kann man R berechnen, denn wenn man $D \cdot 2^r$ durch G teilt, ist der Rest des Wertes genau R

$$R = Rest\left[\frac{D \cdot 2^r}{G}\right]$$

Was leistet bzw. wie funktioniert das CRC-Verfahren? Wozu dient das Generator-Polynom? Wo wird das Verfahren im Kontext von Ethernet eingesetzt?

- Polynom-Codes: Interpretiere Datenbits D als Bitkette eines Polynoms, dessen Koeffizienten d0–10-1-Werte der Bitkette sind
- Prüfung basiert auf Polynom-Arithmetik
- Sender und Empfänger einigen sich auf ein gemeinsam verwendetes Bitmuster der Länge r+1 Bit, das als Generator G bezeichnet wird. Das höchstwertige Bit hiervon ist 1
- Konzept: Berechne die r CRC-bits R so, dass die d + r Bits (als Binärzahl interpretiert) mit der Modulo-2-Arithmetik genau durch G teilbar sind
  - Empfänger kennt G, teilt <D,R> durch G. Falls der Rest ungleich 0, so liegt ein Fehler vor!
  - Kann Burst-Fehler von weniger als r+1 Bits und jede ungerade Fehlerzahl erkennen

Vorlesung 11 - Beispielaufgaben

Übungsaufgabe 1:
Zur Berechnung einer CRC Prüfsumme soll das Generatorpolynom $x^5 + x^3 + x^2 + 1$ verwendet werden. Berechnen Sie die CRC-Prüfsumme zur Bitfolge **11110111** und geben Sie an, welche Daten tatsächlich gesendet werden!

Vorlesung 11 - Lösungen

Übungsaufgabe 1:
Zur Berechnung der CRC Prüfsumme wird das Generatorpolynom in eine Bitfolge mit führender '1' umgewandelt:

$$1x^5 + 0x^4 + 1x^3 + 1x^2 + 0x^1 + 1x^0 -> 101101$$

Das Polynom ist also vom Grad 5, und wir müssen 5 Nullen an die zu sendenden Daten anhängen! Danach rechnen wir so lange in Modulo-2 Arithmetik (XOR-Verknüpfungen), bis keine Bits mehr übrig sind:

1	1	1	1	0	1	1	1	0	0	0	0	0
1	0	1	1	0	1							
0	1	0	0	0	0	1						
	1	0	1	1	0	1						
	0	0	1	1	0	0	1	0				
			1	0	1	1	0	1				
			0	1	1	1	1	1	0			
				1	0	1	1	0	1			
				0	1	0	0	1	1	0		
					1	0	1	1	0	1		
					0	0	1	0	1	1	0	0
							1	0	1	1	0	1
							0	0	0	0	0	1

Das Ergebnis der Prüfsummenberechnung ist 00001, d. h. die zu sendende Bitfolge ist: 1111011100001

Vorlesung 12 - Leitungscodes, WLAN

Erklären Sie den Begriff Signalbildung (bzw. Leitungskodierung)!
Signalbildung ist die Umwandlung der binären Sendedaten (nach eventueller Kompression und/oder Kodierung mit Prüfsummen etc.) in physikalische Signale. Die Signale müssen dabei nicht unbedingt binär sein, sondern können auch mehr als 2 Zustände annehmen.

Welche Anforderungen kennen Sie, die ein guter Leitungscode erfüllen sollte?

- Möglichst hohe Widerstandsfähigkeit gegen Dämpfung
- Effizienz: möglichst hohe Übertragungsraten durch Codewörter
  - binärer Code: +5V / -5V?
  - ternärer Code: +5 V / 0V / -5V?
  - quaternärer Code: 4 Zustände (Codierung von 2 Bit gleichzeitig)
- Taktrückgewinnung beim Empfänger (Synchronisation), dazu möglichst häufige/regelmäßige Pegelwechsel
- Gleichstromfreiheit: positive und negative Signale treten ungefähr gleich oft auf → kein nennenswerter elektrischer Gleichstrom-Fluss
- Robustheit: Können längere Sequenzen von 0 und 1 noch als solche noch erkannt werden? Können fehlerhafte Bits erkannt werden?

Welche Vor- und Nachteile hat ein binärer gegenüber einem quaternären Code?

- Vorteil: Ein quaternärer Code kann 2 Nutzdatenbits in einem Code-Symbol abbilden
- Nachteil: Die Unterscheidung von 4 verschiedenen Signalzuständen kann anfälliger gegenüber Störungen bei der Übertragung sein.

Erklären Sie den Unterschied zwischen Basisband- und Breitband-Übertragung!

- Basisband: Das Basisband ist der natürliche Frequenzbereich des Nutzsignals (untere Grenzfrequenz $f_{\min}$ gleich oder nahe bei 0 Hz). Die digitalen Informationen werden ‚direkt' in physikalische Größen übersetzt und so über die Leitung übertragen. Hierzu sind Kodierungsverfahren notwendig, die festlegen, wie bei der Übertragung eine 0 bzw. eine 1 repräsentiert werden. Es kann nur je ein Signal übertragen werden
- Breitband: Die digitalen Nutzdaten werden nicht direkt übertragen, sondern einem oder mehreren hochfrequenten Trägern aufmoduliert. Durch die Verwendung verschiedener Trägerwellen (Frequenzen) können dann mehrere Informationen gleichzeitig übermittelt werden

Erklären Sie den Unterschied zwischen Bit- und Baudrate!

- Wenn die Zeitdauer (Schrittdauer) eines Symbols bzw. Codeelements T ist, ist die Schrittgeschwindigkeit
$$v_s = \frac{1}{T}$$
(Einheit: Baud), Symbolrate

- Die Übertragungsgeschwindigkeit (äquivalente Bitrate) ist dann

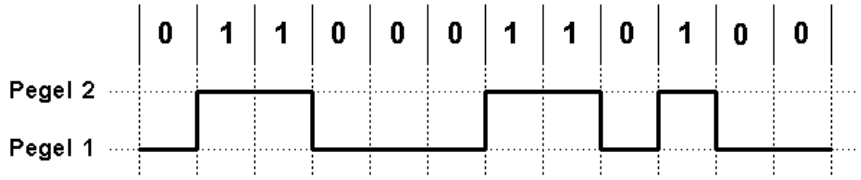
$$v_u = v_s ldn$$

(n = Anzahl diskreter Zustände des Codeelements)

Bei binären Codeelementen stimmen somit Bitrate und Baudrate (Schrittgeschwindigkeit) überein, falls nur Codeelemente für Daten übermittelt werden (es gibt auch Codeelemente für z. B. die Rahmenstruktur)

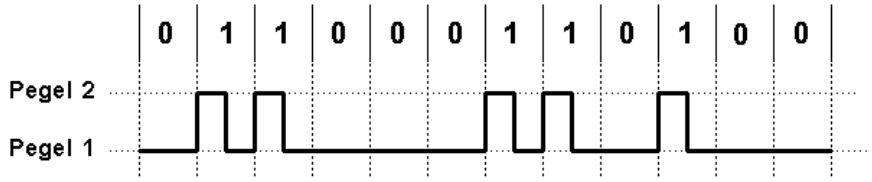
Was ist der Unterschied zwischen einem NRZ- und einem RZ-Code?

- **NRZ / NRZ-L: Non-Return_to_Zero:**
  - Kein automatisches Zurückfallen auf einen Grundpegel. Hier z. B.:
  - 0 = negative Spannung (konstant 0V), Pegel 1
  - 1 = positive Spannung (konstant +5V), Pegel 2
  - Nachteil: bei langen 0 oder 1 Folgen Taktverlust und keine Gleichstromfreiheit
  - Beispiel: UART, RS232 (serielle Schnittstellen)



NRZ-L-Code

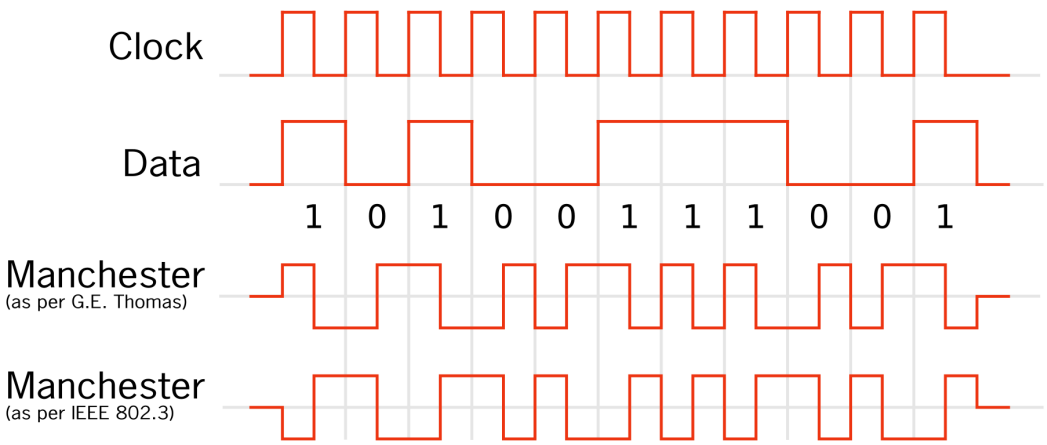
- **RZ: Return to Zero (hier unipolar)**
  - 0 = 0V
  - 1 = $\frac{T}{2}$ lang 1, $\frac{T}{2}$ lang 0
  - Vorteil: Taktrückgewinnung bei 1-Folgen
  - Nachteil: Keine Gleichstromfreiheit, kein Takt bei langen 0-Folgen
  - Beispiel: IrDA – Fernbedienung



RZ-Code

Welche Eigenschaften besitzt der Manchester-Code? Was bedeutet 1B2B? Wie unterscheiden sich die Standards nach G.E. Thomas und IEEE 802.3?

- Eigenschaften:
  - Lange Folgen gleicher Signale werden durch einen Pegelwechsel in der Mitte jedes Bits verhindert. Nach G. E. Thomas:
  - 0 = Polaritätswechsel von negativ (-5V) nach positiv (+5V)
  - 1 = Polaritätswechsel von positiv (+5V) nach negativ (-5V)
  - Vorteil: Gleichstromfrei, Taktrückgewinnung möglich
  - Nachteil: Doppelte Bandbreite im Vergleich zu NRZ, Bitrate = $\frac{Baudrate}{2}$
  - Beispiel: 10Base2



- 1B/2B: ein Bit wird auf zwei Symbole kodiert

Welche Vorteile hat ein 4B/5B Code gegenüber einem 1B/2B Code?

- Nachteil des Manchester-Codes:
  - 50% Effizienz, d. h. 1B/2B-Code (ein Bit wird auf zwei Symbole kodiert) Eine Verbesserung stellt der 4B/5B-Code dar:
  - vier Bit werden in fünf Symbole kodiert: 80% Effizienz
- Arbeitsweise:
  - Pegelwechsel bei 1, kein Pegelwechsel bei 0 (Differentieller NRZ-Code)
  - Kodierung von hexadezimalen Zeichen: 0, 1, ..., 9, A, B, ..., F (4 Bit) in 5 Bit, sodass lange Nullenblöcke vermieden werden.
  - Auswahl der günstigsten 16 der möglichen 32 Codewörter (maximal 3 Nullen in Folge)
  - Weitere 5 Bit-Kombinationen für Steuerinformationen

  - Erweiterbar auf 1000B/1001B-Codes?

Welche Eigenschaften eines Trägersignals können zur Modulation verwendet werden?

- Amplitude
- Frequenz
- Signale
- $s(t) = A \cdot \sin(2 \cdot \pi \cdot f \cdot t + \phi)$

Welche Möglichkeiten kennen Sie, um bei einer Breitbandübertragung die Datenrate zu erhöhen?

- Erhöhung der Bandbreite (des Frequenzbandes, auf dem übertragen wird). Das ist bei höheren Trägerfrequenzen i. d. R. einfacher
- Steigerung der in einem Abtastvorgang modulierten binären Informationen (Verwendung eines Codes mit z. B. 4/8/16 Bits pro Abtastung)

Warum ist PSK weniger störanfällig als z. B. ASK?

- Die Amplitude unterliegt Schwächung/Dämpfung, und ist daher störanfällig
- Die Phase einer Schwingung ist auch bei stärkeren Störungen unverändert

Wie unterscheiden sich QPSK und QAM?

- BPSK (Binary Phase Shift Keying):
  - = einfaches PSK
  - > Bitwert 0: Sinuswelle
  - > Bitwert 1: invertierte Sinuswelle
  - Niedrige Datenraten
  - Robuste Übertragung
  - Auch oft als differentieller Code (DBPSK)
- QPSK (Quaternary Phase Shift Keying):
  - Zwei Bit werden gemeinsam codiert
  - Vier unterschiedliche Phasenlagen
  - Doppelte Datenraten verglichen mit BPSK

Welche Störeinflüsse gibt es bei der Datenübertragung mit Funkwellen?

- natürliche Umgebung: Gebirge, Wasser, Vegetation, Regen, Schnee
- künstliche Umgebung: Gebäude etc.

Worin unterscheidet sich ein kabelgebundenes gemeinsames Medium (z.B. ein Bus bei 10Base2) von einem funkbasierten 'gemeinsamen' Medium (Luftraum bei WLAN)?
Bei einem Kabelgebundenen Medium werden Daten an alle angeschlossenen Teilnehmer weitergeleitet. Bei funkbasierten Techniken teilen sich auch alle Teilnehmer das gleiche Medium ('Luft'), aber je nach Abstand können entfernte Stationen sich nicht mehr 'hören' – das Medium zwischen diesen Stationen ist praktisch unterbrochen.

Wie groß sind typische Übertragungsraten beim WLAN? Welche Frequenzbänder werden benutzt?

- Datenraten:
  - 1, 2, 5.5, 11, 6, 9, 12, 18, 24, 36, 48, 54, ... $\frac{MBit}{s}$ Bruttodatenrate
  - Abhängig von Signalqualität wird die bestmögliche Datenrate gewählt
  - Nutzdatenrate wenig mehr als die Hälfte der jeweiligen Bruttodatenrate
- Frequenzbereich:
  - Freies 2.4 GHz-Band (2.4 - 2.4835 GHz) ISM = Industrial – Scientific – Medical
  - Optional 5 GHz-Band

Warum ist das CSMA/CD-Verfahren bei WLAN nur schwer anwendbar?
Zentral hierbei ist das Hidden-Station-Problem. Dies tritt auf, wenn zwei Stationen sich gegenseitig nicht wahrnehmen, aber gleichzeitig mit einer dritten Station in der Mitte kommunizieren – was unweigerlich zu Kollisionen führt.

Erklären Sie das 'Hidden Station'-Problem bei WLAN!

- A sendet an B, C empfängt A nicht
- C will an B senden, stellt freies Medium fest (CS schlägt fehl)
- Kollision bei B, A bemerkt sie nicht (CD schlägt fehl)
- A ist hidden (versteckt) für C

Erklären Sie das 'Exposed-Station'-Problem bei WLAN!

- B sendet zu A, C will zu D senden
- C muss warten, da CS ein „besetztes“ Medium signalisiert
- da A aber außerhalb der Reichweite von C ist, ist dies unnötig A

Erklären Sie grob das Vorgehen bei CSMA/CA! Wie werden Kollisionen verhindert?

- Carrier Sense Multiple Access with Collision Avoidance
- Kollisionen können nicht erkannt werden, darum wird versucht, sie zu vermeiden
- Carrier Sense mit zufallsgetriebenen Backoff-Mechanismus

- Kollisionsvermeidung Idee:
  - Vor Beginn des Sendens: Carrier Sense
  - Falls Medium frei für mindestens eine Zeit von DIFS, starte direkt mit Übertragung
  - Falls Medium belegt: warte bei Freiwerden erneut für DIFS, wähle dann eine Backoff-Zeit vor nächsten Zugriffsversuch (Kollisionsvermeidung)
    - Backoff-Zeit ist Vielfaches eines Zeitslots
- Kollisionsvermeidung Vorgehen:
  - Falls Medium nach Ablauf der Backoff-Zeit noch immer frei, starte mit Übertragung
  - Falls Medium eher belegt wird:
    - Stoppe Backoff-Zähler
    - Verwende aktuellen Wert beim nächsten Versuch weiter
- Quittierung jeder Übertragung, da Kollisionen nicht erkannt werden können
  - Direkte Bestätigung jedes korrekten Datenrahmens
    - Wichtige Kontrollinformation, daher werden diese bereits nach SIFS ohne jegliches Backoff versendet

Vorlesung 12 - Beispielaufgaben

Übungsaufgabe 1:
Zeichnen Sie die Bitfolge 0 1 1 1 0 1 0 0 1 unter Anwendung der folgenden Leitungscodes:

- NRZ-Code
- NRZ-I Code
- Manchester-Code (nach IEEE 802.3)

Vorlesung 12 - Lösungen

Übungsaufgabe 1:

- Der NRZ-Code übersetzt die Nutzdaten einfach in 2 Signalpegel (z. B. 0 → Pegel 0, 1 → Pegel 1).
- Der NRZ-I-Code übersetzt eine 1 in den Nutzdaten in einen Zustandswechsel im Signalpegel, also 0 → kein Pegelwechsel im Signal, 1 → Pegelwechsel im Signal
- Der Manchester-Code (IEEE 802.3) übersetzt eine 0 in einen Pegelwechsel von +U nach -U, und eine 1 in einen Pegelwechsel von -U nach +U (jeweils gleich lange).