Netzwerk-technologien

Christian Bockermann <christian@ping.de>

Vorstellung

- Christian Bockermann
- Informatikstudent an der Universität Dortmund
- Studentische Hilfskraft bei der concentrade GmbH
- Schulungen im Rahmen des SAN-Projektes des PING e.V.
- Schulungen für QuinScape GmbH

Überblick

- Das Internet
  - Mail und das World Wide Web
- Protokolle
  - Aufgaben
  - Ethernet
  - Internet Protokoll
  - TCP, UDP, ICMP

Internet - Mail und Web

- Das Internet besteht aus einer Reihe untereinander verbundener Netzwerke
- Diese Netzwerke gehören Firmen, Providern, Universitäten und anderen Einrichtungen
- Diese Netzwerke bestehen aus einer Vielzahl verschiedener einzelner Rechner
- Die einzelnen Rechner bieten unterschiedliche Dienste an (Server)

Internet

DFN
(Forschungsnetz)

Router

Internet-Provider

Router

Web-Server
Mail-Server

Einwahl-Server

Heim-Rechner

Universität

Router

Web-Server
www.universität.de

Mail-Server

File-Server

Internet - Mail und Web

- Server stellen bestimmte Funktionen (Dienste) bereit
- Ein Webserver bietet Web-Seiten an, die aus HTML-Text bestehen und von Browsern dargestellt werden
- Ein Mail-Server verschickt E-Mail, die aus Adressat, Absender und Text bestehen an andere Mail-Server, die für den Adressat zuständig sind

Internet - Web-Server

- Beispiel für eine Browser-Anfrage an einen Web-Server (Browser rot, Server grün)

```
Trying www.ping.de...
Connected to www.ping.de.
Escape character is '^]'.

GET test.html
ERROR 404 - File not found
GET index.html
<html>
   <head>
      <title>Meine Seite</title>
   </head>
<body>
   Hier ist der Inhalt
</body>
</html>
```

Internet - Mail-Server

```
Trying mail.ping.de...
Connected to mail.ping.de.
Escape character is '^]'.

220 lilly.ping.de ESMTP
MAIL FROM:christian@ping.de
250 ok
RCPT TO:christian@ping.de
250 ok
DATA
354 go ahead
Subject: Dies ist eine Test-Mail

Dies ist der Inhalt der Test-Mail. Damit der Server
weiss, wann die Mail zu Ende ist, beendet man die Eingabe
mit einem Punkt, der in einer einzelnen Zeile steht.
.
250 ok 1082324786 qp 7315
```

Protokolle

Protokolle

- Woher wissen die Client (Browser, Mail-Programm, etc.), wie sie ihre Anfragen an die Server formulieren müssen?
- Dies steht in den Protokollen
  - http - das HyperText Transfer Protocol
  - smtp - das Simple Mail Transfer Protocol
- Diese Protokolle sind in den RFCs beschrieben

Grundlagen

- Damit Systeme miteinander kommunizieren können ist ein Regelwerk nötig, welches die Art der Kommunikation festlegt
- Dieses Regelwerk der Kommunikation definieren die Protokolle
- Verschiedene Protokolle übernehmen dabei unterschiedliche Aufgaben

Grundlagen

- Die Klassifizierung von Protokollen geschieht über das sogenannte OSI-Modell
- OSI bedeutet "Open System Interconnection" und beschreibt einen systemunabhängigen Kommunikationsstandard
- Es besteht aus 7-Schichten und wird daher auch das 7-Schichten-Modell genannt

Protokolle

Anwendungsschicht	FTP,HTTP,SMTP
Darstellungsschicht	
Kommunikationsschicht	
Transportschicht	TCP,UDP,ICMP
Vermittlungsschicht	Internet-Protokoll (IP)
Sicherungsschicht	Fehlerkorrektur
Physikalische Schicht	Bitübertragung

Protokolle

- Die Aufgaben, die diese Schichten 2,3 und 4 für uns übernehmen sind :
  - Schicht 2 stellt die zur Übertragung verwendete Hardware dar (z.B. Ethernet)
  - Schicht 3 sorgt für eine Hardware-unabhängige Adressierung
  - Schicht 4 ermöglicht logische Verbindungen

Protokolle

- Grundlage des Datenaustausches zwischen verschiedenen Systemen ist eine Hardware um Signale zu übertragen
- Dazu gibt es verschiedene Ansätze
  - Ethernet (wohl am bekanntesten)
  - Token-Ring
  - ATM
  - DSL, ISDN, uvm.

Protokolle

- Grundsätzlich unterscheidet man bei der Transport-Schicht zwischen
  - verbindungslosen Protokollen, die einzelne, in sich abgeschlossene Nachrichten verschicken
  - und verbindungsorientierten Protokollen, die eine persistente (logische) Verbindung ermöglichen und somit einen Strom von Daten transportieren können

Protokolle

- Verbindungslose Protokolle eignen sich für Verzeichnisdienste und Anfragen, z.B.
  - DNS,
  - nfs

Protokolle

- Verbindungsorientierte Protokolle stellen vor der Datenübertragung eine bidirektionale Verbindung her (ähnlich wie ein Telefongespräch)
  - Verbindungsaufbau
  - Datenübertragung
  - Verbindungsabbau
- Verbindungsorientierte Protokolle benutzen verbindungslose zur Datenübertragung

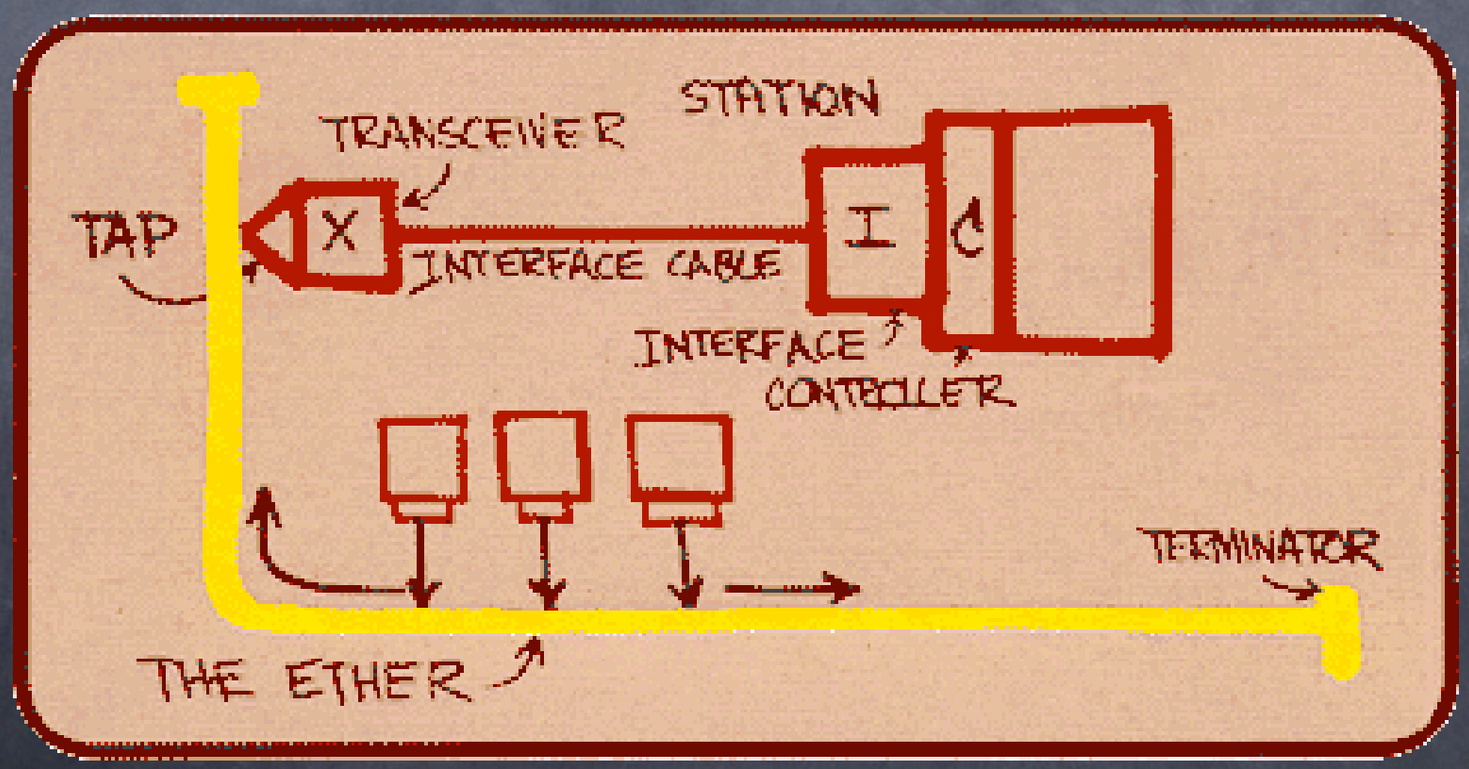
Ethernet

Protokolle - Ethernet

- Ethernet ist eine weit verbreitete Technologie um lokale Netzwerke aufzubauen
- Es ist ein definierter Standard und ermöglicht Transferraten von
  - 10 MBit/s (IEEE 802.3)
  - 100 MBit/s (IEEE 802.3u)
  - 1000 MBit/s (IEEE 802.3z/802.3ab)
  - 10 GBit/s (IEEE 802.3ae)

Protokolle - Ethernet

- Ethernet ist ein Broadcast-System
- Informationen werden durch den Bus immer an alle angeschlossenen Systeme gesandt



Protokolle - Ethernet

- Bevor ein System sendet, prüft es, ob der Bus frei ist und wartet ggf. eine kurze Zeit
- Wenn zwei Systeme gleichzeitig senden gibt es eine sogenannte Kollision
- Diese Kollisionen werden erkannt und beide Systeme warten eine zufällige Zeit lang bevor sie erneut senden

Protokolle - Ethernet

- Während ein System sendet ist der Bus also für alle anderen blockiert (zum senden)
- Damit trotzdem alle das Medium nutzen können, werden die zu sendenden Informationen in kleine Pakete gestückelt
- Diese Pakete (Frames) haben eine Länge von meist 1500 Byte
- Ethernet ist damit im Grunde ein verbindungsloses Protokoll

Protokolle - Ethernet

- Damit ein System unterscheiden kann, ob ein Paket für sich bestimmt ist, definiert Ethernet eine physikalische Adressierung
- Die verwendeten Adressen sind 6 Byte grosse MAC-Adressen

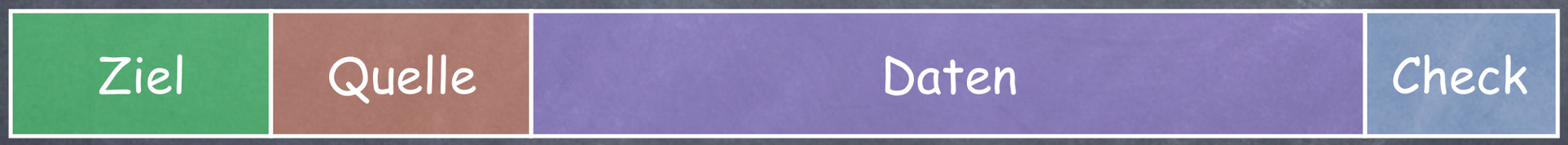
  00:4E:B2:D0:31:24
- Diese Adressen sind fest im ROM der Netzwerkkarte gespeichert

Protokolle - Ethernet

- MAC-Adressen müssen innerhalb eines Ethernet-Segmentes eindeutig sein
- Eine Netzwerk-Karte verwirft Pakete, die nicht an ihre eigene Adresse gerichtet sind

Protokolle - Ethernet

- Ein Ethernet-Frame enthält damit also nicht nur die Nutzdaten, sondern auch Informationen über das Ziel-System
- Ein Ethernet-Frame hat das folgende Format



Protokolle - Ethernet

- Es ist möglich, Netzwerk-Karten in den "promiscous mode" zu setzen
- In diesem Modus werden auch Pakete für andere Karten akzeptiert und können so mitgelesen werden
- Diese Vorgehensweise nennt man "Sniffing"
- Sniffing ist eine Möglichkeit, um evtl. vertrauliche Daten (z.B. Kennwörter) mitzulesen

Protokolle - Ethernet

- Sniffing ist allerdings auch eine gute Möglichkeit,
  - um die Funktionsweise eines Netzwerks zu erklären (Unterricht)
  - zur Fehlersuche
- Es existieren eine Reihe hervorragender Programme, die das Sniffing erleichtern
  - tcpdump (Packet-Sniffer für die Shell)
  - etherreal (Packet-Sniffer mit GUI)

Protokolle - Ethernet

- Sniffen von Netzwerk-Verkehr ist nur innerhalb eines Ethernet-Segmentes möglich
- Durch den Einsatz eines Switches läßt sich ein Netzwerk in mehrere Segmente unterteilen
- In einem ge-switch-ten Netzwerk ist das Sniffen also in dieser einfachen Form nicht möglich

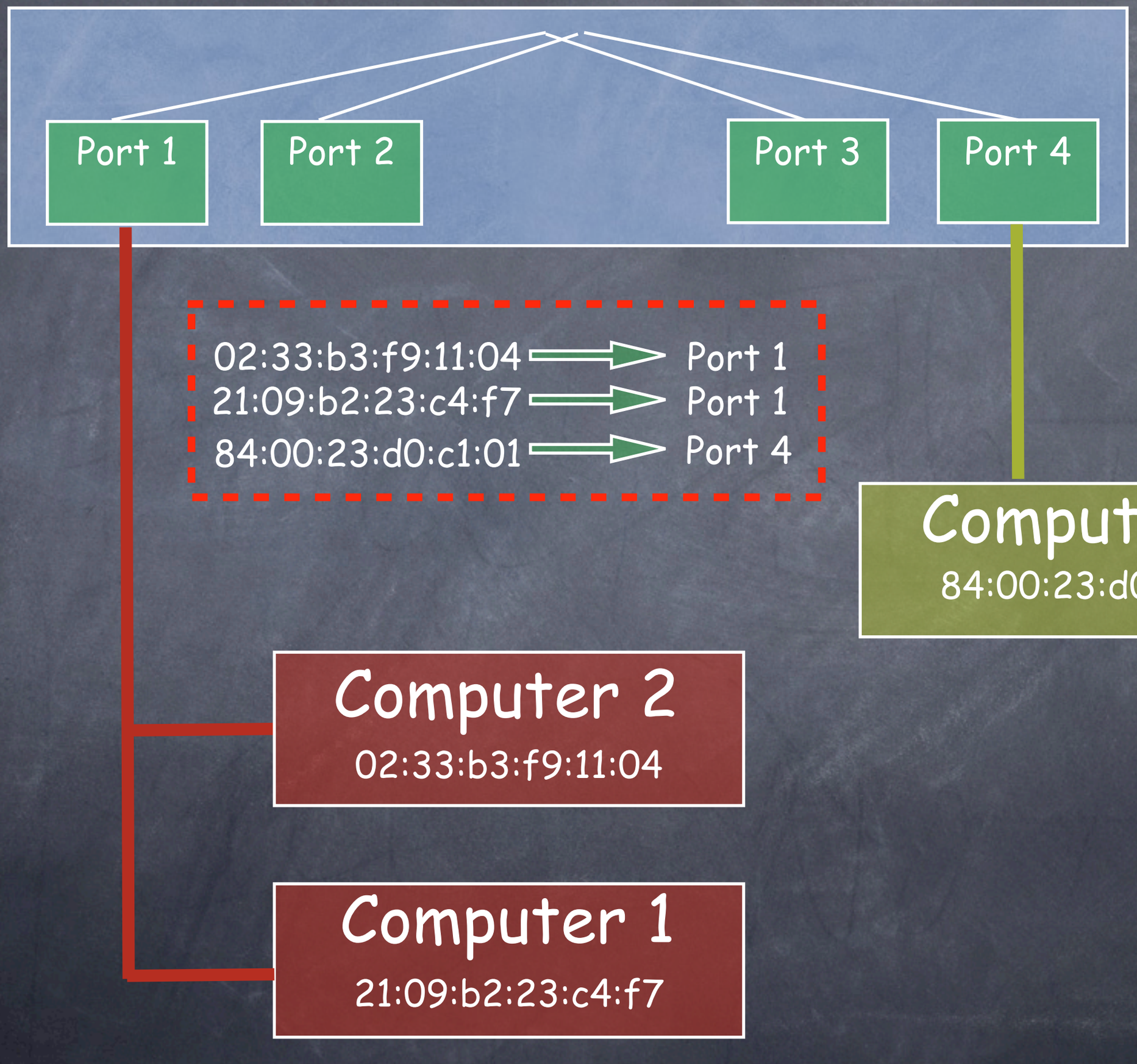
Protokolle - Ethernet

- Derzeit werden eigentlich nur noch ge-switch-te Netzwerke realisiert
- Mit dem Einsatz von Switches hat man damit eine erste Möglichkeit, die lokale Kommunikation ein wenig sicherer zu gestalten

Protokolle

- Wir haben also mit Ethernet eine Technologie, die es uns erlaubt,
  - Systeme zu adressieren (MAC-Adressen)
  - zwischen Systemen Informationen auszutauschen
- Diese Technologie ist allerdings von der verwendeten Hardware abhängig und von der Reichweite her begrenzt

Switch


Port 1
Port 2
Port 3
Port 4
02:33:b3:f9:11:04 Port 1
21:09:b2:23:c4:f7 Port 1
84:00:23:d0:c1:01 Port 4
Computer 3
84:00:23:d0:c1:01
Computer 2
02:33:b3:f9:11:04
Computer 1
21:09:b2:23:c4:f7

IP

Internet
Protocol

Protokoll - IP

- Um von der Hardware unabhängig zu werden, wurde ein abstrakteres Protokoll definiert
- Das Internet-Protokoll gehört zur Vermittlungsschicht und stellt eine Hardware-unabhängige Adressierung bereit
- Es wurde um 1977 herum entwickelt und ist in der Version 4 das Standard-Protokoll im Internet
- Eine Weiterentwicklung zur Version 6 ist abgeschlossen, wird aber noch sehr wenig genutzt

Protokoll - IP

- Das Internet-Protokoll bildet die Eckpfeiler des Internet und ist im RFC 791 spezifiziert
- Zur Aufgabe von IP gehören
  - Adressierung
  - Fragmentierung
- Es ist ein verbindungsloses Protokoll

Protokoll - IP

- Eine IP-Paket hat folgende Gestalt

Version	Länge	Service-Typ	Paketlänge			
Identifikation				DF	MF	Fragmentabstand
Lebenszeit		Transport	Kopfprüfsumme			
Senderadresse						
Empfängeradresse						
Optionen						Füllzeichen
eigentliche Nutzdaten						

Protokoll - IP

- Zur Adressierung verwendet IP 32-Bit grosse Adressen
- Diese Adressen werden als Quatuppel von 1-Byte Zahlen, durch Punkte getrennt, geschrieben
  - z.B. 172.16.0.1
- Jedes am Internet teilnehmende System benötigt eine eindeutige Adresse
- Die Adressierung ist nicht von der Hardware abhängig

Protokoll - IP

- Das Internet-Protokoll definiert also eine rein logische Netztopologie
- Die Vergabe der IP-Adressen wird international von der IANA (Internet Assigned Numbers Association) geregelt
  - die IANA verteilt die Organisation auf mehrere Unterorganisationen
  - Die in Europa zuständige Organisation ist das RIPE (Réseaux IP Européens)

Protokoll - IP

- Version
  - Die Version des IP, die wir hier behandeln ist 4
- Länge
  - Dieses Feld gibt die Länge des IP-Protokoll-Kopfes in 32-Bit-Worten an
  - Die minimale Länge beträgt 5 Worte, was auch der Normalfall ist
  - Vergrösserung durch Angabe von Optionen

Protokoll - IP

- Servicetypen
  - Mit diesem Feld ist es möglich eine Unterscheidung zwischen IP-Pakete zu treffen und bestimmte Pakete bevorzugt zu behandeln
- Paket-Länge
  - Die Länge des Paketes inklusive Protokoll-Kopf
- Identifikation
  - Eine eindeutige Identifikation (Zähler)

Protokoll - IP

- Flags (DF/MF)
  - Diese beiden Bits sind für die Fragmentierung des Paketes zuständig
  - Auf Fragmentierung gehen wir später genauer ein
- Fragmentabstand
  - Position des Paketinhaltes innerhalb der Gesamt-Nachricht in 8-Byte-Einheiten

Protokoll - IP

- Lebenszeit (TTL = Time To Live)
  - Dieses Feld gibt an, wie lange das Paket maximal unterwegs sein darf
  - Jeder Knoten verringert diesen Wert um mindestens 1
- Transport-Protokoll
  - Anhand dieses Wertes bestimmt der IP-Stack den Typ des transportierten Protokolls

Protokoll - IP

- Transport-Protokoll-Nummern (Auszug)

Nummer	Abkürzung	Bezeichnung
1	ICMP	Internet Control Message
2	IGMP	Internet Group Management
3	GGP	Gateway-to-Gateway
6	TCP	Transmission Control Protocol
8	EGP	Exterior Gateway Protocol
17	UDP	User Datagram Protocol
89	OSPF	Open Shortest Path First

Protokoll - IP

- Kopfprüfsumme
  - Prüfsumme der Felder im Protokoll-Kopf
  - Internet-Prüfsumme
    - 1er-Komplement der 16-Bit-Summe aller 16-Bit-Worte der zu prüfenden Daten
    - Einfacher-Algorithmus -> Effizienz
- Sender- und Empfänger-Adressen
  - Die bereits angesprochenen 32-Bit-Adressen

Protokoll - IP

- Optionen und Füllzeichen
  - Für bestimmte Aufgaben (Netzwerk-Management, Sicherheit) muss der Header um Optionen erweitert werden
  - Damit die Anzahl der 16-Bit-Worte immer ein Vielfaches von 4 ist (Kopflängenfeld) wird er ggf. mit Füllzeichen aufgefüllt

Protokoll - IP

- Wie bereits erwähnt ist Adressierung von IP rein virtuell
- In einem Netzwerk wird jedem Host eine IP-Adresse zugewiesen, über die er Daten senden und empfangen kann
- Eine IP-Adresse identifiziert damit nicht nur einen Host, sondern eine Verbindung dieses Hosts an ein Netzwerk

Protokolle - IP

- Die IP-Adresse eines Hosts teilt man in den Netz- und den Host-ID-Teil auf
- Diese Aufteilung geschieht mit der Netzmaske, einer ebenfalls 32-Bit langen Zahl
- Zur Berechnung der Netz-ID (Netz-Adresse) wird die IP-Adresse mit der Netzwerk-Maske bitweise UND-verknüpft

Protokolle - IP

- Durch die Angabe einer Netzwerk-Maske zerfällt eine IP-Adresse in den Netzwerk- und den Host-Teil

IP-Adresse	172.16.1.1
Netzwerk-Maske	255.255.255.0
Netzwerk-Adresse	172.16.1.0

- Die UND-Verknüpfung ist sehr effizient möglich

Protokolle - IP

- Mit Hilfe der Netzwerk-Maske und IP-Adresse lässt sich so eine Gruppe von IP-Adressen als Netzwerk zusammenfassen
- Dafür gibt es zwei grundsätzliche Notationen
  - Paarweise IP/Netzmaske:
    - 172.16.0.1/255.255.255.0
  - CIDR-Notation (Classless Inter-Domain Routing)

Protokoll - IP

- Bei der CIDR-Notation gibt die Zahl hinter dem Slash die Anzahl der führenden Einsen an, also
  - /0 = 0.0.0.0 (= 00000000.000000....)
  - /1 = 128.0.0.0 (= 10000000.000000....)
  - /2 = 192.0.0.0 (= 11000000.000000....)
  - ...
  - /24 = 255.255.255.0 (=11111111.11111111....)
  - /32 = 255.255.255.255 = (11111111.11111111....)

Protokoll - IP

- Es gibt eine Reihe von IP-Adressen, die für bestimmte Zwecke reserviert sind, dazu gehören
  - Adressen deren Netz- und Host-ID-Bits nur 1 oder nur 0 enthalten (0.0.0.0 und 255.255.255.255)
  - Adressen mit einer Host-ID von 0 oder 255
  - Adressen deren Netz-ID mit 127 beginnen

Protokoll - IP

- Desweiteren sind reserviert
  - Multicast-Adressen
    - 224.0.0.0 - 239.255.255.255
  - Für die Zukunft reserviert
    - 240.0.0.0 - 255.255.255.255

Protokoll - IP

- Zur freien Verfügung stehen (nicht geroutet)
  - Private Adress-Räume (RFC 1918)
    - 10.0.0.0 - 10.255.255.255
    - 172.16.0.0 - 172.31.255.255
    - 192.168.0.0 - 192.168.255.255
  - Automatic Assigned
    - 169.254.0.0 - 169.254.255.255

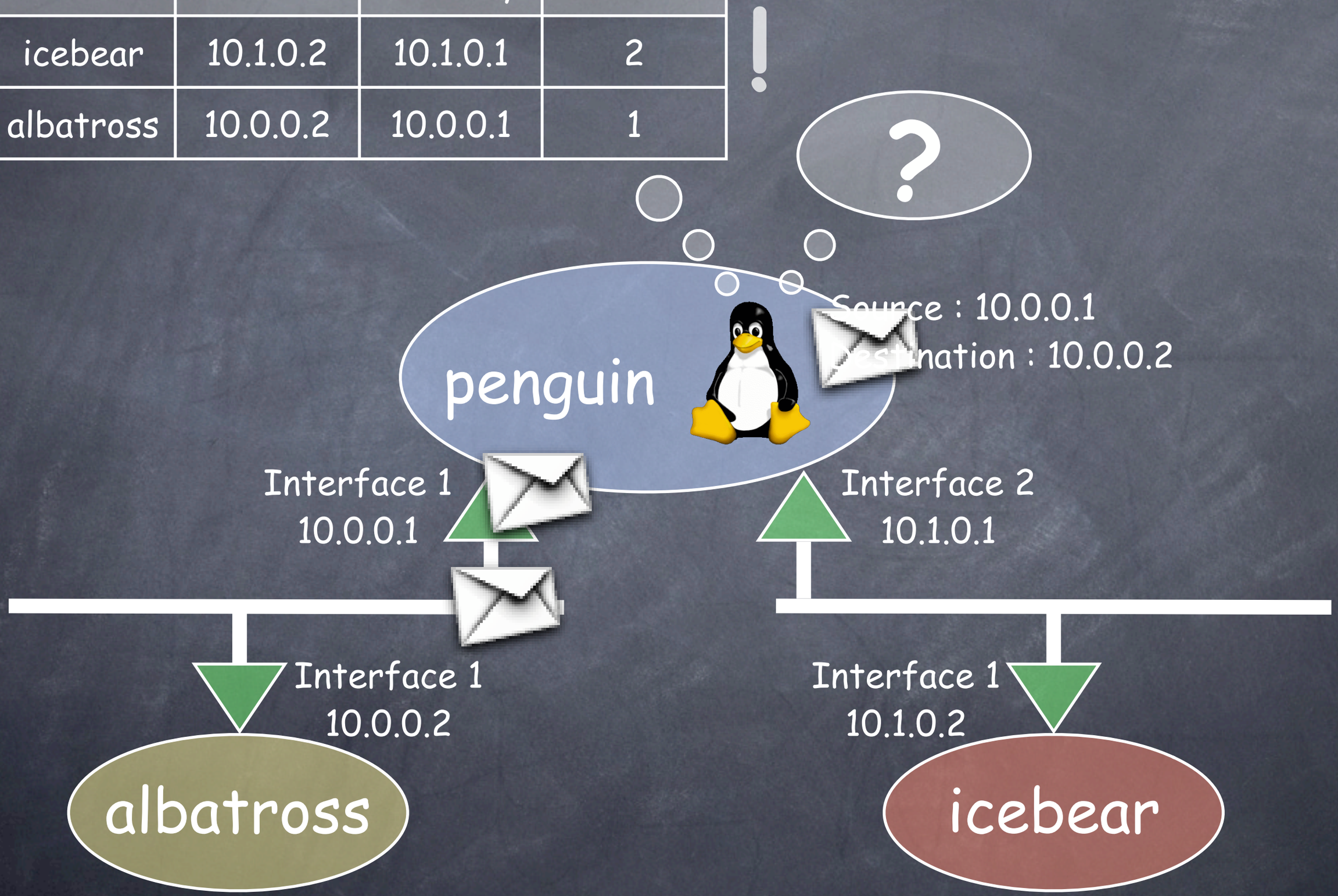
Protokoll - IP

- Mit der Zuweisung einer IP-Adresse hat ein System also eine (logische) Verbindung zu einem Netzwerk definiert
- Dieses Netzwerk stellt die Menge der Hosts dar, die das System direkt erreichen kann
- Ein System kann auch mehrere Adressen haben

Protokoll - IP

- Die Entscheidung, wie ein Paket, welches nicht an das System selbst adressiert ist, weiterzuleiten ist, bezeichnet man als “Routing”
- Dazu verfügt jeder Host im Internet über eine Routing-Tabelle, anhand der er seine Entscheidung fällt

Name	Adresse	Gateway	Interface
icebear	10.1.0.2	10.1.0.1	2
albatross	10.0.0.2	10.0.0.1	1



Protokolle - IP

- Die Routing-Tabelle ist eine einfache Liste die Einträge für verschiedene Adressen (Host- oder Netz-Adressen) enthält
- Jeder Eintrag besteht aus einer Netzwerkmaske, einem Gateway, dem Netzwerk-Interface und einigen anderen Informationen
- Anhand dieser Tabelle entscheidet ein System, was mit Paketen geschehen soll

Protokolle - IP

- Zwei Einträge in der Routing-Tabelle haben eine besondere Funktion (soweit vorhanden)
  - Die Default-Route (0.0.0.0/0)
    - Diese Netz-Adresse passt auf jede IP-Adresse und fängt somit alles auf, was nicht schon früher abgefangen wurde
  - Das Loopback-Netzwerk (127.0.0.0/8)
    - Unter diesen Adressen antwortet sich der Rechner lokal selbst (localhost = 127.0.0.1)

Protokoll - IP

- Über die Adressierung und Routing-Informationen der einzelnen Netz-Knoten lassen sich also Pfade für Rechner finden, die nicht direkt erreichbar sind
- Es existieren eine Menge unterschiedlicher Verfahren, um Routen automatisch zu setzen und zu propagieren (RiP, BGP, OSPF, usw.)
- Dies führt allerdings über den Rahmen dieser Schulung hinaus

Protokoll - IP

- Es gibt bestimmte Situationen, in denen IP-Pakete zu gross sind
  - Die Länge eines IP-Paketes ist auf 65535 Byte begrenzt (Längen-Feld im Header ist 4 Bit)
  - Da IP-Pakete von unterschiedlicher Hardware (ISDN, Ethernet, etc.) transportiert werden, kann es vorkommen, dass die IP-Pakete für die Pakete dieser unteren Transport-Schichten zu gross sind

Protokoll - IP

- Die Spezifikation von IP sieht es vor, bei Bedarf Pakete in mehrere kleinere Pakete zu zerlegen
- Diese Zerlegung wird “Fragmentieren” genannt
- Bei der Fragmentierung spielen 4 Felder des Protokoll-Kopfes eine wichtige Rolle
  - DF- und MF-Bit
  - Fragmentabstand
  - Identifikation

Protokoll - IP

- DF-Bit
  - Diese Bit (don't fragment) gibt an, dass dieses IP-Paket auf keinen Fall fragmentiert werden darf
  - Wenn es dadurch nicht weitergeleitet werden kann, wird es schlicht verworfen
- MF-Bit
  - Das MF-Bit zeigt an, dass diesem Paket weitere Pakete folgen

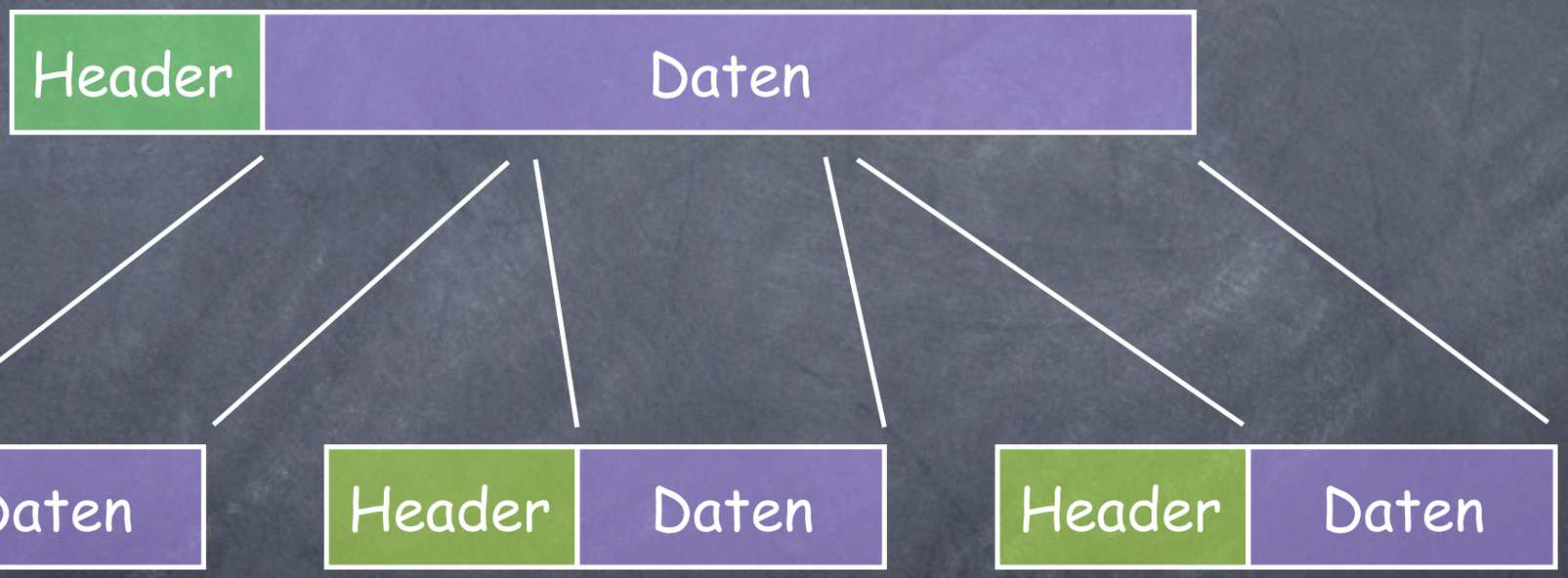
Protokoll - IP

- Identifikation
  - Alle Teil-Pakete eines fragmentierten Paketes müssen die gleiche Identifikationsnummer haben
- Fragmentabstand
  - Beim Zusammensetzen der Pakete zu einem Paket wird der Inhalt jedes Paketes an diese Stelle geschrieben
    (Abstand*8 = Anfang in Byte)

Protokoll - IP

- Beispiel:
  Maximale Paketlänge des Netzwerkes sei 128 Byte

Länge: 300 Byte
DF-Bit: 0
ID: 2354
kein Optionen



Länge: 124 Byte
Abstand: 0
MF-Bit: 1
ID: 2354

Länge: 124 Byte
Abstand: 13
MF-Bit: 1
ID: 2354

Länge: 112 Byte
Abstand: 26
MF-Bit: 0
ID: 2354

Protokoll - IP

- Einige nicht ständig verwendete Parameter sind über die Angabe von Optionen möglich
- Dadurch wurde ein möglichst kleiner Standard-Header erreicht
- Die verfügbaren Optionen wollen wir hier nicht näher betrachten

TCP

Transmission Control Protocol

OSI-Layer 4 - TCP

- Nachdem wir nun durch das Internet-Protokoll ein Vermittlungsprotokoll definiert haben, können wir Rechner adressieren
- Was fehlt ist allerdings die Möglichkeit, ein bestimmtes Programm auf dem Zielsystem anzusprechen
- Diese Möglichkeit bietet die Transport-Schicht des OSI-Modells

Protokoll - TCP

- Auch die Schicht 4 benötigt eine Adressierung, um verschiedene Programme (Services) zu unterscheiden
- Diese Adressierung geschieht über die sogenannten Ports, die in TCP und UDP vorkommen

Protokoll - TCP

- Das Transmission Control Protocol (TCP) ist ein verbindungsorientiertes Protokoll
- es verwendet 16-Bit grosse Portnummern zur Adressierung
- Zusätzlich zur Adressierung übernimmt es die Aufgaben
  - Verbindungsaufbau/-abbau
  - Fehlerkontrolle (-korrektur)

Protokolle - TCP

- Theoretisch ist es möglich TCP mit einem beliebigen Protokoll der Schicht 3 zu kombinieren
- Praktisch wird TCP allerdings immer in IP gekapselt

Protokolle - TCP

- Der TCP-Protokoll-Kopf

Sender-Port			Empfänger-Port
Sequenznummer			
Quittungsnummer			
Datenabstand		Flags	Fenstergrösse
Prüfsumme			Urgent-Zeiger
Optionen			Füllzeichen

Protokoll - TCP

- Sender-Port
  - 16-Bit-Adresse des Quell-Sockets
- Empfänger-Port
  - 16-Bit-Adresse des Ziels (Service)
- Datenabstand
  - Länge des TCP-Headers -> gibt den Startpunkt der Nutzdaten an

Protokoll - TCP

- Zur Flusskontrolle besitzt TCP Sequenz- und Quittungsnummern
  - Sequenznummer
    Dieses Feld gibt im wesentlichen die Position der gesendeten Daten im Datenstrom an
  - Quittungsnummer
    Mit der Quittungsnummer wird angegeben, bis zu welcher Position die Daten im Strom von der Gegenseite sicher empfangen wurden

Protokolle - TCP

- Prüfsumme
  - Die Prüfsumme enthält die Standard-Prüfsumme über die Daten des Paketes und einen Pseudo-Protokoll-Kopf
  - Dieser Pseudo-Protokoll-Kopf hat die Form

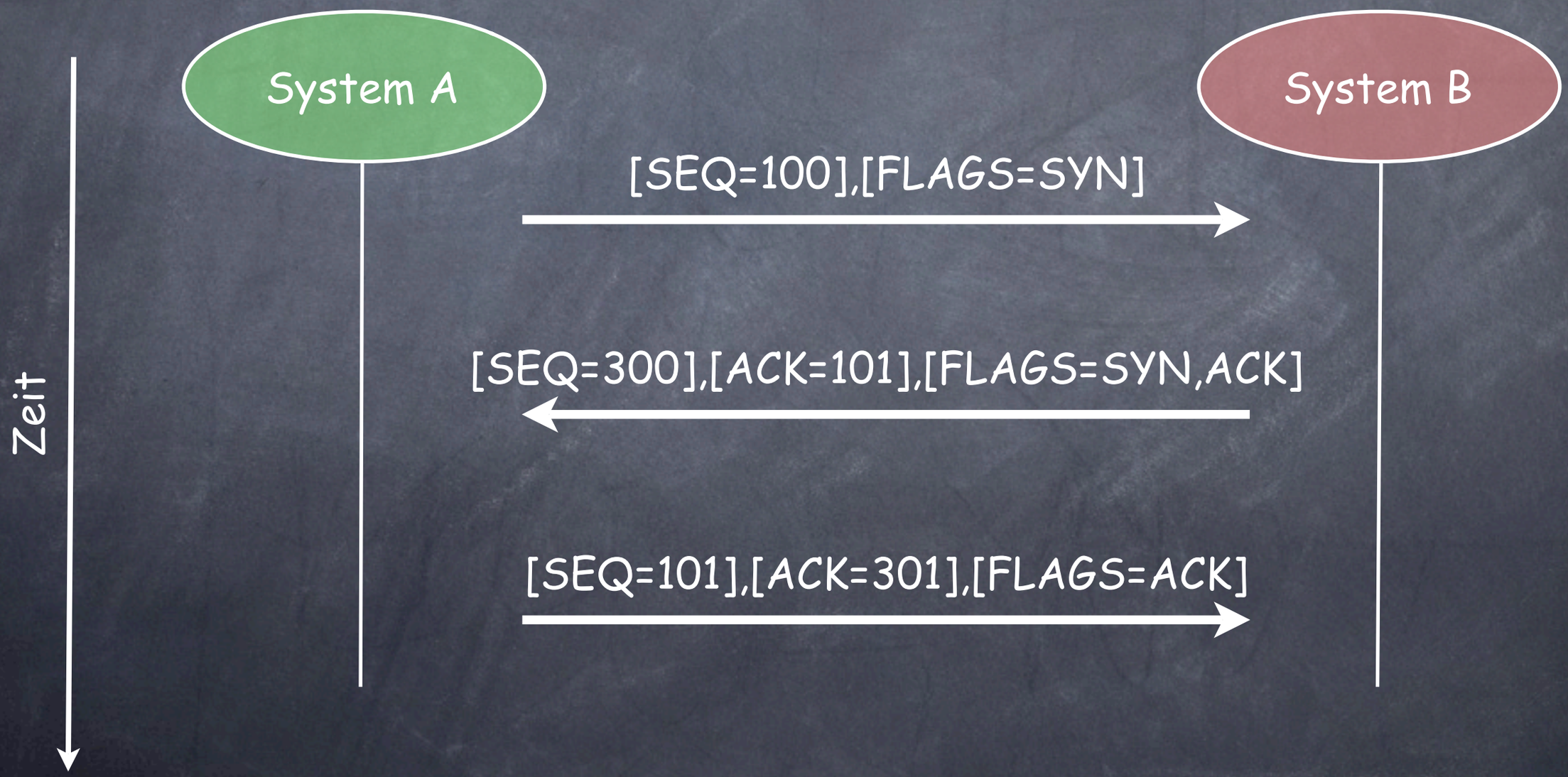
Senderadresse (IP-Adresse)		
Empfängeradresse (IP-Adresse)		
NULL	Transport-Protokoll	Länge des Paketes

Protokolle - TCP

- Zur Steuerung der Verbindung existiert im TCP-Header das Flag-Feld (6 Bit) mit den Bits
  - URG - Urgent Data Pointer gültig
  - ACK - Quittungsnummer gültig
  - PSH - Puffer-Inhalt vollständig übersendet
  - RST - Reset-Anfrage
  - SYN - Verbindungsaufbau (Aufforderung)
  - FIN - Verbindungsabbau (Aufforderung)

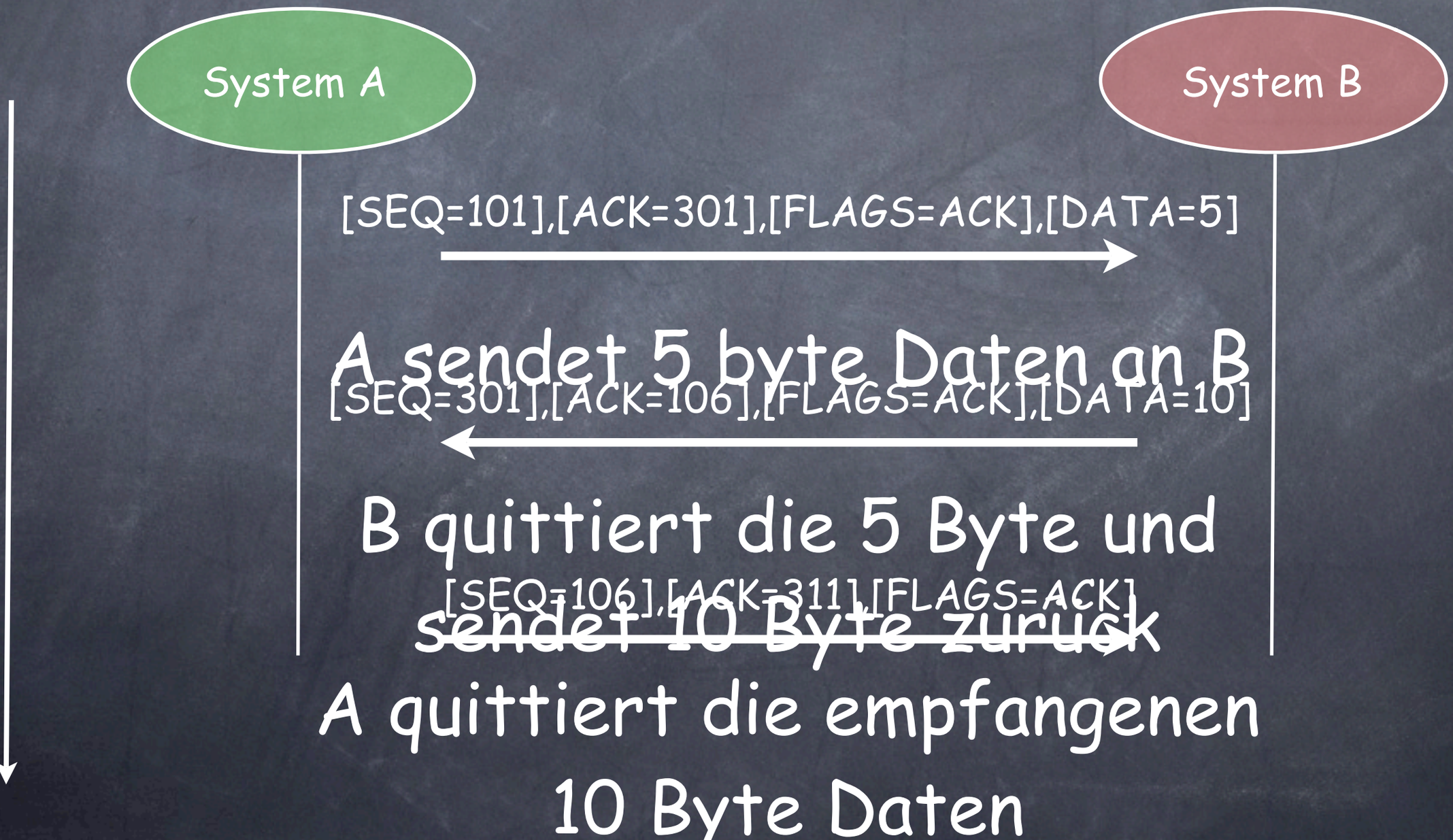
Protokolle - TCP

Verbindungsaufbau in TCP



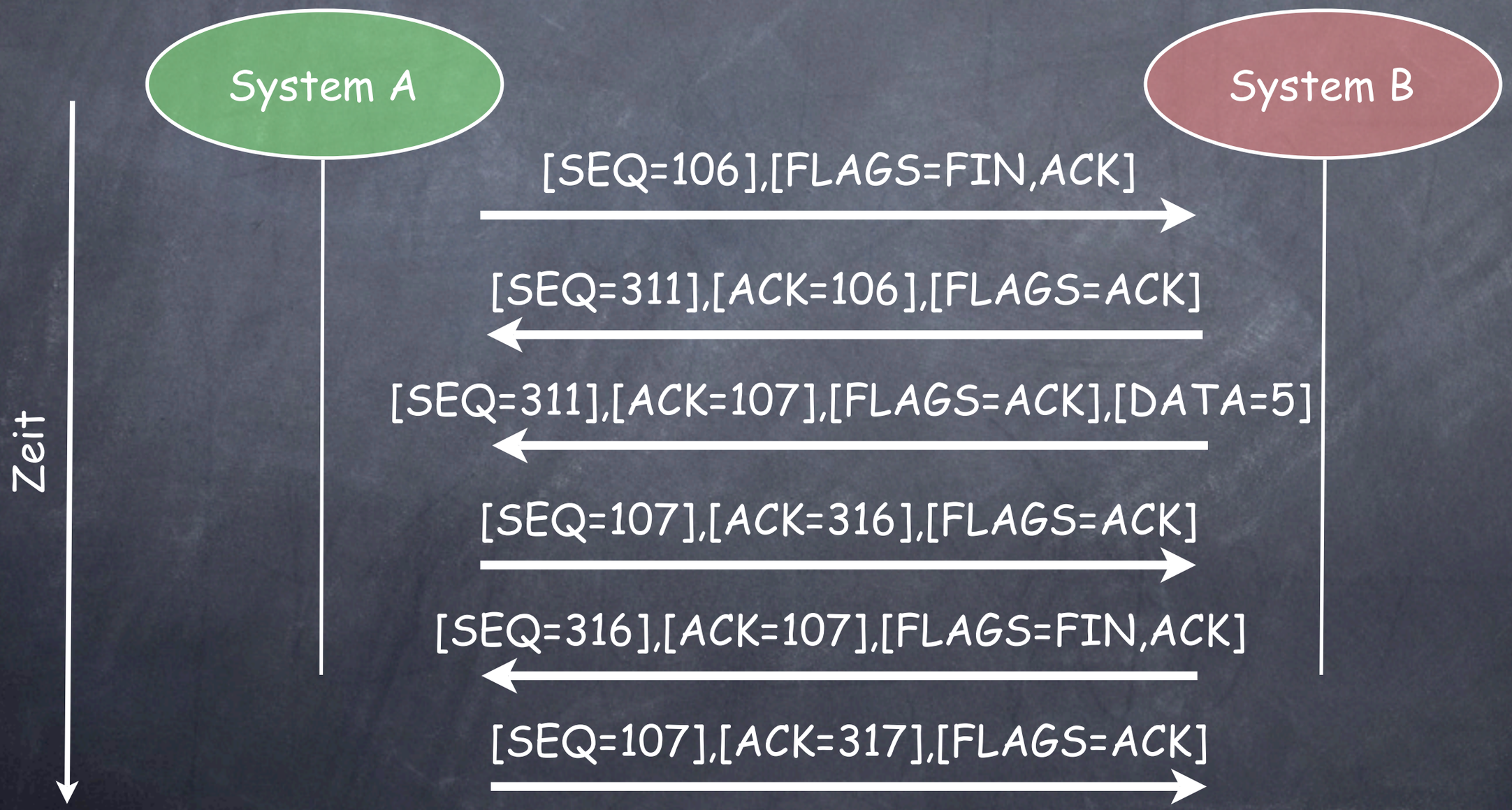
Protokolle - TCP

Datenaustausch in TCP



Protokolle - TCP

Verbindungsabbau in TCP



Protokolle - TCP

- Fenstergrösse
  - Dieses Feld gibt die Anzahl der Bytes an, die ein System senden kann, bevor es auf eine Quittung warten muss
- Urgent-Zeiger
  - Mit dem Urgent-Zeiger können wichtige Nachrichten am "normalen" Strom vorbei gesendet werden
  - Ist nur bei gesetztem URG-Bit gültig

Protokolle - TCP

- Zur Steigerung der Effizienz führen die TCP-Implementierung noch einige Timer mit sich
- Retransmission Timeout
  - Nach dieser Anzahl von Sekunden ohne Quittung wird das Paket nochmal gesendet
- Persistence Timeout
  - Für den Fall, dass die Fenstergrösse auf beiden Seiten auf 0 sinkt, gibt dieser Wert ein Timeout an, nachdem dies überprüft wird

Protokolle - TCP

- Quiet Time
  - Nachdem Verbindungsabbau ist ein Port für die hier angegebene Zeit nicht verfügbar
- Keep Alive Time / Idle Time
  - Wenn für die Zeit der Keep-Alive-Time keine Daten gesendet/empfangen wurden, wird nach Ablauf der Idle-Time die Verbindung abgebrochen
  - Diese Option ist Unix-spezifisch

UDP User Datagram Protocol

Protokoll - UDP

- Im Gegensatz zu TCP ist UDP ein verbindungsloses Protokoll
- Da es keine Angaben über Stati benötigt, kommt es mit einem sehr einfachen Protokoll-Kopf aus
- UDP wird überall dort verwendet, wo in sich abgeschlossene Nachrichten übertragen werden

Protokoll - UDP

- Die Adressierung geschieht wie bei TCP ebenfalls über 16-Bit Portnummern
- Die Portnummern von UDP und TCP sind aber voneinander unabhängig (theoretisch)
- Der UDP-Protokoll-Kopf hat folgende Gestalt

Sender-Port	Empfänger-Port
Prüfsumme	Urgent-Zeiger

Protokoll - UDP

- Länge
  - Die Länge bezieht sich auf das gesamte Datagram, inklusive Header
- Prüfsumme
  - UDP verwendet die Standard-Internetprüf-summe
  - trägt ein Sender als Prüfsumme die 0 an, wird vom Empfänger auf die Prüfung verzichtet

ICMP

Internet Control Message Protcol

Protokoll - ICMP

- Das ICMP-Protokoll ist ein verbindungsloses Protokoll, welches keine Anwendungsspezifischen Aufgaben erledigt
- Es dient der Fehler-Kontrolle und zu Diagnose-Zwecken
- Da ICMP verschiedene Nachrichten transportiert, besteht der Header aus einem Grundaufbau, wobei die Bedeutung einiger Felder wechselt

Protokoll - ICMP

- Ein ICMP-Paket hat folgenden Aufbau

Typ	Code	Prüfsumme
Verschiedenes		
IP-Kopf und 8 weitere Bytes oder Test-Daten		

Protokoll - ICMP

- Typ
  - Das Typ-Feld gibt die Art des ICMP-Paketes an

Typ	Funktion
0	Echo Reply
3	Destination Unreachable
4	Source Quench
5	Redirect (Routenwechsel)
8	Echo Request
11	Time Exceeded for Datagram
12	Parameter Problem on Datagram
13	Timestamp Request
14	Timestamp Reply

Protokoll - ICMP

- Wir wollen hier die Bedeutung einiger ICMP-Typen genauer darstellen, da diese auf allen Unixen implementiert sind
- SourceQuench
  - Diese Meldung sendet ein Gateway, wenn keine Kapazität zur Pufferung einer Nachricht vorhanden ist
  - Das sendende System muss dann die Aussenderate weiterer Nachrichten verringern

Protokoll - ICMP

- Redirect
  - Wenn ein Gateway erkennt, dass ein System ein Datagramm auch direkt an das Zielsystem senden kann, kann es einen Redirect senden
- Echo-Request / Echo-Reply
  - Mit diesem Typ lassen sich kurze Testdaten an ein System schicken, die diese unverändert zurückschickt
  - Dies dient zum Testen der Erreichbarkeit

Protokoll - ICMP

- Time Exceeded
  - Mit dieser Nachricht verständigt ein Gateway das sendende System über den Ablauf der TTL
  - Diese Nachricht wird auch versendet, wenn der Timer des Fragment-Reassemblierers abläuft
- Parameter Problem
  - Wenn der Absender eines IP-Datagrammes fehlerhafte Angaben im IP-Protokoll-Kopf macht, wird er durch diesen Typ benachrichtigt

Protokoll - ICMP

- Code
  - Der Code gibt eine Unterfunktion des Typs an z.B.
    - Typ=3 (Destination Unreachable)
    - Code=3 (Port Unreachable)
- Prüfsumme
  - Die Standard-Internetprüfsumme über die gesamte ICMP-Nachricht

Protokoll - ICMP

- IP-Protokoll-Kopf
  - Dieses Feld enthält das auslösende IP-Datagramm, sowie die ersten 8 Byte des Inhalts
  - Wurde die ICMP-Nachricht durch ein TCP oder UDP-Paket ausgelöst, kann Anhand dieser ersten 8 Byte das Anwendungsprogramm identifiziert werden
  - Für ein ECHO-Request können hier Testdaten abgelegt werden

Weiterer Überblick

- Tafelbild zu
  - DNS, Mail-Routing