Netzwerke

Inhaltsverzeichnis

1 Kapitel 1 **3**
1.1 DNS - Domain Name System 3
1.2 LAN - Local Area Network 3

2 Kapitel 2 **3**
2.1 Ethernet 3
2.1.1 Kabelspezifikationen 3
2.1.2 5-4-3(-2-1)-Regel 4
2.1.3 Ethernet Brücke 4
2.2 Aloha 5
2.2.1 CSMA / CD (Carrier Sense Multiple Access / Collision Detection) 5
2.2.2 Ethernet II 6
2.2.3 IEEE 802.3 6
2.2.4 Spanning Tree 7
2.2.5 Switching 7
2.2.6 VLAN 7

3 Kapitel 3 **8**
3.1 ARP - Address Resolution Protocol 8
3.2 ICMP - Internet Control Message Protocol 9

1 Kapitel 1

1.1 DNS - Domain Name System

Ein Domain Name System nimmt Internetadressen wie 'facebook.com' und liefert dessen IP-Adresse, damit Rechenr sich damit verbinden können. Wobei 'com'[1] eine TLD (Top Level Domain) ist. Man unterscheidet TLDs wie folgt:

gTLD (auch: genericTLDs, allgemeine TLD) Diese werden wieder in 2 Untergruppen aufgeteilt:

- **sTLD** (auch: sponsored TLD) Diese TLD werden nur an Websiten vergeben, welche bestimmte Forderungen erfüllen. '.gov'
- **uTLD** (auch: unsponsered TLD) TLD werden ohne Vorgaben vergeben. '.com, .xyz'

ccTLD (auch: country-codeTLD) TLD die zeigen aus welchem Land die Website kommt. '.de oder .us'

Beim Beispiel von facebook.com nennt man das .facebook eine Second-Level Domain, würde da noch www. stehen wäre das die Third-Level Doamin, Es können (quasi) beliebig viele Subdomains eingeführt werden. Die niedrigste Subdomain heißt hierbei Lowest-Level Domain.
Eine FQDN (Fully Qualieified Domain Name) setzt sich aus TopLevelDomain, Lowest-LevelDomain und mindestens einer Domain dazwischen zusammem.

1.2 LAN - Local Area Network

Das LAN vernetzt Geräte auf einen bestimmten (o.a. begrenzten Bereich) Normalerweise ein Haus im privaten Gebrauch oder ein Firmen-Campus etc. Dabei sind die Geräte ständig miteinander verbunden.

2 Kapitel 2

2.1 Ethernet

Jede Netzwerkkarte hat eine eigene MAC-Adresse, die benutzt wird damit Rechner sich gegenseitig Nachrichten schicken können. Die Nachrichten bei Ethernet werden auch Frames, Package und Header genannt

2.1.1 Kabelspezifikationen

Das LAN-Kabel kann je nach Spezifikation verschiedene Eigenschaften. Eine sehr frühe Version ist das 10Base5 Kabel. Damals wurde noch ein Koaxialkabel als physikalisches Medium"benutzt. Außerdem musst man ein "Dropkabel"benutzen, welches dann

[1] Eigentlich ist der Punkt rechts von der Domain. Bei der TTL wird der Punkt meistens weggelassen. Richtig heißt es beispielsweise 'com.'

einerseits an den Rechner angeschlossen wird und anderesiets an einen 'Transceiver', an welchem wiederum das Koaxialkabel angeschlossen ist. Spezifikationen:

Übertragungsrate	10Mbit
Maximale Gesamtlänge des Netzes	2500m
Maximale Segmentlänge	500m
Maximale Anzahl an Knoten	1024
Zugriffsverfahren	CSMA / CD

Ein weiterer Standard ist der 10BaseT Standard. Hier löst das Twisted Pair[2] Es gibt 4 Paare im Kabel, also 8 Pins insgesamt. An einem NIC sind Pin 1 und 2 zum senden und Pin 3 und 6 zum empfangen verantwortlich. Bei Hubs und Switches ist genau das umgekehrt da anonsten am Etherentplug beim Switch beide auf den selben Pins senden würden und beide auf den selben Pins zuhören (auf denen aber nichts gesendet wird). Möchte man jetzt zwei Rechner diretk verbinden nutzt man ein Crossover Kabel welches das Sendepaar und Empfängerpaar an einem Ende des Kabels vertauscht.

2.1.2 5-4-3(-2-1)-Regel

Wie schon erwähnt können Rechner direkt mit einem Crossover Kabel miteinander kommunizieren. Wenn das Netzt aber mehr als 2 Teilnehmer haben soll werden die Patch Kabel mit ihren Transceiver benötigt. Dabei hat sich die 5-4-3 oder auch die Repeater-Regel entwickelt. Sie gilt wenn sich Netzsegmente (10 Mbit) zu einer Baumtopologie verbinden.
Der Pfad zwischen 2 Rechnern verläuft durch maximal

5 Segemte mit
4 Repeatern verlaufen darf. Es dürfen nur an
3 Segmente aktive Endgeräte angeschlossen sein.
2 Segmente sind dabei Linksegmente (nur Repeater). Dies bildet
1 Kollisionsdomaine

2.1.3 Ethernet Brücke

Ein Hub ist eine Netzkomponente welceh Rechner miteinander verbindet und erstellt dadurch eine Kollisionsdomaine. Die verfügbare Bandbreite wird dann von den Rechnern geteilt. Eine transparent Bridge entkoppelt Kollisionsdomaine (erstellt aus einer großen, mehrere kleine Kollisionsdomaine) wodruch dann eine Broadcastdomaine entsteht. Will ein Rechner ein Paket an einen anderen Rechner senden, muss die Bridge das Paket anschauen um dann zu schauen ob das Paket in eine andere Kollisionsdomaine weitergeleitet werden muss, oder ob das Paket in der jetzigen Kollisionsdomaine bleibt. Arbeitweise von einer Bridge:

1. Bridge empfängt ein Paket

2. Die Source-Mac wird dann in die Porttabelle eingetragen.

[2]Ein Kabel, welches aus mehreren Kabelpaaren besteht die miteinander verdrillt sind

3. Ist die Destination-Mac in der Porttablle bekannt wird das Paket dementsprechen weitergeleitet (forwarding) bzw. wenn die Source-Mac und die Destination-Mac in der selben Kollisionsdomaine sind, wird gefiltert (Paket bleibt in der Kollisionsdomaine)

4. Wenn nicht, wird ein Broadcast an alle Ports (außer dem Source Port) gesendet und auf eine Antwort gewartet (flooding)

5. Sobald die Antwort eingetroffen ist, wird die Mac des Rechners in die Porttabelle eingetragen.

6. = Schritt 3

2.2 Aloha

Aloha ist ein Zugriffsverfahren für Ethernet. Aloha ist der Vorgänger von CSMA / CD. Zugriffsverfahren werden bei Etherent benötigt, damit mehrere Rechner nicht gleichzeitig auf einem Kanal senden, da sie sonst ihre Nachrichten gegenseitig verfälschen. Aloha schaut zuerst ob der Kanal frei ist und sendet eben nur dann, wenn der Kanal frei ist. Dabei hört der Rechner die ganze Zeit den Kanal ab und vergleicht die Daten im Kanal mit seinen eigenen. Sind diese nicht identisch gibt es eine Störung auf dem Kanal. Es wird angenommen das ein anderer Rechner sendet, der ebenfalls merkt dass seine Daten verfälscht wurden. Beide Rechner sendet jetzt ein sogenanntes JAM-Signal (32-bit langes, zufälliges Datenmuster). Nach dem Senden muss noch herausgefunden werden, wer jetzt senden darf, damit es nicht wieder zu einer Kollision kommt. Das Verfahren wird 'truncated binary exponential backoff' genannt. Als erstes wird eine Zufallszahl 'i' ermittelt [3] 'i' wird jetzt mit der Slottime 'T' (Die Zeit die ein Paket braucht um 2^4 mal das ganze Segment zu durchlaufen). Die Formel lautet dann

$$W = i \cdot T$$

2.2.1 CSMA / CD (Carrier Sense Multiple Access / Collision Detection)

A, B und C sind Rechner im selben Netzwerk A und C senden zum selben Zeitpunkt, das sie merken der Kanal ist frei Es kommt zur Kollision die erkannt wird. Da beide Rechner den Kanal abhören merken sie, dass das Signal verfälschtist, brechen ab Pakete zu senden und senden JAM und nutzen 'truncated binary exponential backoff' (Rechung wie bei Aloha) um nicht wieder direkt eine Kollision zu verursachen.
Eine logische '0' darf nicht als 0V gesendet werden, da ein Rechner anonsten denken könnte das der Kanal frei ist obwohl gerade gesendet wird. Zur Codierung wird der Manchester Code beutzt.
Daten werden in Ethernet zu einem Datenpaket zusammengefasst, auch 'data frame' genannt. Dieser besitzt u.a. eine Prüfsumme und Mindestlänge. Die Mindestlänge ist wichtig, da sich das Paket über das Kabel komplett ausbreiten muss. Am ende des

[3] wobei i $\leq 2^k$ und 'k' die Anzahl der registrierten Kollisionen ist, und k ≤ 10 ist
[4] 'Hin- und Rückweg'

Kabels ist ein Widerstand, der das Paket vernichtet Kommt kein signal zurück, ist die Übertragung gelungen, kommt ein Signal zurück muss ein anderer Rechner gesendet haben. Es kommt zur Kollision. Sobald aber A mit senden fertig ist, warten die anderen Rechner eine gewisse Zeit, bevor sie mit dem senden anfangen (interframe gap), um sicherzustellen, dass A auch wirklich fertig ist.

2.2.2 Ethernet II

Preamble	SFD	Dest. MAC	Source MAC	Type	Data	FCS

Preamble 7 × 01010101, wird zu Taktsynchronisation benutzt. Wird von der NIC gelöscht (7 Byte)

SFD 1 × 01010101, zeigt dass die Preamble fertig ist. Wird von der NIC gelöscht (1 Byte)

Destination Mac Die MAC Adresse an den der Frame gerichtet ist (6 Byte)

Source MAC Die MAC Adresse vom Sender (6 Byte)

Type Gibt wie die Daten in 'Data' zu interpretieren ist. Ist oft an die nächst höhere Schicht wichtig. Außerdem gilt wenn 'Type' $\leq$ 0x600, handelt es sich um ein IEEE802.3 Frame (2 Byte)

Data Inhalt des Frame (min 46 Byte aber höchstens 1500)

FCS Frame Checks Sum, beim Senden wird die FCS berechnet und gesetzt. Beim Empfangen wird diese wieder berechnet und verglichen. Sind die Werte nicht identisch, wird der Frame verworfen (4 Byte)

2.2.3 IEEE 802.3

Preamble	SFD	Dest. MAC	Source MAC	Length	Data	PAD	FCS

Preamble 7 × 01010101, wird zu Taktsynchronisation benutzt. Wird von der NIC gelöscht (7 Byte)

SFD 1 × 01010101, zeigt dass die Preamble fertig ist. Wird von der NIC gelöscht (1 Byte)

Destination Mac Die MAC Adresse an den der Frame gerichtet ist (6 Byte)

Source MAC Die MAC Adresse vom Sender (6 Byte)

Length Länge der Bits Die 'Data' benötigt

Data Inhalt des Frame (0 - 1500 Byte)

PAD Abgesehen von Preamble und SFD muss ein Frame 64 Byte groß sein. Bei IEE wird deshalb das Feld 'PAD' mit Füllbytes belegt so dass 'Data' + 'Pad' $\geq$ 46. Dabei schaut 'PAD' auf das 'Length' Feld (0 - 46 Byte)

FCS Frame Checks Sum, beim Senden wird die FCS berechnet und gesetzt. Beim Empfangen wird diese wieder berechnet und verglichen. Sind die Werte nicht identisch, wird der Frame verworfen (4 Byte)

Da IEEE 802.3 kein Type-Feld explizit angegeben hat, wird dies in

2.2.4 Spanning Tree

2.2.5 Switching

Ein Switch funktioniert wie eine Bridge, nur hat eine Bridge idR. nur 2 Ports, was heutzutage nicht mehr aussreicht. Pufferung: Bei einem Switch können mehrere Rechner miteinander kommunizieren, da ein Switch Pakete zwischenspeichern (puffer) kann. Ist das Zielsegmetn belegt speichert der Switch das Paket in den Pufferspeicher. Hier gibt es 2 Arten:

port-base memory jeder Port hat eigenen Speicher

shared memory buffering alle Ports haben einen gemeinsamen Speicher

Bei 'shared memory buffering' ist der Vorteil dass jeder Port sich einfach so viel Speicher belegt wie benötigt wird. Dies ist besonder nützlich wenn ein Switch mit verschieden Geschwindigkeiten arbeitet (100Mbit und Gigabit), da wenn ein Gerät nur 100 Mbit braucht nicht 900 Mbit verschwendet werden. Hier muss der Switch aber 'asymmetric switching' unterstüzen, da anonsten nur eine Geschwindigkeit für alle Ports benutzt werden kann (wird dann 'symmetric switching' genannt).
Desweiteren kann ein Switch auf verschiedene Arten arbeiten::

Store and Forward Die Checksum wird vom Paket überprüft. Ist diese falsch wird das Paket verworfen, ansonsten wird dieser weitergeleitet (wie bei der Bridge)

cut-trough Hier gibt es noch 2 Abspaltungen:

- **fast-forwarding** Mac wird sofort weitergeleitet sobald diese "gefunden"wurde, keine Checksum Überprüfung was die Latenz verbessert aber die Fehlerqoute der Pakete erhöht.
- **fragment-free-switching** Wenn 64 Byte ohne Kollision empfagen werden, wird das Paket erst weitergeleitet, da ab 64 Byte keine reguläre Kollsion entstehen kann.

Manchmal werden auch beide Methoden verwendet, wenn z.B. cut trough zu viele fehlerhafte Frames sendet wird auf store and forward geswitcht (wird intelligent switching genannt).

2.2.6 VLAN

3 Kapitel 3

3.1 ARP - Address Resolution Protocol

ARP wird verwendet, wenn ein Computer oder Router ein Paket an ein Gerät im eigenen Netz senden will, aber nur die Ziel-IP-Adresse kennt. Er schickt dann ein Ethernet II Frame mit dem Typ-Feld 0x608 an die Broadcast-Adresse FF-FF-FF-FF-FF-FF. Wenn der gesuchte Rechner das Paket empfängt, antwortet er mit seiner MAC-Adresse.

1	2	3	4
Hardware Type		Protocol Type	
HLEN	PLEN	Operation	
Sender Hardware Address Byte 0-3			
Sender Hardware Address Byte 4-5		Sender Internet Address Byte 0-1	
Sender Internet Address Byte 2-3		Target Hardware Address Byte 0-1	
Target Hardware Address Byte 2-5			
Target Internet Adress Byte 0-3			

Die einzelnen Felder bedeuten dabei:

Hardware Type beschreibt, über welches Mittel kommuniziert wird. Ethernet bedeutet dabei 1.

Protocol Type Mit welchem Protokoll soll später kommuniziert werden? Das gleiche wie bei Ethernet II, also 0x800 für IP.

HLEN beschreibt, wie lange eine Hardware-Adresse ist. Ist bei Ethernet immer 6.

PLEN beschreibt, wie lange eine Protokoll-Adresse ist. Ist bei IPv4 immer 4.

Operation Was wird gerade ausgeführt? 1 für Request, 2 für Response

Sender Hardware Address ist die MAC-Adresse des Senders

Sender Internet Address ist die IP-Adresse des Senders

Target Hardware Address ist die MAC-Adresse des Empfängers

Target Internet Address ist die IP-Adresse des Enpfängers.

Die gesuchten Felder werden mit Nullen gefüllt. Mit “reverse ARP” kann ein Computer, der über das Netzwerk gebootet wurde, die IP-Adresse zu seiner eigenen MAC-Adresse erfragen. Dazu ist allerdings ein Server nötig.

3.2 ICMP - Internet Control Message Protocol

ICMP-Pakete sind in IP-Pakete eingepackt (Protocol-Feld wird auf 1 gesetzt). Es wird unter anderem verwendet, um die Erreichbarkeit von Systemen im Internet zu testen (ping), Netzwerkfehler zu erkennen und um bei Zeitüberschreitungen benachrichtigt zu werden.

1	2	3	4
Type	Code	Checksum	

Die gültigen Werte für das Type-Feld sind:

0: Echo Reply (bei ping)

3: Destination unreachable (der Sender wird benachrichtigt, wenn das Ziel nicht erreichbar ist). Die Gründe dafür können im Code-Feld stehen

- **0:** net unreachable
- **1:** host unreachable
- **2:** protocol unreachable
- **3:** port unreachable
- **4:** Fragmentation needed and DF set
- **5:** source route failed (der Sender hat eine Route im IP-Header angegeben, die nicht funktioniert hat)

4: Source Quench (der Empfänger bittet den Sender, weniger Pakete zu senden)

5: Redirect (Wird von Routern verwendet, um die Netzwerkroute zu beeinflussen)

8: Echo (bei ping)

11: Time exceeded (TTL wurde unterschritten)

12: Parameter Problem, ungültiger IP Header

13: Timestamp (für Zeit-Synchronisierung)

14: Timestamp Reply (für Zeit-Synchronisierung)

Durch das Code-Feld können zusätzliche Informationen mitgegeben werden, z.B. warum die Verbindung gescheitert ist.