Netzwerke

Inhaltsverzeichnis

1 Kapitel 1

1.1 DNS - Domain Name System

Ein Domain Name System nimmt Internetadressen wie 'facebook.com' und liefert dessen IP-Adresse, damit Rechner 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

Kenngrößen von Bridges:

Filter Rate Wie viele Frames können pro Zeiteinheit gefiltert werde. Höher als bei Forwarding, da frames nur geprüft und ggf. verworfen werden

Forwarding Rate Anzahl der Frames, die pro Zeiteinheit weitergeleitet werden können. Ist Höchstanzahl erreicht, arbeitet diw Bridge in full wired speed"

Anzahl der Adresstabelleneinträge: Wie viele MAC-Adressen in Porttabelle gespeichert werden können

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

$$W = i \cdot T$$

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

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 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' ≥ 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

Um Schleifen beim Weiterleiten von Paketen zu vermeiden wurde das Spanning Tree Protocol (STP) eingeführt. Dafür geht man von einer Root-Bridge, von der aus dann andere Bridges durch eine Baumtopologie angesprochen werden können. Außerdem werden noch Pfade nach bestimmten Kriterien berechnet, die dann auch eindeutig bestimmt sind. Merkt die Route-bridge, dass eine andere Bridge eine Schleife erzeugt, wird diese in Stand-By gesendet. Die Bridge erhält weiterhin Pakete, leitet diese aber nicht weiter. Außerdem erhält sie dauernd von der Root-Bridge sogenannte (BPDU) Pakete. Wenn diese nicht ankommen wird von einem Fehler im Netz ausgegangen und die komplette Baumstruktur wird neu erstellt.

BPDU

Der Aufbau einer BPDU (Bridge Protocol Data Unit) ist wie folgt:

Protocol Identifier Wert = 0 da SPT (2 Byte)

Protocol Version Identifier Wert = 0 da SPT (1 Byte)

BPDU (Bridge Protocol Data Unit) Type: 0 : Configuration (1 Byte)

Flags z.B. wird hier angezeigt, ob sich die Topologie geändert hat (1 Byte)

Root ID Bridge Identifier der Root-Bridge (8 Byte)

Root Path Cost Summe der Kosten des Pfades von der Root-Bridge an gemessen (4 Byte)

Bridge Identifier Identifier der Bridge, die diesen Datenrahmen ausgesendet hat (8 Byte)

Port Identifier Kennzeichnung des Ports über das dieser Datenrahmen gesendet wurde (2 Byte)

Message Age Geschätzte Zeit in 1/256 Sekunde ab dem Absenden der BPDU durch die Root Bridge (2 Byte)

Max Age Zeiteinheit in 1/256 Sekunde nach der Protokoll- Informationen, die über ein Port empfangen wurden, von der Bridge gelöscht werden sollen (2 Byte)

Hello Time Zeitdauer zwischen dem Absenden von 2 aufeinander folgenden Hello-Nachrichten (besondere BPDUs) durch die Root- Bridge (2 Byte)

Forward Delay Zeitdauer, die ein Bridgeport in den Zuständen listening und learning verweilt, bevor dieser Port in den Zustand forwarding übergeht (2 Byte)

Für das Flag-Byte gelten folgenden Werte:

bits	usage
1	0 or 1 for Topology Change
2	0 (unused) or 1 for Proposal
3-4	00 (unused) or 01 for Port Role Alternate/Backup 10 for Port Role Root 11 for Port Role Designated
5	0 (unused) or 1 for Learning
6	0 (unused) or 1 for Forwarding
7	0 (unused) or 1 for Agreement
8	0 or 1 for Topology Change Acknowledgement

Aufbau des Baums

Zuerst wird die Root Bridge ermittelt. Danach wird mit Hilfe des Root Path Cost (RPC) feld (in der BPDU) emittlett, welcher Pfad zur Root-Brige der Günstigste ist. Die Kosten werden durch die Geschwindigkeit (Bandbreite) ermittelt, desto höher die Geschwindkeit desto niedriger die Kosten. Die Root-Bridge hat 0 Im Kosten Feld. Es werden BPDUs abwärts geschickt (Bridge empfängt am Root Port die BPDU) und jede Bridge addiert ihre RPC zu dem in der BPDU stehenden RPC. Bei einer Schleife empfangen 2 verschieden Bridges gegenseitig ihre RPC. Einer der beide Bridges wird in StandBy geschickt (wenn RPC unterschiedlich, dann die mit der niedrigeren RPC, bei gleicher RPC, die mit niedrigerem Bridge Identifier).

Zustände

Werden Bridges während dem Betrieb ausgewächselt oder entfernt (topologie change), könnte es zu Schleifen kommen wenn Bridge direkt vom blocking Zustand in den for-

warding Zustand gewchselt wird. Deshalb gibt es Zwischenzustände die eben zwischen blocking und forwarding liegen:

1. Nach dem Einschalten in den Zustand blocking
2. Aus dem Zustand blocking in einen der Zustände disabled oder listening
3. Aus dem Zustand listening in einen der Zustände disabled oder learning
4. Aus dem Zustand learning in einen der Zustände disabled oder forwarding
5. Aus dem Zustand forwarding in den Zustand disabled

Bei korrekter Konfiguration ist am Ende die Bridge entweder im blocking oder forwarding Zustand.

Zustand listening Protokollinformation werden ausgewertet (kann sein dass port hier in StandBy gesetzt wird wenn eine Schleife erkannt wurde). Port wartet auf ablaufen des Forward Delay Timer und wechselt in listening Zustand. Es werden keine Frames weitergeleitet. Der Forward delay timer wird zurückggesetzt.

Zustand learning Es werden immernoch keine Frames weitergeleitet aber die Bridge merkt sich Dource MAC von Paketen und am welchem Port der Frame empfangen wurde. Beim Ablauf vom Forward Delay Timer wird in Zustand forwarding gewechselt.

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

Switches lassen sich per Software in logische switches aufteilen. Ein logischer Switch entspricht dann einem VLAN. Rechner könne an verschiedenen physikalischen switches angeschlossen sein aber sich im selben logischen VLAN befinden. Nur Rechner im selben VLAN können direkt kommunizieren. Broad/Multicast gelten dann auch nur im VLAN.
Damit Switches die verschiedenen VLAN berücksichtigen können, wird der IEEE802.1Q Datenrahmen benutzt, welcher 'tagging' unterstützt. Der 4 Byte lange 'tag' befindet sich dann zwischen dem 'source mac' und dem 'type' Feld. Rechner mit selben Tag können untereinander kommunizieren, ansonsten muss ein Router verwendet werden wenn Rechenr aus 2 verschiedenen VLANs kommunizieren möchten.
Da Spanning Tree die Mac Adressen vom Switch (Bridge) benutzt um die Topologie aufzubauen, wird die Bridge-ID modifiziert. Die Priority ist anstatt 2 Byte nur noch 4 Bit (halbes Byte) groß. Die restlichen 12 Bits ist die VLAN-ID. Ein Switch hat für alle VLANs die er in seiner Datenbank hat eine nicht eindeutige MAC-Adresse die dann eben den MAC-adress Anteil in der Bridge-ID ersetzt. Für jedes VLAN wird dann das STP ausgeführt.

3 Kapitel 3

3.1 IPv4

Jedes Gerät hat eine IPv4 Adresse, jeweils 4 Byte, dargestellt durch Dezimalzahlen durch Punkte getrennt. Beispiel 141.69.1.23.

3.1.1 Adressklassen

Klasse A: Erstes Bit ist 0, die nächsten 7 Bit dienen der Netzwerkadressierung und die restlichen 24 Bit zur Geräteadressierung. (erstes Byte 0-127). Maske 255.0.0.0

Klasse B: Erste beiden Bits sind 10, die nächsten 14 Bit sind zur Netzwekadressierung und die restlichen 16 Bit zur Geräteadressierung. (erstes Byte 128-191). Maske 255.255.0.0

Klasse C: Beginnt mit 110, dann 21 Bit zur Netzwerkadressierung und 8 Bit zur Geräteadressierung. (erstes Byte 192-223). Maske 255.255.255.0

Klasse D: Beginnt mit 1110 und dient dem Multicasting. Die restlichen 26 Bit dienen der Gruppenadresse

Klasse E: Beginnt mit 1111, ausschließlich für Forschungszwecke reserviert.

3.1.2 APIPA-Adressen

Falls ein Computer keine IP von einem DHCP-Server zugewiesen bekommt, vergibt er sich selbst eine IP von 169.254.0.0-169.254.255.255. Diese Adressen werden nie von einem Router weitergeleitet.

3.1.3 Eigene Subnetze

Mit einer Netzwekmaske kann die Host-ID zusätzlich in Subnetze unterteilt werden. So kann eine skalierbarere Netzwerkstruktur geschaffen werden.

3.2 IP-Routing

Die Routing-Tabelle eines Routers oder Computers enthält folgende Einträge:

Netzwerkziel: Das Netzwerk, das über das das entsprechende Interface erreicht werden kann.

Netzwerkmaske: Zum Feststellen der Net-ID des Netzwerks

Gateway: Wohin soll geschickt werden, wenn kein direct Routing zum Ziel möglich ist?

Schnittstelle: Über welche Ausgang-Schnittstelle soll das Paket versendet werden?

Metrik: Bei mehreren zur Verfügung stehenden Pfaden wird der Weg mit der geringsten Metrik verwendet.

Wenn kein passender Eintrag in der Routing-Tabelle gefunden wird, wird automatisch die **Default Route** verwendet. Meistens 0.0.0.0 als Netzwerkziel und Netzwerkmaske

Net-Specific Routes: Routingeinträge zu Netzen und Subnetzen. Wird automatisch für alle Netze eingetragen, in denen sich der Router selbst befindet.

Host-Specific Routes: Routingeinträge zu einzelnen Hostrechnern, z.B. DNS-Rootservern

3.3 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.

3.4 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.

3.5 TCP

TCP stellt eine virtuelle Verbindung zwischen den Kommunikationspartnern her. Durch die Verbindung können Daten zuverlässig übermittelt werden. Bei TCP und UDP gibt es Ports, an die die Daten gesendet werden. *Well known Ports* gehen von 0 bis 1023 sind u. a.:

Dienst	Portnummer
http	80
https	443
SMTP (E-Mail versenden)	25
POP3 (E-Mail abholen)	110
FTP	20, 21
ssh	22

Damit der Server antworten kann, sendet der Client auch eine Portnummer als *source port* mit, an die die Antwort geschickt werden soll. Weil sich diese Ports immer ändern können, heißen sie auch dynamische Ports. Sie gehen von Port 49152 bis 65535. Zwischen den Well known ports und den dynamic ports liegen die registered Ports von 1024 bis 49151.

Eine TCP-Verbindung entsteht über einen **3way Handshake**.

1. **(SYN)** Der Client sendet ein Paket, bei dem das SYN-Feld gesetzt ist und mit welcher Sequence Number er beginnen möchte.
2. **(ACK+SYN)** Der Server antwortet dem Client mit einem Paket, bei dem die SYN + ACK Felder gesetzt sind. Außerdem teilt er dem Client die eigene Sequence Number mit.
3. **(ACK)** Der Client bestätigt die Antwort und beide bauen eine sichere Verbindung zur Kommunikation auf.

Nun kann kommuniziert werden. Der Client sendet die Daten und zählt dabei die gesendeten Bytes mit der Sequence Number hoch. Die Sequence Number ist immer ein Pointer auf das erste Byte im aktuellen Paket. Er kann nur so viele Daten wie die Window size senden, ohne auf ein acknowledgen des Servers zu warten. Der Server acknowledged ein einzelnes oder mehrere Pakete mit einem ACK-Paket. Acknowledgement Number ist dabei die als nächstes erwartete Sequence-Number des Gegenübers. Die TCP-Verbindung wird über einen **4way Handshake** geschlossen.

1. **(FIN)** Der Client will die Verbindung trennen und sendet ein FIN-Paket.
2. **(ACK)** Der Server bestätigt den Erhalt des FIN-Pakets.
3. **(FIN)** Sobald das Programm auf dem Server bereit ist, die Verbindung zu schließen, wird ein FIN-Paket an den Client gesendet.
4. **(ACK)** Der Client bestätigt den Erhalt des Pakets. Die Verbindung wird beendet.

<table>
<tr><td>1</td><td>2</td><td>3</td><td>4</td></tr>
<tr><td colspan="2">Source Port</td><td colspan="2">Destination Port</td></tr>
<tr><td colspan="4">Sequence Number</td></tr>
<tr><td colspan="4">Acknowledgement Number</td></tr>
<tr><td>data offset</td><td>reserved</td><td>flags</td><td colspan="2">window</td></tr>
<tr><td colspan="2">checksum</td><td colspan="2">urgent pointer</td></tr>
<tr><td colspan="4">options
0 oder mehr 32bit Wörter</td></tr>
<tr><td colspan="4">Daten...</td></tr>
</table>

Die Felder bedeuten dabei folgendes:

Source Port Port, von dem aus das Paket geschickt wird.

Destination Port Port, an den das Paket gesendet wird.

Sequence Number Alle übertragenen Bytes sind durchnummeriert, beginnend bei einem zufälligen Wert.

Acknowledgement Number Nur gültig, wenn die ACK-Flag gesetzt ist. Quittiert alle Pakete vom Gegenüber mit einer Acknowledgement Number = Sequence Number+1.

Data Offset gibt die Zahl der 32bit-Wörter im TCP-Header an. Min 5, wenn keine Options verwendet werden.

reserved Bits werden nicht verwendet.

Flags Es gibt folgende Flags:

- **0: CWR** Für uns irrelevant
- **1: ECE** Für uns irrelevant
- **2: URG** Das Urgent Pointer Feld enthält gültige Daten
- **3: ACK** Die Acknowledgement Nummer ist gültig
- **4: PSH** Die Daten des TCP Nutzlasten-Feldes sofort an die nächsthöhere Schicht liefern. (z.B. Telnet)
- **5: RST** Reset: Die Verbindung soll vom Rechner, der RST sendet, zurückgesetzt werden.
- **6: SYN** Wird beim Verbindungsaufbau verwendet.
- **7: FIN** Wird beim Schließen der Verbindung verwendet.

window Teilt dem Kommunikationspartner mit, wie viele Datenbytes er noch senden darf, bevor er auf eine Quittierung warten muss.

checksum Prüfsumme auf Fehler im Header

urgent pointer Pointer auf das letzte Byte, was zu den Vorrangsdaten (urgent data) gehört.

options Optionale Daten

3.6 UDP

UDP bietet einen Datagramm-Dienst für die darüberliegende Schicht an. UDP ist unzuverlässig und verbindungslos. Wird oft verwendet, wenn die Ziel-Adresse Broadcast oder Multicast ist. Der UDP-Header sieht wie folgt aus:

1	2	3	4
Source Port		Destination Port	
Length		Checksum	
Daten...			

Das **Length**-Feld bezieht sich dabei auf die Länge von UDP-Header + Daten.
UDP wird u. a. verwendet für:

Dienst	Portnummer
Trivial File Transfer Protocol (TFTP)	69
Domain Name Services (DNS)	53
Simple Network Management Protocol (SNMP)	161/162
Routing Information Protocol (RIP)	520

4 Kapitel 4

4.1 Router

Ein Router empfängt Pakete der Schicht 3 (IP-Frame) und schaut in seiner Routing Tablle nach ob wohin das Paket geschickt werden muss. Kollisionsdomaine und Broadcastdomaine enden bei einem Router. Es können aber Ausnahmen konfiguriert werden, die dann einen Broadcast weiterleiten, was beispielsweise für DHCP wichtig ist.
Cisco Router sind Rechner mit spezieller Software:

RAM/DRAM speichert Routing-Tabellen, enthält ARP-Speicher, schnelles Switching und Paketzwischenspeicher (gemeinsam genutztes RAM) sowie Warteschlangenspeicher zum Halten von Paketen. Verliert Daten bei unterbrochener Stromversorgung

NVRAM speichert BackUp/Startkonigzrationsdateien von Router, Daten überleben Stromunterbrechung

FLASH programmierbarer ROM welche idR das Betriebssytem enthält, dadurch muss nicht gelötet werden für ein Softwarupdate, bzw mehrere Versionen von können IOS gespeichert werden

ROM enthält Einschaltdiagnosefunktionen, ein Bootstrap-Programm und Betriebssystemsoftware

Software IOS (Internetwork Operating System) Betriebssystem von Cisco Routern, Router kann über Telnet konfiguriert (Routen setzen etc.) werden bzw. Informationen weitergeben die beispielsweise für Fehlersuche wichtig sein könnten

4.2 RIP - Routing Information Protocol

RIP dient zur dynamischen Erstellung von Routing Tabellen.

4.2.1 Distanzvektoralgorithmus

RIP benutzt den Distanzvektoralgorithmus um die 'schnellste' Route von einem Router zum anderen anzugeben. Die 'Geschwindigkeit' wird hierbei mit den hop counts angegeben, weniger Router hops $\Leftrightarrow$ höhere 'Geschwindigkeit'. Router die direkt verbunden sind haben die metric 0, Router können ihre Routen an andere Router weiterleiten und der Empfänger Router erhöht dann einfach die metric[5] für jede Route um eins. Bekommt ein Router eine bessere Route als eingespeichert, so ersetzt er diese mit der besserern, bekommt ein Router eine Route die gleich gut ist, wird die neue gesepeichert, wobei die alte Route bestehen bleibt.

4.2.2 Arbeitsweise

Alle 30 Sekunden (Update Timer) senden Router ihre Routen weiter als flooded broadcast (IP = 255.255.255.255, MAC = FF:FF:FF:FF:FF:FF) und bekommt den UDP port 520_{dec} (sowohl Source als auch Destination) Dabei hat jeder Router seinen eigenen Timer $\Rightarrow$ asynchron. Wenn ein Router die Routeninforamtion erhält verändert er wenn nötig seine eigene Routingtabelle

Desweiteren haben Routen auch selbst einen eigenen Timer. Läuft dieser ab wird die Route dann an andere Router gesendet, bzw. Router erwarten, dass Routen gesendet werden. Empfängt ein Router 180 Sekunden lang kein Update der Route, wird diese als unerreichbar markiert (metrix wird auf 16 gesetzt). Ausßerdem wird wieder ein Routing update gesendet (außerhalb des 30 Sekunden Zeitfenster), Das sogennante 'triggered update'. Dies wird allgemein ausgelöst, wenn sich in einer Route die metric ändert und es werden hier auch nur die geänderten Routen an die Router gesendet.
Wird nach weiteren 120 (Bei Cisco 240) Sekunden (Flush Timer) immernoch nicht die

[5] hop count $\Leftrightarrow$ metric

Route empfangen wird diese dann gelöscht (garbage collection).
Da jetzt noch die anderen Router von der falschen Route erst noch erfahren müssen, gibt es noch Holddown Tiemr (180 Sekunden). Er erhält die falsche Route in dieser Zeit damit Schleifen nicht auftauchen können.

4.3 Aufbau einer RIP Nachricht

1	2	3	4
command	version	must be zero	

command

1. RIP-Request: Router wird auffgefordert sofort einen RIP response zu senden. Enthält die Routen vom Sender und fordert auf die Routen an die Nachbarrouter zu senden.
2. RIP-Response: RIP Routenankündigun. Entweder zyklisch alle 30 Sekunden oder als triggered update.

version Hier wird die RIP-Version angegeben. Dieses Feld enthält bei RIP 1 immer den Wert 1.

must be zero Die Bits werden nicht verwendet. Sie sind auf 0 gesetzt.

Routenangabe

1	2	3	4
Adress Family Identifier		must be zero	
IP Adresss			
must be zero			
must be zero			
Metric			

Adress Family Identifier Dieses Feld gibt darüber Aufschluss, für welches Schicht 3–Protokoll die Routing-Informationen in der RIP-Nachricht gelten. Bei IP-Routing-Informationen wird dieses Feld auf den Wert 2 gesetzt.

IP Adress In diesem Feld wird die IPv4-Adresse des Netzwerkziels angegeben. Dabei kann es sich um eine Route zu einem Netz, einem Subnetz oder zu einem einzelnen Rechner (host-specific route) handeln. Findet sich hier der Eintrag 0.0.0.0, so handelt es sich um die Ankündigung der default route.

Metric In dieses Feld wird der hop count zum Netzwerkziel eingetragen. Der hop count gibt an, wie viele Router besucht werden müssen, um das betreffende Netzwerkziel zu erreichen. Der maximal erlaubte hop count liegt bei einer gültigen Route beim Wert 15. Der Wert 16 bedeutet, dass ein Netzwerkziel nicht erreichbar ist.

Probleme bei Routenausfall

Ein Router A sendet an Router B die Route zum Router C. Jetzt fällt Router C aus aber Router B denkt er hat die Route zu C und sagt Router A bescheid. Router A trägt jetzt eine Route zu C über B in sich ein. Router B merkt aber jetzt dass keine updates von der Route kommen und löscht diese Route. Router A sagt jetzt aber, dass er eine Route zu C hat und Router B trägt das auch in seine Routingtabelle ein. Das wiederholt sich bis die metric auf 16 gesetzt ist. Da dies aber einige Minuten dauern kann wurden vorgehensweisen etwickelt, um eben dies zu beschleunigen:

Split-Horizon Wenn Router A Routen vom Router B lernt, sendet er diese Routen nicht mehr zurück (an Router B). Hat Router A aber auch Routen von einem Router C sendet A die Routen von C an den Router B

Split-Horizon with poison revers Wie split Horizion nur dass antatt Routen die eigentlich nicht gesendet werden, die metric einfach auch 16 gesetzt wird. (Router A sendet die Routen von Router B an den ROuten B zurück mit metric = 16)

triggered-update Bei Topologie Änderung (metric ändert sich) wird sofort ein RIP-Update an die Nachbarn gesendet