Einführung in die Netzwerktechnik

Ein Überblick

Autoren:
Simon Ebnicher - IW3BWH
Simon Kofler - IN3FQQ

Inhalt

1. Einführung Internet
2. ISO/OSI und TCP/IP Protokollstack
3. Physical Layer: Kabel + Stecker
4. Data Link Layer: Ethernet + Switches
   -> Problem mit MAC adressen
5. Network Layer
   -> ARP
   -> IPv4 Adressierung (Klassenbasiert) + Einführung zu Subnetzmasken
   -> Motivation für CIDR, erklärung der CIDR Notation
   -> Routing
   -> Private Adressbereiche
6. Transport Layer
   -> Motivation Ports
   -> Kurz: TCP vs UDP (ganz oberflächlich)
7. Session, Presentation, Application: Zusammenfassen
8. Firewall und NAT

Einführung Internet

Internet - ein Netz von Netzen

Historisch gab es zuerst lokale Netze in Universitäten und Forschungseinrichtungen. Und schon bald begann man die ersten Daten auszutauschen und damit die Standorte zu vernetzen.

Paketvermittlung und Leitungsvermittlung

Ein leitungsvermitteltes Netz wie z.B. das Telefonnetz baut zu beginn eines Nachrichtenaustausches einen Pfad durch das Netz zwischen den beiden Teilnehmern auf und hält diese Leitung für die Dauer der Verbindung diese Leitung exklusiv aufrecht.
Ein paketvermitteltes Netz hingegen kennt keine Verbindungen, sondern leitet einfach Datenstücke im Netz weiter. Die unterschiedlichen Datenfragmente auf einem Leitungsstück können von vielen unterschiedlichen Teilnehmern sein.
Der Vorteil eines Paketvermittelten Netzes ist, dass einzelne Leitungen besser genutzt werden, da Kapazitäten (wie im Leitungsvermittelten Netz) für einzelne Teilnehmer reserviert werden, egal ob Daten ausgetauscht werden oder nicht.
Der Nachteil von Paketvermittelten Netzen ist die schlechtere Planbarkeit der Auslastungen. Es können Engpässe entstehen bei denen Pakete verworfen werden müssen.

Protokolle

Ein Protokoll ist eine Sprache, auf die sich mehrere Teilnehmer geeinigt haben um miteinander zu kommunizieren.
Das kann eine natürliche Sprache sein: “Dieser Kurs wird in der deutschen Sprache abgehalten”.
Maschinen haben ihre eigenen Sprachen. Diese sind meist sehr stark auf den Verwendungszweck zugeschnitten und eindeutig definiert.

Protokollstapel (Protokollstack)

Ein Protokollstack ist eine Sammlung von mehreren Protokollen, die übereinander geschichtet werden und definierte Schnittstellen zur jeweils oberen und unteren Protokollschicht haben. Dadurch können einzelne Schichten optimiert oder sogar ausgetauscht werden, ohne dass andere Protokollebenen angepasst werden müssen. Beispielweise könne IP Pakete problemlos über WLAN oder Ethernet übertragen werden ohne, dass es für das IP Paket einen Unterschied macht.

ISO/OSI und TCP/IP Protokollstack

Das “ISO Open System Interconnection Model” und das “Transmission Control Protocol und Internet Protocol” sind zwei Protokollstapel. Durchgesetzt hat sich TCP/IP, oder manchmal auch einfach “Internetprotokoll”. Als OSI erstellt wurde, war TCP/IP bereits im Einsatz und das ISO/OSI Modell blieb dadurch ein hauptsätzlich theoretisches Konstrukt. Das heutige Internet verwendet fast ausschließlich TCP/IP.

<table>
<tr><th>Schicht</th><th>ISO/ISO</th><th>TCP/IP</th><th>Beispiele</th></tr>
<tr><td>7</td><td>Anwendung</td><td rowspan="3">Anwendungen</td><td rowspan="3">DNS, HTTP, FTP, SMTP, POP, IMAP, Telnet, SSH, SMB/CIFS, NFS, SIP, NTP,</td></tr>
<tr><td>6</td><td>Darstellung</td></tr>
<tr><td>5</td><td>Sitzung</td></tr>
<tr><td>4</td><td>Transport</td><td>Transport</td><td>TCP, UDP, TLS</td></tr>
<tr><td>3</td><td>Vermittlung</td><td>Internet</td><td>IPv4, IPv6, ICMP</td></tr>
<tr><td>2</td><td>Sicherung</td><td rowspan="2">Netzzugang</td><td rowspan="2">Ethernet, Token Ring, IPoAC,
WLAN, ARP, AX.25</td></tr>
<tr><td>1</td><td>Bitübertragung</td></tr>
</table>

Schicht 1 - Bitübertragung (Physical Layer)

Hier werden die elektrischen und mechanischen Eigenschaften einer Verbindung definiert und die Übertragung von Bits zu ermöglichen. Darunten fallen z.B. die Definition von Steckern und Anschlüssen, elektrischen Pegeln, Modulationsverfahren und Codierungen.

Schicht 2 - Sicherungsschicht (Data Link Layer)

In diese Schickt fallen alle Verfahren um die weitgehend einwandfreie Übertragung zu gewährleisten. Dazu gehört das Erstellen und Mitschicken von Prüfsummen (Kanalcodierung). Damit können fehlerhafte Blöcke beim Empfänger erkannt und verworfen werden, oder sogar korrigiert werden.
Die ebenso dazugehörende Datenflusskontrolle steuert den Zugriff auf den Datenkanal damit mehrere Geräte nicht gleichzeitig senden (z.B. bei einer Bustopologie oder beim WLAN). Ein Beispiel für Datenflusskontrolle ist CSMA/CD (Carrier Sense Multiple Access / Collision Detect).

Schicht 3 - Vermittlungsschicht (Network Layer)

Bei Leitungsvermittelten Netzen kümmert sich die Vermittlungsschicht um den Aufbau der Verbindung durch das Netz. Bei Paketvermittelten Netzen um das Weiterleiten der Pakete. Dazu muss jeweils der korrekte Weg durch das Netz bestimmt werden “Routing”.
Das Routing kann entweder statisch (von einem Mensch) eingestellt werden, oder automatisch mit Hilfe von Algorithmen und Protokollen erfolgen.

Schicht 4 - Transportschicht (Transport Layer)

Die Transportschicht kümmert sich und die Aufteilung der Daten in kleinen Pakete (Segmente), Nummerierung und die Stauvermeidung. Ebenso können verloren gegangene Pakete neu angefordert werden.
Ebenso können virtuelle Verbindungen aufgebaut werden (TCP).

Schicht 5 - Sitzungsschicht (Session Layer)

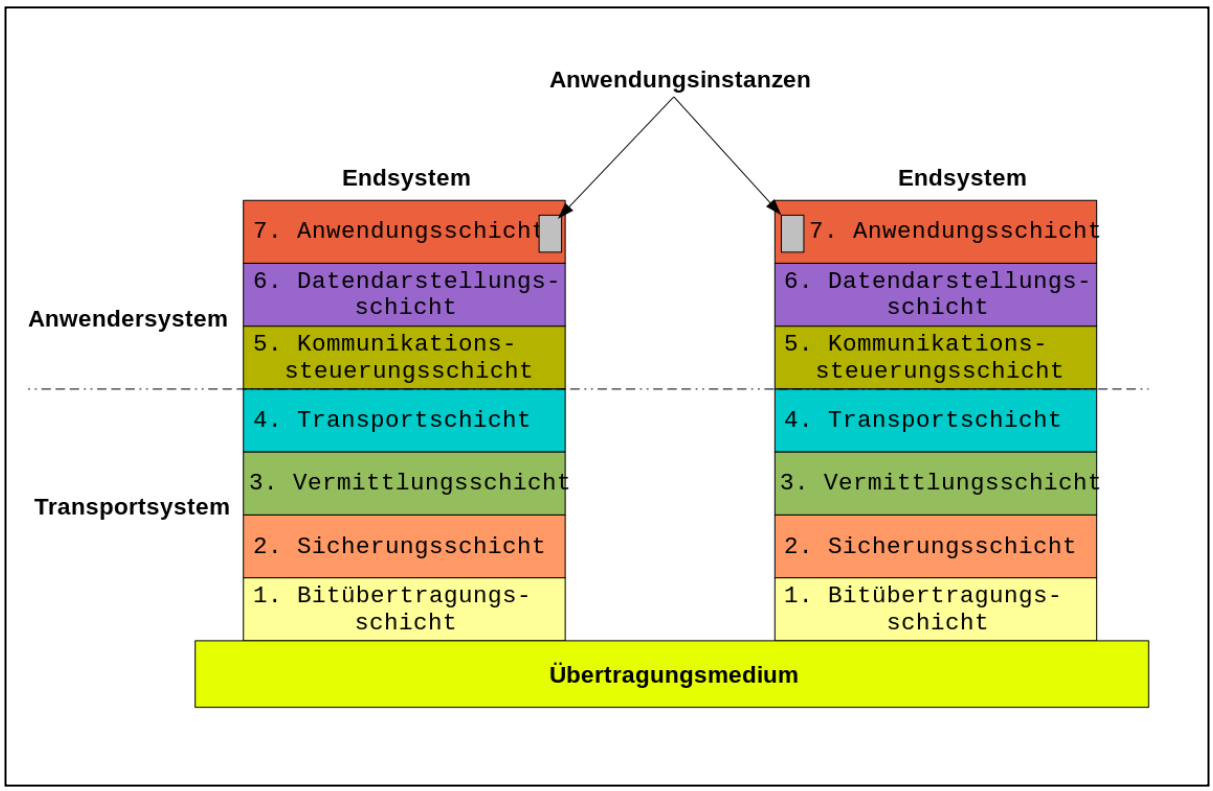
Die Sitzungsschicht bietet einen Mechanismus um abgebrochene Verbindungen wieder aufzubauen ohne, dass z.B. Datenübertragungen von vorne beginnen müssen.

Schicht 6 - Darstellungsschicht (Presentation Layer)

Die Darstellungsschicht definiert die Darstellung der Daten. Darunter fallen z.B. die verwendeten Zeichensätze ASCII, UTF-8, … wenn es sich um Menschenlesbaren Text handelt, oder auch alle anderen Arten von Datenstrukturen.

Schicht 7 - Anwendungsschicht (Application Layer)

Dienste und Anwendungen. Z.B. Browser, E-Mail Programme, Chatprogramme, …



Quelle: Wikipedia Deadlyhappen - Eigenes Werk, CC-BY-SA 4.0, https://commons.wikimedia.org/w/index.php?curid=37544652

Physical Layer

Topologien

- Punkt zu Punkt
- Bus
- Ring
- Stern
- Mesh (Vermaschtes Netz)

Ethernet (IEEE 802.3) - Kabel und Stecker

Ethernet beschreibt eine Reihe von kabelgebundenen Übertragungsmethoden.
Die Kabel/Leitungen können Koaxialkabel, Twisted Pair oder Lichtwellenleiter (Glasfaser) sein.

Die bekanntesten Übertragungsmethoden sind:

- **10BASE5 Thicknet**: 10 MBit/s über 50 Ohm Koaxialkabel mit 9,5 mm Durchmesser (RG-8/U) und N Steckern
- **10BASE2 Thinnet**: 10 MBit/s über 50 Ohm Koaxialkabel mit 5 mm Durchmesser (RG-58A/U) und BNC Steckern
- **10BASE-T**: 10 MBit/s über Twisted Pair (2 Adernpaare) mit RJ45 Steckern
- **100BASE-TX**: 100 MBit/s über Twisted Pair (2 Adernpaare) mit RJ45 Steckern
- **1000BASE-T**: 1 GBit/s über Twisted Pair (4 Adernpaare) mit RJ45 Steckern

Zugriffsverfahren

Wenn sich mehrere Teilnehmer ein Medium untereinander aufteilen müssen, kann diese Aufteilung mit verschiedenen Methoden geschehen:

- **Time Division Multiple Access (TDMA)**: die Teilnehmer belegen das Medium abwechselnd nacheinander (Zeitschlitzverfahren)
- **Frequency Division Multiple Access (FDMA)**: Das Medium “Frequenzspektrum”, beispielsweise frequenzen in einem Kabel oder die Wellenlänge des Lichts in Glasfaserkabeln wird aufgeteilt, indem jeder Teilnehmer eine eigene Frequenz zugewiesen bekommt.
- **Code Division Multiple Access (CDMA)**: Die Teilnehmer verwenden verschiedene Alphabete um miteinander zu sprechen.

WLAN (IEEE 802.11)

WLAN dient der drahtlosen Übertragung von Daten. Die Frequenzbänder für WLAN liegen bei 2,4 und 5 GHz. Es wurden im Laufe der Zeit immer wieder Anpassungen und Verbesserungen vorgenommen. Die folgende Auflistung folgt (ungefähr) der historischen Einführung des Unterstandards:

Standard	Frequenz GHz	Datenraten	Modulation	Bandbreite MHz
802.11a	5	6, 9, 12, 18, 24, 36, 54 MBit/s	OFDM	20
802.11b	2,4	1, 2, 5,5, 11 MBit/s	DSSS	22
802.11g	2,4	6, 9, 12, 18, 24, 36, 54 MBit/s	OFDM	20
802.11n	2,4 + 5	max. 600 MBit/s (4x MIMO)	MIMO-OFDM	20/40
802.11ac	5	max. 6,77 GBit/s (8x MIMO, 160 MHz Bandbreite)	MIMO-OFDM	20/40/80/160

Data Link Layer

Codierungsverfahren würden den Rahmen sprengen und werden in diesem Kurs nicht behandelt.

MAC-Adressen

“Media Access Control” Adressen sind fest in die Netzwerkchips (NIC) eingebrannte Adressen und weltweit Eindeutig.
Bei Ethernet und WLAN ist die Adressen aus 48 Bit (6 Byte) aufgebaut. Die ersten drei Bytes werden eindeutig einem Hersteller zugewiesen (OUI) und die letzten drei Bytes dienen der Durchnummerierung der Netzwerkchips.

MAC-Adressen werden laut Notationsvorschrift hexadezimal aufgeschrieben und die Bytes durch Doppelpunkt getrennt.

Darstellungen:

- 45:67:89:ab:0c:1d
- 45-67-89-ab-0c-1d

Spezielle MAC-Adressen:

- Broadcast Adresse: ff:ff:ff:ff:ff:ff

Wichtige Stolperfalle: MAC-Adressen werden zwar bei der Herstellung des Netzwerkchips fest eingebrannt. Allerdings wird die Adresse vom Betriebssystem ausgelesen und dann vom Betriebssystem weiter zur Verfügung gestellt. Das bedeutet, dass die MAC-Adresse auch geändert werden kann kein Sicherheitsmerkmal darstellt. Sicherheitssysteme wie z.B. Zugangskontrollen auf Basis der MAC-Adresse (z.B. bei WLAN) bieten nur sehr geringen Schutz und können sehr leicht überwunden werden.

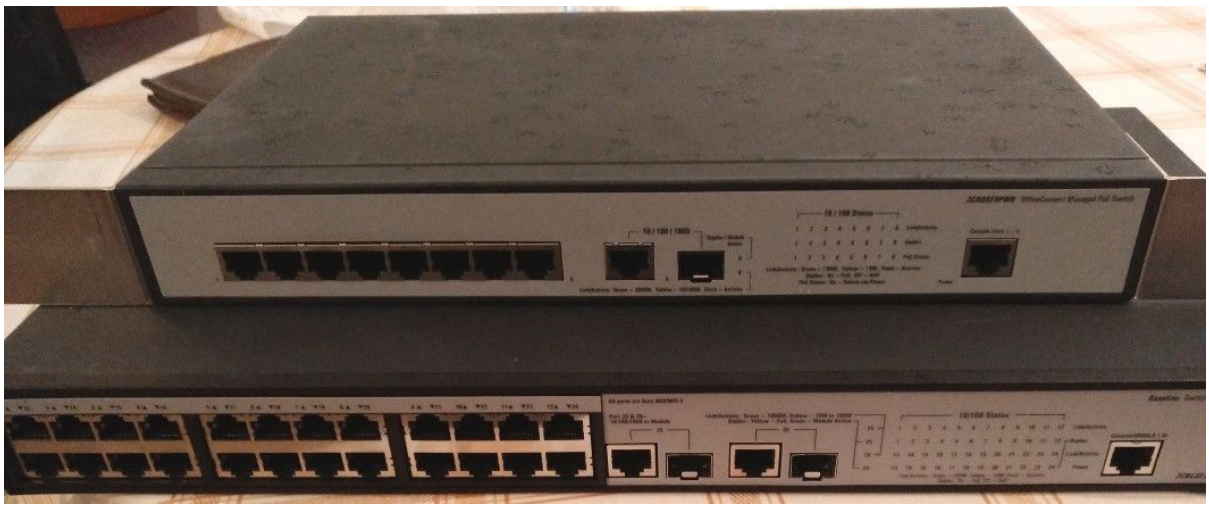
Ethernetframe

Dest MAC	Source MAC	Payload (Daten)

Switch

Ein Switch ist ein Gerät um mehrere Teilnehmer in einem Ethernetnetz zu verbinden. Ein Switch hat mehrere Anschlussports an denen je ein Netzwerkteilnehmer angeschlossen werden kann. Die Entscheidung, an welchem Port Datenframes hinausgeschickt werden, trifft der Switch anhand der Ziel-MAC-Adresse. Dazu hält der Switch eine Liste von MAC-Adressen und dem zugehörigen Switch-Port.
Zu Beginn (beim Booten) ist diese Liste leer. Aus den ankommenden Datenframes lernt der Switch, welche MAC-Adressen an welchen Ports angeschlossen sind. Hat der Switch für eine MAC-Adresse noch keine Information über den richtigen Port so wird der Frame an allen Ports hinausgeschickt. Achtung, die Liste hat eine limitierte Größe und wird vom Hersteller angegeben. Diese Zahl limitiert auch die Anzahl der Netzwerkteilnehmer in einem Netz.

Bilder von Switches:



Network Layer

IP Adressen

Warum braucht es eine weitere Ebene der Adressierung?
MAC-Adressen können in einem Netz nicht gruppiert werden. Somit müssten im Internet die Routinginformationen für jedes einzelne Netzwerkgerät vorgehalten werden. Ebenso kann man sich MAC-Adressen schlecht merken.
IP Adressen wurden eingeführt um diese Probleme lösen und sind weltweit eindeutig. Sie lassen sich gruppieren und können somit als Block z.B. einer Firma zugewiesen werden (vgl. Blöcke von Telefonnummern). Dies ist mit MAC-Adressen nicht möglich.

Aufbau von IP Adressen

Die IP Adresse ist eine binäre Zahl mit 32 Bit Länge (4 Byte). Die Notation ist in 4 Blöcke (jeweils 1 Byte oder 8 Bit) aufgeteilt und durch Punkte getrennt. Die Zahlen werden dezimal angegeben. Damit kann je eine Zahl nur Werte von 0 … 255 annehmen.
Beispiele:

192.168.10.237
8.8.8.8
44.134.190.1

Historisch wurden die Adressen in Klassen eingeteilt. Damit wurde zugleich die Größe des jeweiligen Netzes definiert:

Class A	0. 0. 0. 0	00000000.00000000.00000000.00000000
	127.255.255.255	01111111.11111111.11111111.11111111
		0nnnnnnn.HHHHHHHH.HHHHHHHH.HHHHHHHH
Netmask	255.0.0.0	11111111.00000000.00000000.00000000

Class B	128. 0. 0. 0	10000000.00000000.00000000.00000000
	191.255.255.255	10111111.11111111.11111111.11111111
		10nnnnnn.nnnnnnnn.HHHHHHHH.HHHHHHHH
Netmask	255.255.0.0	11111111.11111111.00000000.00000000

Class C	192. 0. 0. 0	11000000.00000000.00000000.00000000
	223.255.255.255	11011111.11111111.11111111.11111111
		110nnnnn.nnnnnnnn.nnnnnnnn.HHHHHHHH

Netmask	255.255.255.0	11111111.11111111.11111111.00000000

In einem Klasse C Netz haben maximal 256 Adressen platz. Die erste Adresse in jedem Netz steht immer für das Netz selbst, die letzte Adresse steht für den IP-Broadcast. Somit sind in einem Klasse C Netz effektiv nur 253 Adressen nutzbar.
Wenn beispielsweise eine Firma 400 Rechner in einem gemeinsamen Netz zusammenfassen möchte, muss dafür ein Klasse B Netz verwendet werden. Dieses hat dann jedoch 65534 (65536-2) nutzbare Adressen. Das würde bedeuten, dass die Firma 65134 Adressen für sich beansprucht, davon aber nur 400 nutzt. Dies ist eine ungewollte Verschwendung von IP Adressen.

Aufgrund dessen wurde 1993 die klassenbasierte Adressierung aufgeweicht und durch die sogenannte klassenlose Adressierung ersetzt. Diese erlaubt verschiedene Abstufungen zwischen den verschiedenen Klassen:

CIDR	Subnet Mask	Binary Mask
/8	255. 0. 0. 0	11111111.00000000.00000000.00000000
/9	255.128. 0. 0	11111111.10000000.00000000.00000000
/10	255.192. 0. 0	11111111.11000000.00000000.00000000
/11	255.224. 0. 0	11111111.11100000.00000000.00000000
/12	255.240. 0. 0	11111111.11110000.00000000.00000000
/13	255.248. 0. 0	11111111.11111000.00000000.00000000
/14	255.252. 0. 0	11111111.11111100.00000000.00000000
/15	255.254. 0. 0	11111111.11111110.00000000.00000000
/16	255.255. 0. 0	11111111.11111111.10000000.00000000
/17	255.255.128. 0	11111111.11111111.11000000.00000000
/18	255.255.192. 0	11111111.11111111.11100000.00000000
/19	255.255.224. 0	11111111.11111111.11110000.00000000
/20	255.255.240. 0	11111111.11111111.11111000.00000000
/21	255.255.248. 0	11111111.11111111.11111100.00000000
/22	255.255.252. 0	11111111.11111111.11111100.00000000
/23	255.255.254. 0	11111111.11111111.11111110.00000000
/24	255.255.255. 0	11111111.11111111.11111111.00000000

/25	255.255.255.128	11111111.11111111.11111111.10000000
/26	255.255.255.192	11111111.11111111.11111111.11000000
/27	255.255.255.224	11111111.11111111.11111111.11100000
/28	255.255.255.240	11111111.11111111.11111111.11110000
/29	255.255.255.248	11111111.11111111.11111111.11111000
/30	255.255.255.252	11111111.11111111.11111111.11111100
/31	255.255.255.254	11111111.11111111.11111111.11111110
/32	255.255.255.255	11111111.11111111.11111111.11111111

Subnetzberechnung

Anzahl an Adressen = 2 hoch (Anzahl Bits die in der Subnetzmaske 0 sind) minus 2

```
/24: 2^8   = 256  - 2 = 254
/19: 2^11  = 8192 - 2 = 8190
```

ARP

Innerhalb eines Netzes sind Geräte direkt erreichbar. Allerdings wird zur Zustellung der Daten die MAC-Adresse benötigt. Aus diesem Grund muss eine IP-Adresse einer MAC-Adresse zugeordnet werden können. Dies geschieht automatisch mit dem “Adress Resolution Protocol” (ARP).
Dabei schickt ein Gerät das die Ziel-MAC-Adresse zu einer IP-Adresse benötigt eine Nachricht an die Broadcast-MAC-Adresse (wird von allen Geräten empfangen) und das betroffene Gerät antwortet dann mit den entsprechenden Daten. Diese Daten werden in der sogenannten ARP-Tabelle gespeichert.

Routing

Liegt das Ziel außerhalb des eigenen Subnetzes, wird zur Weiterleitung der Daten ein spezielles Gerät benötigt, welcher zwischen verschiedenen Netzen vermitteln kann. Der Router.
Der Router hält die Pfade zu verschiedenen Netzen in einer Routingtabelle vor. Diese Tabelle wird entweder manuell (statische Route) oder, automatisch, durch spezielle Routingprotokolle befüllt.

Private IP-Adressen

Da IP-Adressen normalerweise bei einer Behörde beantragt werden müssen, wurden einige Bereiche zur freien privaten Nutzung reserviert und können von allen Eingesetzt werden.

Da dies aber gegen den Grundsatz der weltweit eindeutigen Adressen verstößt können diese Adressen nur lokal verwendet werden und werden nicht ins Internet weitergeleitet.

```
192.168.  0.  0 /16 (üblicherweise 256 Netze /24)
172. 12.  0.  0 /12 (üblicherweise  16 Netze /16)
 10.  0.  0.  0 /8  (üblicherweise   1 Netz  /8)
```

DHCP

DHCP, oder “Dynamic Host Configuration Protocol” ist ein Protokoll das es Netzwerkteilnehmern erlaubt automatisch eine IP Adresse und andere wichtige Parameter in einem Netzwerk zugeteilt zu bekommen. Auf diese weise wird der Aufwand zur Konfiguration der Netzwerkparameter eingespart. Besonders wichtig ist das z.B. in großen Netzwerken wo sonst eine große Anzahl von Netzwerkgeräten von Hand eingestellt werden müssten. Gleichzeitig muss beachtet werden, dass eine IP Adresse nicht versehentlich doppelt vergeben wird. All diese Probleme kann ein DHCP Server deutlich vermindern, er verwaltet Adressbereiche die er an Netzwerkgeräte ausgeben kann.
Die wichtigsten Parameter die üblicherweise von einem DHCP Server verteilt werden:

- IP Adresse
- Subnetzmaske
- Standartgateway
- DNS Server

Üblicherweise wird DHCP in Kombination mit statischen IP Bereichen verwendet.
Dabei werden Netzwerkinfrastrukturgeräte sehr oft statisch (manuell) konfiguriert (z.B. Router, Gateway, Drucker, Netzwerkspeicher, WLAN Access Point, DNS Server, NTP Server, u.s.w.), Rechner hingegen werden häufig über DHCP automatisch konfiguriert. Gerade bei mobilen Geräten (Notebooks, Smartphones) die sehr häufig das Netz wechseln ist ein DHCP Server eine Grundvoraussetzung.

Transport Layer

Beim Transport Layer wird den Verschiedenen Diensten auf einem Host (Netzwerkteilnehmer) eine Nummer zugewiesen. Der sogenannte Port. Die ist nötig um mehr als einen Dienst pro IP-Adresse zu ermöglichen.
Es gibt wieder Quell- und Ziel-Ports, über die die verschiedenen Programme auf einem Rechner oder anderem Netzwerkgerät miteinander kommunizieren.
Für verschiedene Anwendungsanforderungen gibt es unterschiedliche Protokolle. Die beiden wichtigsten sind TCP und UDP.

TCP

Das “Transport Control Protocol” ist ein verbindungsorientiertes Protokoll. Zu Beginn einer Übertragung wird die Verbindung aufgebaut. Weiters wird von TCP die fehlerfreie Datenübertragung weitgehend garantiert. Dazu werden Prüfsummen eingesetzt und fehlerhafte Datensegmente neu angefordert.
Die wichtigsten Anwendungen von TCP sind Übertragungen bei denen die fehlerfreie Übertragung von den Daten vorrangig ist.
Nachteile von TCP sind der große Protokoll Overhead und die fehlende Echtzeitfähigkeit.

UDP

Das “User Datagram Protocol” arbeitet im Gegensatz zu TCP verbindungslos. Die Pakete kommen ohne weitere Sicherungsschicht an. Die Reihenfolge und Fehlerfreiheit der Pakete ist ebenso nicht garantiert.
Der Vorteil von UDP ist, dass das Protokoll weniger Zusatzdaten generiert und dadurch besser für Echtzeitanwendunge geeignet ist. Z.B. Sprach- oder Videoübertragungen.

Firewalls

Eine Firewall ist eine geordnete Liste von Regeln die angeben, welche Pakete durchgelassen werden und welche blockiert.
Dabei können Pakete nach verschiedenen Kriterien gefiltert werden, beispielsweise Quell/Ziel MAC-Adresse, Quell/Ziel IP, Transportprotokoll (TCP/UDP) oder Quell/Ziel Port. Diese Kriterien können in jeder erdenklichen Weise kombiniert werden.

Bei Firewalls unterscheidet man zwischen zwei grundlegend verschiedenen Typen:

- eine **Stateless-Firewall** ist, wie der Name schon verrät, nicht in der Lage sich den Status von Verbindungen zu merken. Das Bedeutet konkret, dass jedes Paket einzeln, unabhängig von allen vorhergehenden behandelt wird.
- eine **Stateful-Firewall** (Stateful Packet Inspection, SPI) ist hingegen in der Lage, sich den Status von Verbindungen zu merken. Das bedeutet im Konkreten, dass Antworten auf vorhergehende Anfragen, die per Firewallregeln erlaubt worden sind, automatisch auch durchgelassen werden.

Private Netze und NAT

Wegen der begrenzten Anzahl an IP Adressen wurden gewisse IP-Bereiche für die private Verwendung reserviert. Diese Adressen werden im Internet nicht weiter geroutet und müssen deshalb nicht weltweit eindeutig sein. Verwendet werden diese IP-Adressen vor allem für private Heimnetze oder Firmennetze.

Für die private Nutzung wurden die folgenden drei Adressbereiche reserviert:
192.168.0.0/16, also die “Klasse C” Netze 192.168.0.0/24 bis 192.168.255.0/24
172.16.0.0/12, also die “Klasse B” Netze 172.16.0.0/16 bis 172.31.0.0/16
10.0.0.0/8, “Klasse A”

Der Kunde erhält dann vom Internet-Provider nur noch eine einzige öffentliche IP-Adresse, anhand welcher mit dem Internet kommuniziert werden kann. Diese ist meist auf dem (ADSL-)Router konfiguriert.
Wenn nun ein Host im privaten Netz ein Paket an einen Host im Internet (z.b. www.google.de) verschicken will, so muss die Quell-IP des Pakets auf die öffentliche IP umgeschrieben werden, damit der Zielhost antworten kann. Diesen Vorgang, den normalerweise der (ADSL-)Router übernimmt, nennt man Network Address Translation (NAT).
Sobald der NAT-Router ein Paket bearbeitet, merkt er sich in einer sogenannten NAT-Tabelle die Quell- und Ziel-IP sowie die Quell- und Zielports im Paket.
Diese Infos braucht der NAT-Router dann, um zu wissen, an wen er die eintreffenden Antworten weiterleiten muss.

Anwendungen

DNS

Das “Telefonbuch” des Internets. Das “Domain Name System” übersetzt Namen von (z.B.) Websites in IP Adressen. Ohne DNS Server müsste man sich die IP Adressen alle interessanten Websites merken.
Üblicherweise stellt der Internetprovider auch mindestens zwei DNS Server für seine Kunden bereit.
Es gibt aber auch öffentliche DNS Server:

- Google: 8.8.8.8 und 8.8.4.4
- Level 3: 4.2.2.1 bis 4.2.2.6
- OpenDNS: 208.67.222.222 und 208.67.220.220
- Hurricane Electric: 74.82.42.42

Zu beachten ist, dass es in Italien ein Internetzensur gibt die unter anderem über die DNS Server der italienischen Internetprovider durchgesetzt wird. Eine zensierte Seite wird dann auf eine Seite des italienischen Staates umgeleitet.

Ausländische DNS Server unterliegen dieser Zensur nicht (aber evt. der eines anderen Staates).

SMTP, POP, IMAP

Diese Protokolle dienen der Auslieferung von Emails. SMTP (Simple Mail Transfer Protocol) dient zum Versenden von Emails an den Mailserver und zwischen Mailservern.
POP (Post Office Protocol) und IMAP (Internet Message Access Protocol) dient dazu Emails, die auf dem eigenen Mailserver angekommen sind, abzurufen.

TELNET, SSH

Telnet und SSH (Secure Shell) ermöglichen es, mit Geräten über das Netzwerk (meist über eine Kommandozeile) zu interagieren. Zu beachten ist, dass Telnet über keinerlei Verschlüsselung verfügt und deshalb leicht abgehört werden kann. Auch die Zugangsdaten werden im Klartext übertragen. SSH hingegen baut eine verschlüsselte Verbindung auf.
Die meisten Server, beispielsweise, verfügen über keine grafische Oberfläche und werden über SSH administriert.

HTTP, HTTPS

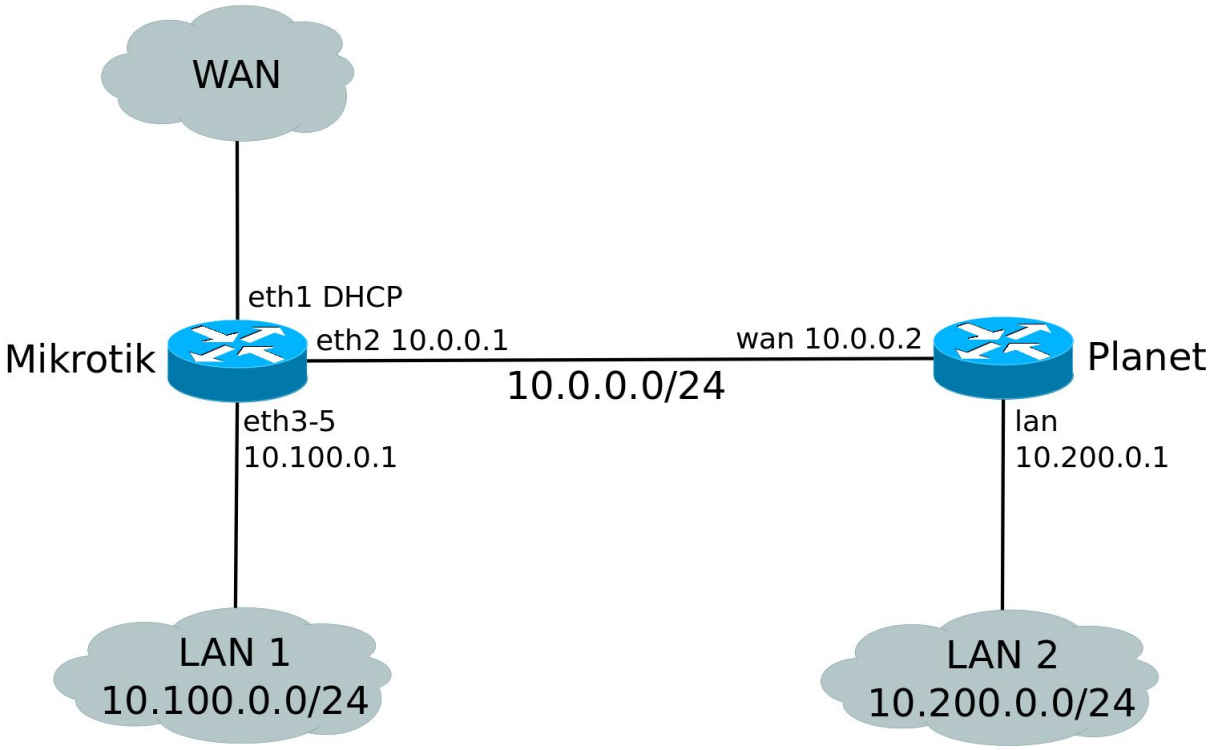
Hypertext Transfer Protocol (Secure) ist das Protokoll zum Aufruf von Websites. Mit Hypertext ist historisch “Text und Hyperlink (also Links zu anderen Textstellen und Websites)” gemeint.
HTTP ist immer unverschlüsselt. HTTPS hingegen arbeitet mit (besseren oder schlechteren) Verschlüsselungsverfahren um eine sichere Verbindung aufzubauen.

NTP

Das “Network Time Protocol” erlaubt den Abruf der aktuellen Uhrzeit und des Datums von Servern. Zudem ermöglicht es die eigenen Uhr im Rechner sehr genau mit der offiziellen Uhrzeit zu synchronisieren (im schlechtesten Fall bis auf wenige 10 Millisekunden über das Internet).
Beispiele für NTP Server:

- INRIM: “ntp1.inrim.it” (193.204.114.232) und “ntp2.inrim.it” (193.204.114.233)
- Die Server vom NTP Pool Project (pool.ntp.org)

Testnetz


WAN
eth1 DHCP
Mikrotik
eth2 10.0.0.1
wan 10.0.0.2
Planet
10.0.0.0/24
eth3-5
10.100.0.1
lan
10.200.0.1
LAN 1
10.100.0.0/24
LAN 2
10.200.0.0/24