

S e m i n a r - A r b e i t

IP - Das Internetprotokoll

vorgelegt von

MIN-Fakultät

Fachbereich Informatik

Seminar Das Internet: Architektur und Anwendungen

Leitung: Dr. Klaus-Dieter Heidtmann

Abgabedatum: 30.03.2018

Inhaltsverzeichnis

Abkürzungsverzeichnis	3
Einleitung	4
IP-Adressierung -Allgemein	4
IP-Adressierung-Verwendungszweck	5
IP-Adressierung- Aufbau einer IPv4-Adresse	6
IP-Adressierung- Netzklassen	6
Classless Inter-Domain Routing	7
IP-Adressierung IPv6	7
IP-Adressierung IPv6 Adresszuweisung	8
IP-Adressierung-IPv6-Aufteilung der Adresse	9
Dual Stack	9
Vorteile von IPv6	10
Statische und dynamische IP-Adresse	11
Vergabe von IP-Adressen	11
IP-Routing	12
IP-Routing-Algorithmus	13
ICMP	14
ICMP-Grundsätze	14
Traceroute	14
Domain Name System	14
Domain Namensraum	14
Domain Name Server	14
Auflösung eines DNS Requests	14
DNS-Angriffe	14

Abbildungsverzeichnis	15
Literaturverzeichnis und Quellenverzeichnis	15

Abkürzungsverzeichnis

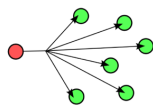
Einleitung

Im Rahmen des Seminars "Das Internet: Architektur und Anwendungen" geht es darum, den Grundaufbau und wichtige Anwendungen des Internets zu verstehen. Diese Hausarbeit orientiert sich speziell am Thema "Das Internetprotokoll". Aufbauend auf der Definition der IP-Adresse werden vertieft in die Themen der IP-Adressierung, der Aufbau und Vergleich von IPv4 und IPv6 Eingegangen.

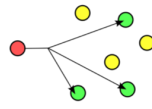
Dies ist ein kleiner Einblick in das Thema und wird in den nächsten Kapiteln ausgearbeitet.

IP-Adressierung -Allgemein

Die IP-Adresse ist eine Adresse in Netzwerken, die auf dem Internetprotokoll aufbaut. Jedes Gerät, dass an einem Netz gebunden ist, bekommt eine IP-Adresse zugewiesen. Somit sind die Geräte eindeutig gekennzeichnet und identifizierbar. Einem Rechner können eine oder mehrere IP-Adressen zugeordnet werden. Die IP-Adresse dient dazu, dass Daten vom Absender zum Empfänger versendet werden. Der Transport der Daten ist übertragbar mit der Postanschrift eines Briefumschlages. Die Datenpakete sind mit einer IP-Adresse gekennzeichnet, sodass der Empfänger eindeutig identifiziert wird. Anhand der IP-Adresse leiten die Router die Datenpakete in die entsprechenden Subnetze und werden dort weiter transportiert. Eine IP-Adresse ist nicht verbindlich einem Empfänger zuzuordnen, sondern kann auch ein gesamtes Netz kennzeichnen. Beispiele hierfür sind Broadcast oder Multicast. Unter einem Broadcast versteht man eine Nachricht, die von einem Rechner ausgelöst wird. Dabei werden die Datenpakete an alle Rechner im selben Netz verschickt und auf keinen Fall über einen Router zu jeweils anderen Subnetzen weitergeleitet. Ein Broadcast wird in der Vermittlungstechnik einer Mehrpunktverbindung zugeordnet. Wichtiger Hinweis hierbei ist, dass IPv6 keine Broadcasts mehr unterstützt. Stattdessen wird Multicasts verwendet. Bei einem Multicast handelt es sich ebenso um eine Mehrpunktverbindung. Die Nachricht wird von einem Punkt zu einer beliebigen Gruppe versendet. Der Unterschied zum Broadcast ist, dass es bei einem Multicast notwendig ist, sich vorerst beim Sender anzumelden. Beim Broadcast hingegen werden die Inhalte an alle Teilnehmer im Netz gesendet.



(a) Subfigure Bild Nr. 1



(b) Subfigure Bild Nr. 2

Abbildung 1: Broadcast und Multicast

IP-Adressierung-Verwendungszweck

Die Hauptaufgabe der IP-Adressierung besteht im Transport der Daten. Dabei werden die Daten vom Absender zum Empfänger mit Hilfe von Datenpaketen weitergeleitet.

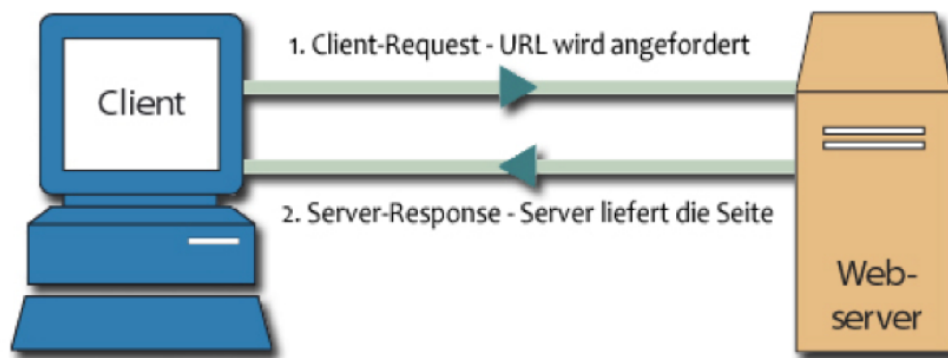


Abbildung 2: Beispiel mit einem Klienten und Webserver für den Verwendungszweck der IP-Adressierung

Beispielsweise ist ein Webserver von einem Webbrowser über die IP-Adresse erreichbar. So kann eine Kommunikation untereinander erfolgen. Dazu muss der Webbrowser bei einem Nameserver nach der zugehörigen IP-Adresse des Webserver anfragen, die einer Domain angehört. Dabei wird die URL zu einer IP-Adresse umgeformt mittels der Namensauflösung, welches im Kapitel Domain Namensraum behandelt wird. Diese IP-Adresse wird verwendet, um Daten an den Webserver zu senden.

IP-Adressierung- Aufbau einer IPv4-Adresse

Jede IP-Adresse besteht aus 4 Zahlenblöcken. Diese wird als Dezimalzahl notiert. Die interne Verwaltung ist jedoch die binäre Darstellung. Dabei belegt jeder Zahlenblock 8 Bits. Somit sind Zahlen von 0-255 darstellbar. Da jeder Zahlenblock mit 8 Bits belegt ist, besteht eine IP-Adresse aus 32 Bits und deswegen sind insgesamt $2^{32} = 4.294.967.296$ IP-Adressen darstellbar.

Beispiel:

Dezimale Schreibweise: 171.15.245.1

→ binäre Schreibweise: 10101011 00001111 11110101 00000001

Die IP-Adresse setzt sich zusammen aus einer Netzadresse und einer Hostadresse. Für die Trennung in Netz- und Hostadresse ist die Subnetzmaske verantwortlich. Diese bestimmt an welcher Stelle genau die Trennung stattfindet. Die Hostadresse bestimmt den Rechner und die Netzadresse bestimmt das Subnetz, um den Rechner letztendlich über die Hostadresse zu finden. Wenn man Datenpakete verschicken möchte, schaut man sich zunächst die Netzadresse an. Ist die Netzadresse sowohl beim Absender, als auch beim Empfänger identisch bleibt das Datenpaket im selben Subnetz und muss nicht über einen Standard-Gateway in ein anderes Subnetz mittels eines Routers weitergeleitet werden.

IP-Adressierung- Netzklassen

Netzwerke sind in verschiedene Klassen unterteilt. Die Klasse A hat eine Netzmaske von 255.0.0.0 und somit werden 8 Bits für die Netz-Adresse und 24 Bit für die Host Adresse verwendet. Insgesamt erhält man $2^{24} - 2$ Hostadressen, die darstellbar sind. Der Adressbereich geht von 0-127. Bei der Klasse B ist die Subnetzmaske 255.255.0.0. Somit werden 16 Bits für die Netzadresse und 16 für die Hostadresse verwendet. Insgesamt $2^{16} - 2$ Hosts im Netz. Der Adressbereich geht von 128-191. Bei der Klasse C ist die Subnetzmaske 255.255.255.0 und somit werden 24 Bits für die Netzadresse und 8 Bits für die Host Adresse verwendet. Durch die Netzklasse wird die Netzadresse, als auch die Hostadresse abgeleitet, da man anhand der Subnetzmaske festlegt, wie diese auszusehen haben.

Netzklasse	Präfix	theoretischer Adressbereich	Netzmaske	Netze	Hosts im Netz
Klasse A	0	0.0.0.0 – 127.255.255.255	255.0.0.0	128	16 777 216
Klasse B	10	128.0.0.0 – 191.255.255.255	255.255.0.0	16 384	65 536
Klasse C	110	192.0.0.0 – 223.255.255.255	255.255.255.0	2 097 152	256
Klasse D	1110	224.0.0.0 – 239.255.255.255	Multicast-Anwendungen		
Klasse E	1111	240.0.0.0 – 255.255.255.255	reserviert für zukünftige Anwendungen		

Abbildung 3: Aufteilung in Netzklassen

Netzklassen werden in der Praxis kaum verwendet. Aufgrund der Netzklassen wurden die meisten zur Verfügung stehenden öffentlichen IP-Adressen vergeben. Die Größe eines Netzwerkes wird anhand der Angabe der Subnetzmaske bestimmt und nicht aus der IP-Adresse und der Netzklasse.

Classless Inter-Domain Routing

Unter einem Classless Inter-Domain Routing versteht man das effiziente Nutzen des bestehenden Adressraums einer IPv4-Adresse. Man möchte erreichen, dass die Routingtabellen reduziert werden, sodass der bestehende Adressraum effizient genutzt werden kann. Damit benötigt man die Netzklassen nicht mehr, da die IPv4-Adressen nicht mehr zu einer Klasse zugeordnet werden müssen. Zudem ist die Präfixlänge frei wählbar, sprich man erkennt, wie viele IPv4-Adressen für Hosts im Netzwerk verfügbar sind.

IP-Adressierung IPv6

Der Grund, weshalb IPv6 eingeführt wurde, ist, dass der IPv4 Adressraum in Zukunft ausgebraucht wird. Der IPv6 Adressraum besteht aus 128 Bits. Somit können $2^{128} = 340.282.366.920.938.463.463.374.607.431.768.211.456 \approx 3,4 \cdot 10^{38}$ ca. 340 Sextillionen IP-Adressen dargestellt werden. Die Dezimaldarstellung ist:

Die Adresse setzt sich zusammen aus 8 Blöcken mit jeweils 16 Bits. Die Notation dieser Adresse ist eine Hexadezimalzahl. Beispielsweise könnte diese so aussehen "2001:0db8:85a3:0000:0000:8a2e:0370:7344". Man verwendet die Hexadezimaldarstellung, weil die Dezimaldarstellung unübersichtlich wäre aufgrund der langen Adresse, die sich deshalb ergibt. Damit es übersichtlicher wird, werden zwei Oktette der Adresse zusammengefasst, sodass man insgesamt 8 Blöcke mit jeweils 16 Bit hat. Diese werden mit einem Doppelpunkt getrennt. Jeweils vier Bits der IPv6 Adresse stellen eine Hexadezimalzahl dar.

Die ersten 32 Bits der IPv6 Adresse bekommt der Internetprovider von der Regional Internet Registry (RIR) zugewiesen. Diese werden in weitere Subnetze aufgeteilt. Der Internet Provider ist für die Zuteilung der Länge verantwortlich. Eine minimale Zuteilung eine /64-Netzes ist vorgeschrieben. Die erste Hälfte mit 64 Bit einer Adresse ist das Netzsegment und die restlichen 64 Bits gehören zum Interface-Identifizier. Die beiden zusammen bilden die IPv6-Adresse. Üblicherweise wird der Interface-Identifizier aus der Mac-Adresse der Schnittstelle bestimmt werden. Ein Beispiel hierfür ist: 2001:0db8:85a3:08d3:1319:8a2e:0370:7347/64.

IP-Adressierung-IPv6-Aufteilung der Adresse

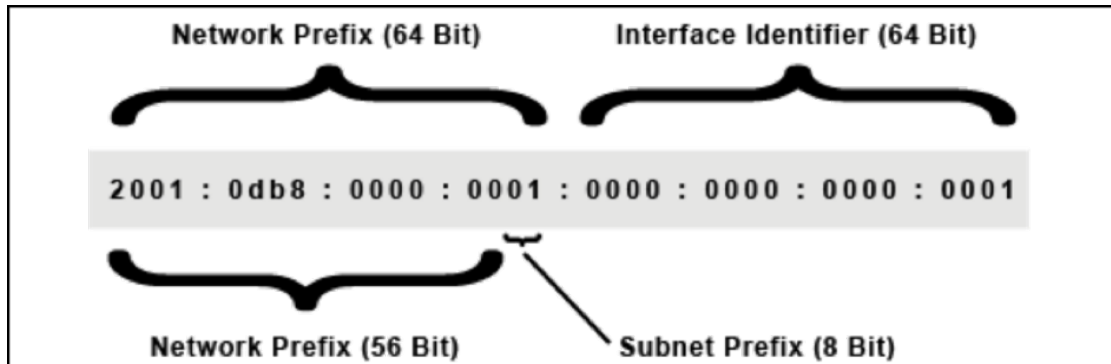


Abbildung 4: IPv6-Aufteilung der Adresse

Dual Stack

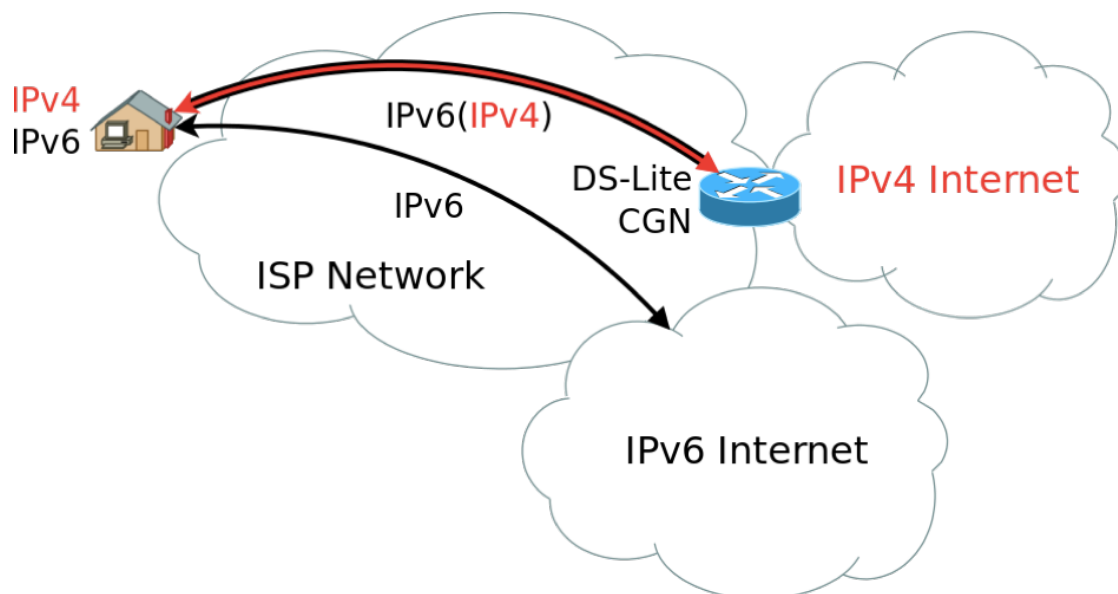


Abbildung 5: Dual Stack

Zurzeit besteht ein geringer Bestand an IPv4 Adressen. Wenn diese aufgebraucht sind, ist es notwendig auf IPv6 zurückzugreifen. Somit kann es zu einem Wechsel kommen,

wenn der bestehende Adressbereich nicht effizient genutzt wird. Die Kunst hierbei ist, dass einerseits nicht nur die Einführung von IPv6 in Vordergrund steht, sondern gleichzeitig auch, dass IPv4 zur selben Zeit betrieben wird. Diesen Zustand bezeichnet man als "Dual Stack". Anhand der Abbildung wird im Folgenden auf die Funktionsweise eingegangen.

Der DS-Lite besitzt einen Internet-Anschluss, der einen öffentlichen IPv6-Präfix erhält. Damit ist er von überall aus erreichbar. Aus dem bestehenden Präfix weist der Router allen Geräten im selben Netz öffentliche IPv6-Adressen zu, die sich ins Internet verbinden möchten. Diese werden mit dem IPv6 Internet verbunden. Der DS-Lite-Anschluss erhält im Allgemeinen keine öffentlichen IPv4-Adressen. Jedoch wird ihm eine private IPv4 Adresse zugeteilt, welches jedoch nicht vom Internet aus erreichbar ist. Vom Internet sind nur IPv6 Adressen erreichbar. Die privat adressierten IPv4-Pakete werden vom Provider zu einer öffentlichen IPv4-Adresse maskiert. Die Maskierung bezeichnet man als Carrier Grade NAT (CGN). Der DSL-Router funktioniert im Prinzip genauso. Dieser besitzt eine öffentliche IPv4-Adresse und weist allen Geräten im Netzwerk private Adressen zu.

Man muss sowohl IPv4 als auch IPv6 betreiben, weshalb der Dual Stack bedeutend ist. Dieser Betrieb muss solange erfolgen, bis alle Geräte mit IPv6 umgehen können. Es gibt viele Endgeräte, die kein IPv6 unterstützen und erst durch entsprechende Komponenten ausgetauscht werden müssen. Außerdem ist der Markt für IPv6 nicht groß genug und eine Entwicklung als auch der Aufwand, die IPv4 Produkte auf IPv6 zu übertragen sich nicht lohnt.

Vorteile von IPv6

Die Vorteile der IPv6 Adressierung sind, dass aufgrund der längeren Adresse ein viel größerer Adressraum existiert. Es können mehrere IPv6-Adressen pro Hosts verwendet werden. Diese haben dementsprechend unterschiedliche Gültigkeitsbereiche. Zudem ist eine Autokonfiguration der einzelnen Adressen möglich und ein Multicast ist ebenso durch spezielle Adressen möglich. Die IPv6 Adressierung ermöglicht ein schnelleres Routing und eine Punkt-zu-Punkt-Verschlüsselung mit IPsec. IPsec ist dafür zuständig, dass eine sichere Kommunikation aufgebaut wird, welches beispielsweise über das Internet eine sichere Kommunikation ermöglichen kann, da das Internet ein unsicheres

Netz ist. Auf dem DoD Model wird das IPsec der Internetschicht zugeordnet. IPsec ist eine Weiterentwicklung der IP-Protokolle. Auf der Netzwerkebene möchte man eine verschlüsselungsbasierte Sicherheit aufstellen. Mit IPsec wird die Authentizität der Paketreihenfolge mittels Verschlüsselung gewährleistet. Die Datenpakete einer IPv6 Adresse sind bis zu 4 GByte groß.

Statische und dynamische IP-Adresse

Nach der Zuweisung einer IP-Adresse ändert sich die IP-Adresse einer statischen Adresse nicht. Die Zuweisung selbst kann sowohl statisch als auch dynamisch sein. Zu einer statischen Adresse beispielsweise gehören Rechner, die sich fortlaufend im Internet befinden, wenn Sie bestimmte Dienste anbieten. Jeder Rechner kann sich eine eigene IP-Adresse zukommen lassen. Bei einer dynamischen IP-Adresse ist dies jedoch anders. Diese werden automatisch vom Internet Service Provider (ISP) vergeben, sobald man im Internet ist. Dynamisch Adressen ändern sich regelmäßig. Bei Routern beispielsweise ändert sich die IP-Adresse alle 24 Stunden. Dies geschieht in der Regel bei lokalen Netzwerken. Der Admin muss jedoch nicht jede einzelne statische IP-Adresse ins Netzwerk integrieren. In der Regel wird dies von einer Software übernommen, die für die Verteilung der dynamischen IP-Adressen zuständig sind.

Vergabe von IP-Adressen

Zuständig für die Vergabe von IP-Adressen ist der IANA. Die IANA vergibt gesamte IP-Adressblöcke an die RIR. Diese vergibt die IP-Adressen in Regionen. Die Vergabe von IP-Adressen erfolgt durch die oberste Instanz "Internet Assigned Numbers Authority" (IANA), die über den gesamten IP-Adressraum herrscht. Sie vergibt IP-Adressblöcke an so genannte "Regional Internet Registries" (RIR), die für die IP-Adressvergabe in Regionen zuständig sind. Diese vergeben ihrerseits IP-Adressbereiche an z.B. Internet-Service-Providern (ISP) wie Telekom, 1&1, Vodafone, O2, die ihren Endkunden gegen eine Gebühr den Zugang zum Internet ermöglichen.

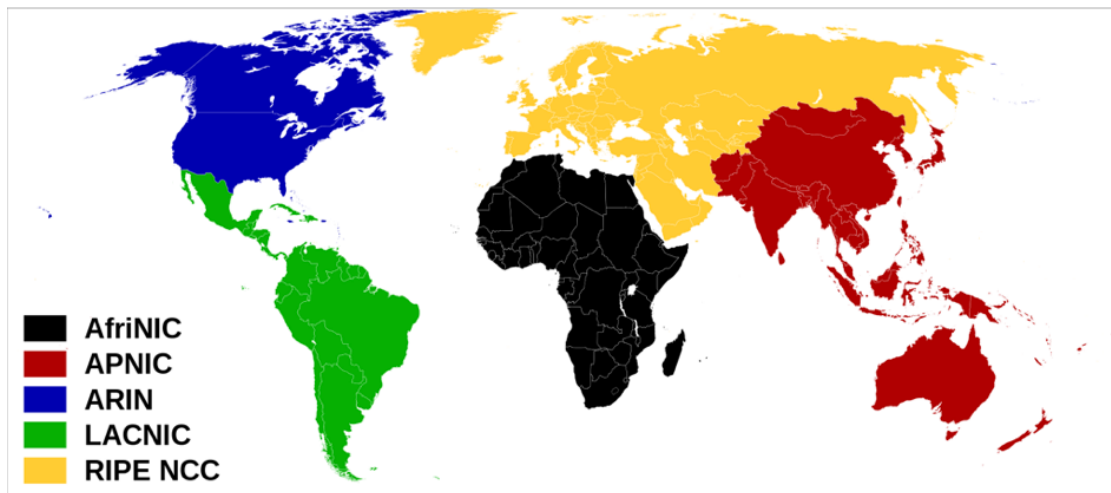


Abbildung 6: Vergabe von IP-Adressen

Es gibt seit Februar 2005 insgesamt fünf regionale Vergabestellen, welche man als Regional Internet Registries (RIR) bezeichnet. Dazu gehören Afrinic (African Network Information Centre). Diese ist zuständig für die Adressvergabe in Afrika. Hinzu kommt die APNIC (Asia Pacific Network Information Centre), welches zuständig für die Region Asien-Pazifik ist. Zudem gibt es die ARIN (American Registry for Internet Numbers), die für Nordamerika zuständig ist. Die LACNIC (Latin-American and Caribbean Network Information Centre) Vergabestelle ist für Lateinamerika und Karibik verantwortlich und zuletzt das RIPE NCC (Réseaux IP Européens Network Coordination Centre), welches für Europa, den Nahen Osten und Zentralasien zuständig ist.

IP-Routing

Das Internetprotokoll (IP) ist routingfähig. Damit werden Datenpakete an Hosts gesendet. Wenn diese nicht im selben Subnetz sind, werden diese über einen Router zum entsprechenden Subnetz transportiert und weitergeleitet. Der Vorgang, wie das Internetprotokoll die Datenpakete vom Sender zum Empfänger schickt, wird als Routing bezeichnet. Dabei sind alle verfügbaren Routen in einer Routing-Tabelle gespeichert. Aus dieser wird dann bestimmt in welches Netz das Datenpaket weitergeleitet wird. Da Broadcasts ein Netzwerk belasten, versuchen die Router die Weiterleitung eines

solchen zu verhindern. Jedoch nur dann, wenn sie selbst nicht darauf angewiesen sind aufgrund der Routing-Tabellen.

IP-Routing-Algorithmus

Alle Datenpakete, die empfangen werden, durchlaufen einen Routing-Algorithmus. Dieser gewährleistet, dass die Datenpakete zugeordnet und zum Ziel-Empfänger weitergeleitet werden.

An erster Stelle des Routing-Algorithmus steht die Frage "Ist das Datenpaket für mich?". Wenn die Ziel-Adresse des Datenpakets mit der eigenen IP-Adresse übereinstimmt, dann hat das Datenpaket sein Ziel erreicht und kann verarbeitet werden. Wenn die Adresse nicht übereinstimmt, dann wird die zweite Frage gestellt: "Ist das Datenpaket für mein Subnetz?". Dabei wird die Zieladresse mit der Subnetzmaske maskiert. Anhand des verbleibenden Adressanteils wird festgestellt, ob das Datenpaket in den eigenen Netzabschnitt (Subnetz oder Subnet) gehört. Stimmt auch das Subnetz nicht, wird die dritte Frage gestellt: "Ist mir die Route zum Empfänger des Datenpakets bekannt?". Manchmal wissen die Hosts die Route für bestimmte IP-Adressen. Wenn die Route bekannt ist, wird das Datenpaket über diese Route weitergeleitet. Ist die Route nicht bekannt wird die vierte Frage gestellt: "Ist mir ein Standard-Gateway bekannt, wohin ich das Datenpaket weiterleiten kann?". Das Standard-Gateway ist in der Regel ein Router, der eingehende Datenpakete anhand der Zieladresse und einigen Regeln an seine Routing-Ausgänge verteilt. Ist kein Standard-Gateway vorhanden führt das zu einer Fehlermeldung. Das Datenpaket wird verworfen.

ICMP

ICMP-Grundsätze

Traceroute

Domain Name System

Domain Namensraum

Domain Name Server

Auflösung eines DNS Requests

DNS-Angriffe

Abbildungsverzeichnis

Abbildung 1: Broadcast und Multicast	5
Abbildung 2: Beispiel mit einem Klienten und Webserver für den Verwendungs- zweck der IP-Adressierung	5
Abbildung 3: Aufteilung in Netzklassen	7
Abbildung 4: IPv6-Aufteilung der Adresse	9
Abbildung 5: Dual Stack	9
Abbildung 6: Vergabe von IP-Adressen	12

Literaturverzeichnis und Quellenverzeichnis

Internetquellen:

<http://www.itwissen.info/IP-Multicast-IP-multicast.html>
<http://ip-klaeden.selfhost.eu/netz/iuk99/kap1a/ipfrag.htm>
<https://www.elektronik-kompodium.de/sites/net/0901141.htm>
http://openbook.rheinwerk-verlag.de/c_von_a_bis_z/025_c_netzwerkprogrammierung_001.htm#mja8101c6e0e4cb2e6fd8312114dad30d7
<http://www.itwissen.info/>
<https://de.wikipedia.org/wiki/Paketvermittlung>
https://de.wikipedia.org/wiki/Internet_Protocol
<https://www.elektronik-kompodium.de/sites/net/2011211.htm>
<http://www.itwissen.info/IPv4-Internet-protocol-version-4-IPv4-Protokoll.html>
<http://www.itwissen.info/IPv6-Internet-protocol-version-6-IPv6-Protokoll.html>
http://www.webschmoeker.de/grundlagen/internet-protocol/#was_bedeutendie_einzelnen_felder_des_ip-headers

<http://www.informatik.uni-hamburg.de/TKRN/world/lernmodule/LMint/Popup/IP.htm>
<http://einstein.informatik.uni-oldenburg.de/rechnernetze/diagramm.htm>
<http://www.cip.ifi.lmu.de/~leinfeld/tcpip/node9.html>
<http://www.linux-praxis.de/linux2/datagram.html>
<https://www.tecchannel.de/a/grundlagen-zu-routing-und-subnetzbildung,434734,9>
<https://de.wikipedia.org/wiki/IP-Paket>

Bildquellen:

http://www.dslundfestnetz.net/images/Fotolia_76722255_XS.jpg
http://www.techweekeurope.co.uk/wp-content/uploads/2012/09/shutterstock_98826353.jpg
DKR-Skript/5.2 Vermittlungstechniken - Screenshot
[https://en.wikipedia.org/wiki/Broadcasting_\(networking\)](https://en.wikipedia.org/wiki/Broadcasting_(networking))
<https://upload.wikimedia.org/wikipedia/commons/thumb/3/30/Multicast.svg/1200px-Multicast.svg.png>
<https://upload.wikimedia.org/wikipedia/commons/thumb/f/f6/DSLite.svg/939px-DSLite.svg.png>
https://upload.wikimedia.org/wikipedia/commons/thumb/9/95/Regional_Internet_Registries_world_map.svg/940px-Regional_Internet_Registries_world_map.svg.png
<http://www.itwissen.info/lex-images/tos-feld-im-ip-header.png>
<http://www.itwissen.info/lex-images/bitkombinationen-fuer-das-tos-datenfeld.png>
<http://www.freesoft.org/CIE/RFC/791/ipflags.gif>
<http://www.itwissen.info/lex-images/protokollnummern-fuer-das-protokolltypfeld.png>
http://ip-klaeden.selfhost.eu/netz/iuk99/kap1a/b_frag.gif
<http://www.itwissen.info/lex-images/hierarchie-der-dns-adresse.png>
<https://upload.wikimedia.org/wikipedia/commons/thumb/f/f1/Dns-abfrage.>

svg/568px-Dns-abfrage.svg.png

https://upload.wikimedia.org/wikipedia/commons/thumb/7/72/IP_spoofing_en.svg/220px-IP_spoofing_en.svg.png