Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

Seminar-Arbeit

IP - Das Internetprotokoll

Leitung: Dr. Klaus-Dieter Heidtmann

vorgelegt von Hanife

MIN-Fakultät

Fachbereich Informatik

Seminar Das Internet: Architektur und Anwendungen

Abgabedatum: 30.03.2018

Inhaltsverzeichnis

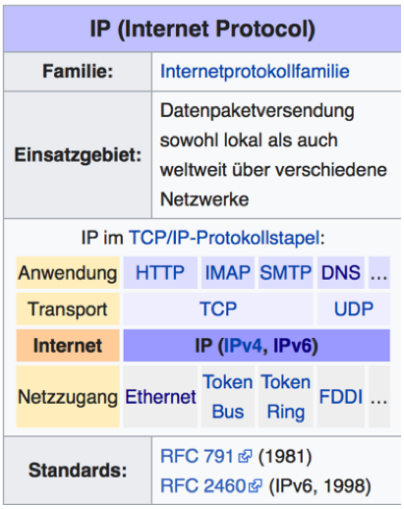
Abkürzungsverzeichnis

Abbildungsverzeichnis

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.

Internetprotokoll (IP) - Einordnung Schichtenmodell



IP (Internet Protocol)					
Familie:	Internetprotokollfamilie				
Einsatzgebiet:	Datenpaketversendung sowohl lokal als auch weltweit über verschiedene Netzwerke				
IP im TCP/IP-Protokollstapel:					
Anwendung	HTTP	IMAP	SMTP	DNS	...
Transport	TCP			UDP	
Internet	**IP (IPv4, IPv6)**				
Netzzugang	Ethernet	Token Bus	Token Ring	FDDI	...
Standards:	RFC 791 (1981) RFC 2460 (IPv6, 1998)				

(a) Internet Protocol

DoD-Schichtenmodell	OSI-Schichtenmodell
Anwendungsschicht Application Layer	Anwendungsschicht
	Darstellungsschicht
	Kommunikationsschicht
Transportschicht Transport Layer	Transportschicht
Internetschicht Internet Layer	Vermittlungsschicht
Netzzugangsschicht Network Access Layer	Sicherungsschicht
	Bitübertragungsschicht

(b) DoD&OSI-Schichtenmodell

Abbildung 1: Schichtenmodell

Internetprotokoll (IP) - Einordnung Vermittlungstechnik

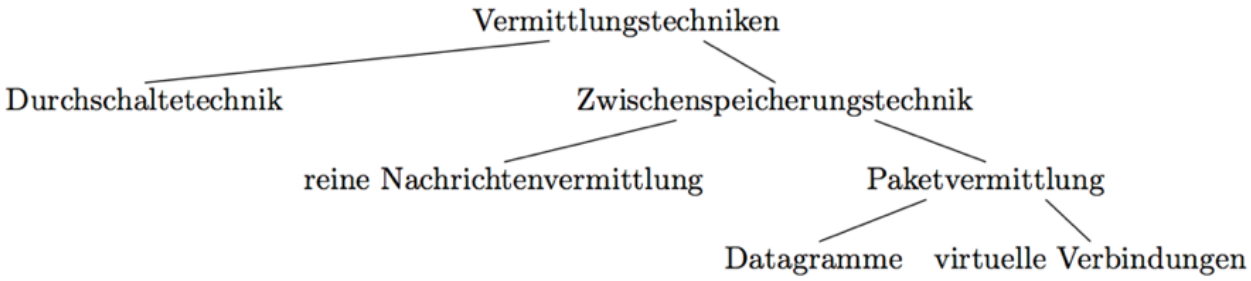
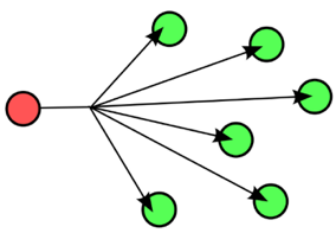


Abbildung 2: Vermittlungstechnik

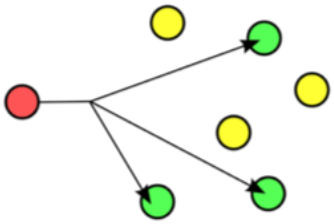
IP-Adressierung -Allgemein

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) Broadcast



(b) Multicast

Abbildung 3: 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.

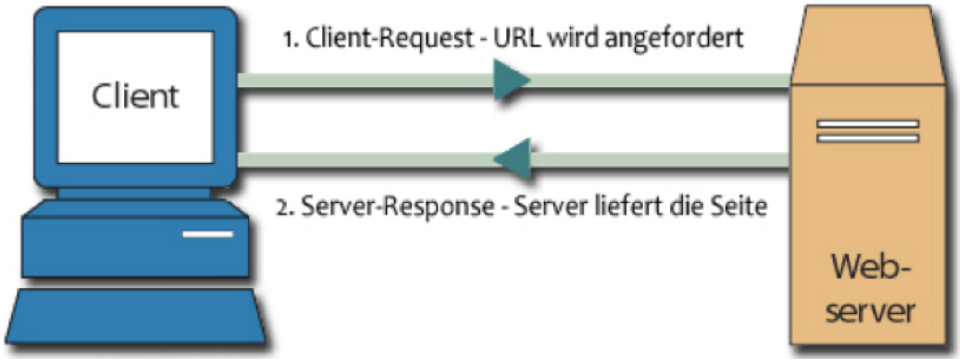


Abbildung 4: Beispiel mit einem Klienten und Webserver für den Verwendungszweck der IP-Adressierung

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 Webservers 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 232 = 4.294.967.296 IP-Adressen darstellbar.
Beispiel:
Dezimale Schreibweise: 171.15.245.1
$\longrightarrow$ 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 Standart-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 5: 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 Routing-tabellen 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:
ddd.ddd.ddd.ddd.ddd.ddd.ddd.ddd.ddd.ddd.ddd.ddd.ddd.ddd.ddd.ddd.
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.

IP-Adressierung IPv6 Adresszuweisung

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-Identifier. Die beiden zusammen bilden die IPv6-Adresse. Üblicherweise wird der Interface-Identifier 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

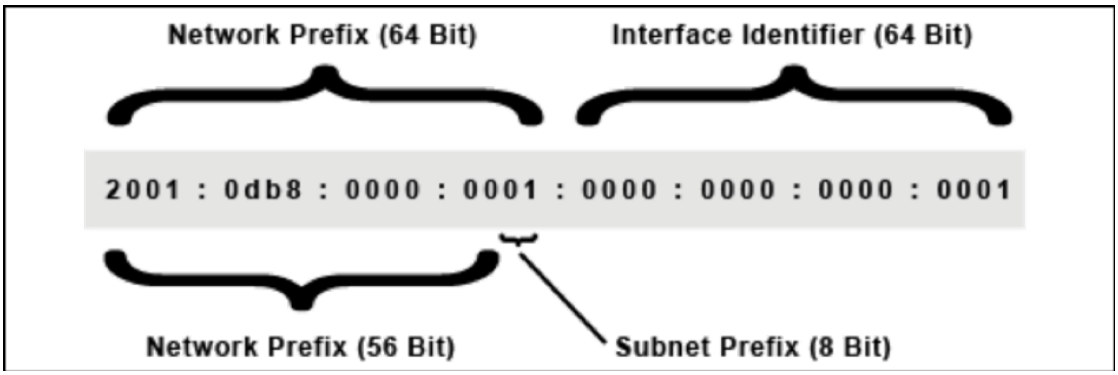


Abbildung 6: IPv6-Aufteilung der Adresse

Dual Stack

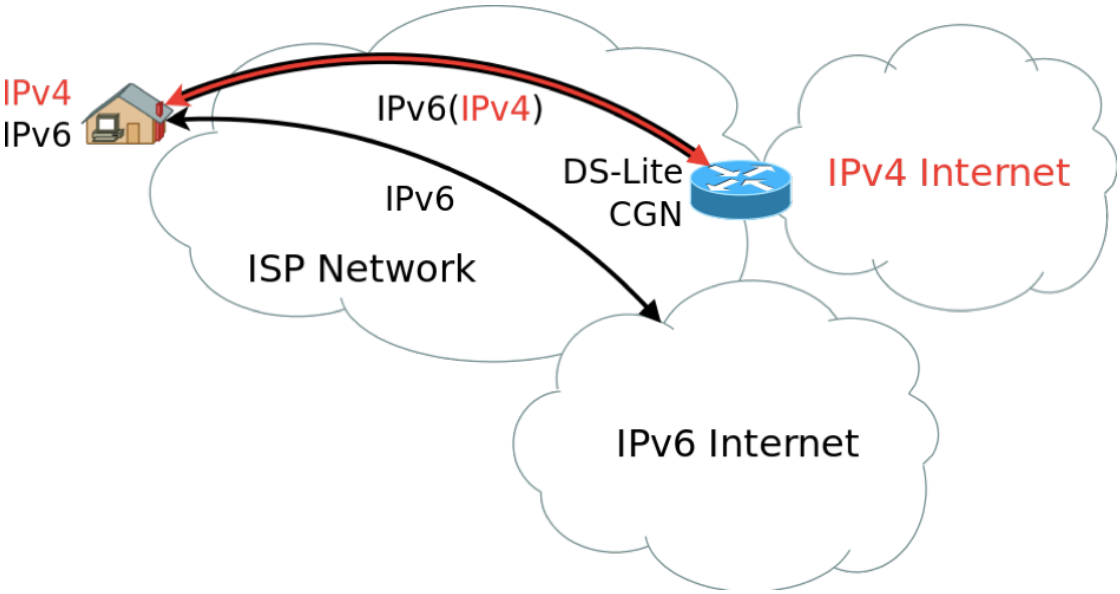


Abbildung 7: Dual Stack

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 mittesls 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.

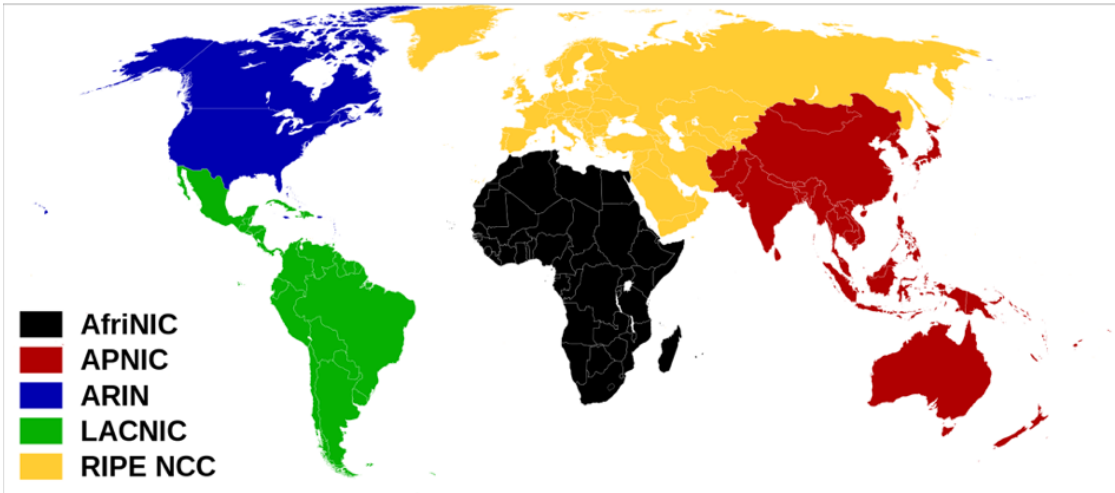


Abbildung 8: Vergabe von IP-Adressen

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-Algoritmus. Dieser gewährleistet, dass die Datenpakete zugeordnet und zum Ziel-Empfänger weitergeleitet werden.
Die Abbildung 7 zeigt, wie der Routing-Algorithmus abläuft. Im Algorithmus geht es die ganze Zeit um das Datenpaket. Zunächst wird geprüft, ob das Datenpaket für einen selbst ist. Dabei wird die Ziel-Adresse des Datenpakets mit der eigenen IP-Adresse verglichen. Wenn diese übereinstimmt, kann mit der Verarbeitung begonnen werden. Andernfalls wird geprüft, ob das Datenpaket im selben Subnetz bleiben soll. Ist dies der Fall, wird das Datenpaket weitergeleitet. Ist dem nicht so, wird geprüft, ob die entsprechende Route bekannt ist. Ist die Route bekannt, wird weitergeleitet, ansonsten muss geprüft werden, ob ein Standartgateway vorhanden ist, der das Datenpaket weiterleiten kann. In der Regel schaut man hier in die Routing-Tabelle und leitet das Datenpaket gegebenfalls weiter. Wenn kein Standartgateway vorhanden ist, kommt es zu einer Fehlermeldung und das Datenpaket wird entsprechend verworfen.

Abbildung 9: IP-Routing-Algorithmus

IP-Paket

Datagramm

Aufbau

IP-Header

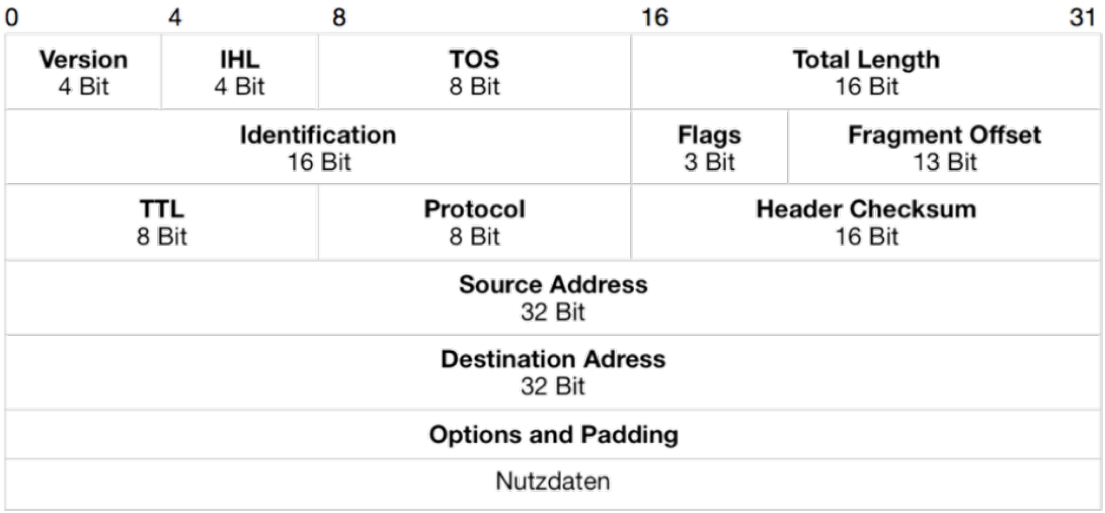
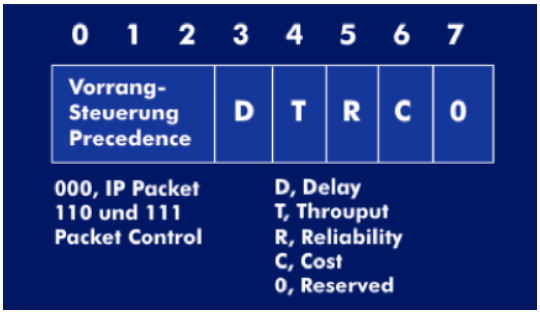


Abbildung 10: IP-Header

Version

IHL

TOS



(a) Vorrang-Steuerung

TOS-Bits	Diensteigenschaft
1000	Minimale Verzögerung
0100	Maximaler Durchsatz
0010	Maximale Zuverlässigkeit
0001	Minimale Kosten
0000	Normaler Dienst

(b) TOS-Bit

Abbildung 11: TOS

DiffServ

Total Length

Identification

Flags

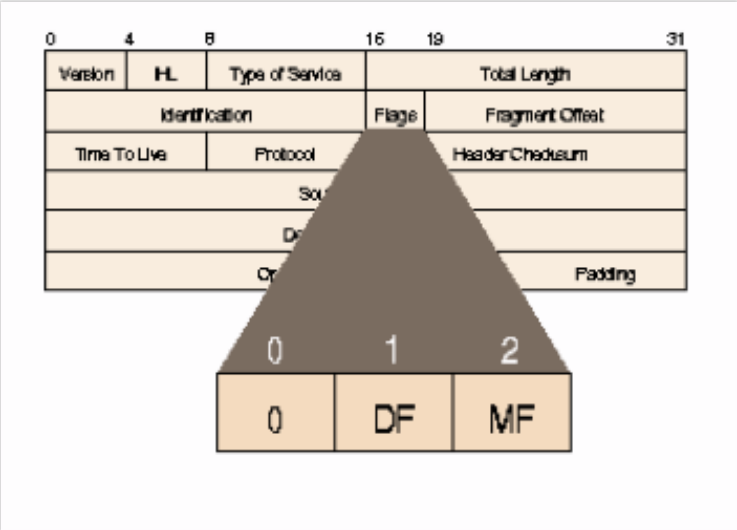


Abbildung 12: Flags

Fragment Offset

TTL

Protocol

Protokoll-nummer	Protokoll	Protokoll-nummer	Protokoll
0	IP	12	PUP
1	ICMP	17	UDP
2	IGMP	20	HMP
3	GGP	27	RDP
6	TCP	29	OSI-TP4
8	EGP		

Abbildung 13: Protocol

Header Checksum

Source Adress

Destination Adress

Options and Padding

IPv6-Header im Vergleich zu IPv4

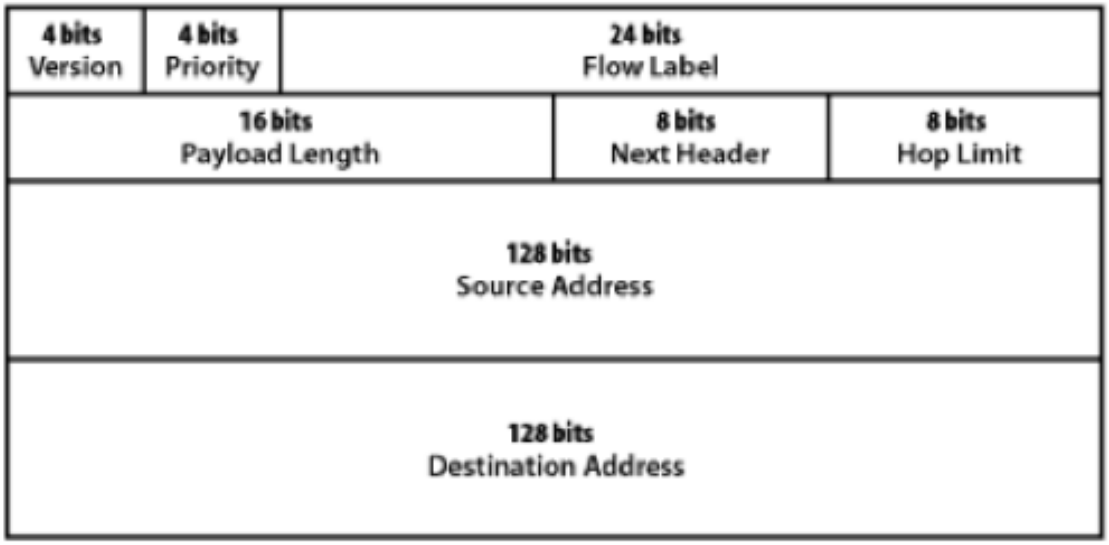


Abbildung 14: IPv6-Header

Fragmentierung/Defragmentierung

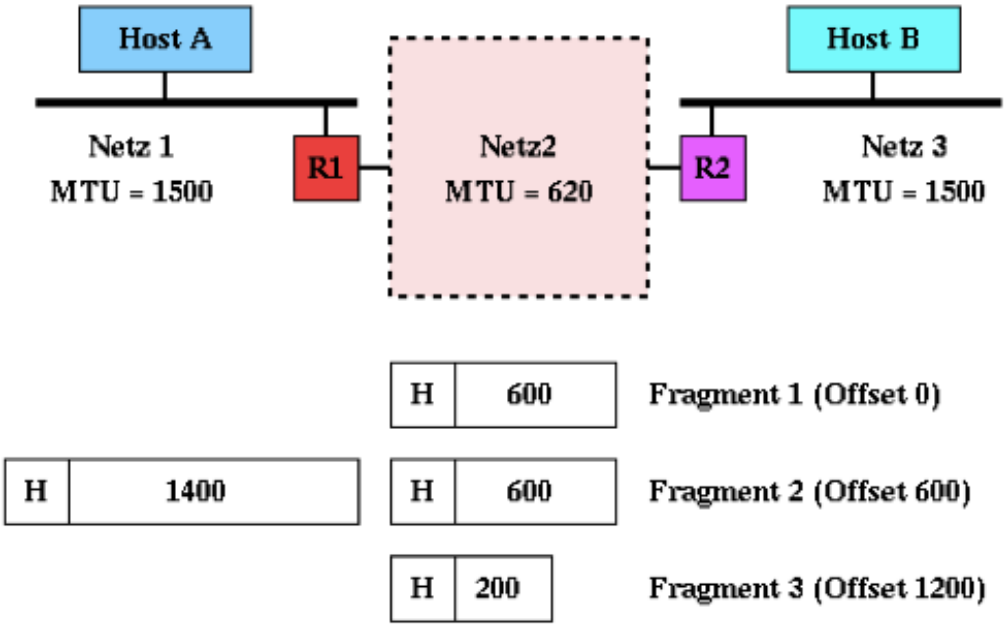


Abbildung 15: Fragmentierung

ICMP

Das sogenannte Internet Control Message Protocol (ICMP) ist ein Bestandteil der IPv4 Adresse. Jedoch wird dies als ein eigenes Protokoll verwendet. Jeder Router, als auch jeder Rechner sind in der Lage mit dem ICMP Protokoll zu kommunizieren. Dieser ist für den Austausch von Informations- und Fehlermeldungen über das Internet-Protokoll in der Version 4 (IPv4) zuständig. Für IPv6 existiert ein ähnliches Protokoll mit dem Namen ICMPv6.

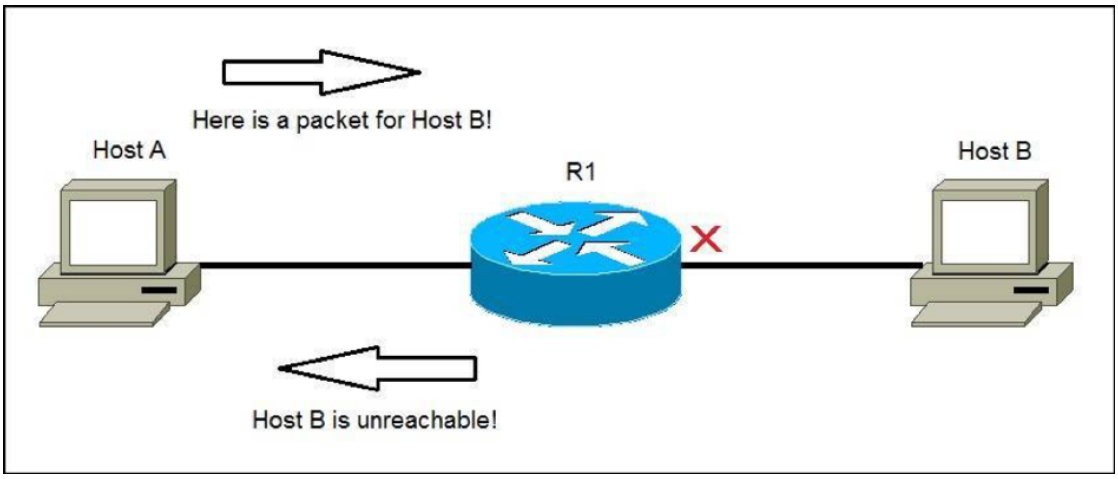


Abbildung 16: ICMP

Der Abbildung ist zu entnehmen, dass die ICMP-Pakete vom Router (R1) zur Quelle (Host A) zurückgeschickt werden, sobald der Router Pakete verwirft. Dies geschieht genau dann, wenn das Ziel (Host B) nicht erreichbar ist oder die TTL (Time to live) abgelaufen ist. Die ICMP-Pakete enthalten in der Regel Informationen über das IPv4-Protokoll.

ICMP-Grundsätze

Das ICMP Protokoll benutzt das IP-Protokoll, um kommunizieren zu können. Das ICMP Protokoll sieht sich selbst als ein Protokoll einer höheren Schicht. Dies hat zur Folge, dass die ICMP-Nachrichten in den IP-Paketen eingegliedert werden. ICMP kann Fehlerzustände erkennen. Hierfür analysiert das Protokoll Fehler in jedem einzelnen

IP-Datenpaket, die keine ICMP-Nachrichten beinhalten. Auf Datenpakete, die von einem Multicast oder Broadcast ausgelöst werden, werden keine ICMP-Nachrichten als Antwort versendet. ICMP Nachrichten antwortem nur Quell-IP-Adressen. Das Paket selbst ist eine 8-Bit Zahl, die sich im ICMP-Header befindet.

Traceroute

Unter einem Traceroute versteht man einen Programm, welches die Route und Internet-Knoten bestimmt, die IP-Datenpakete benötigen, um zum Ziel zu gelangen. Ihr Hauptziel ist es, welche Stationen ein Datenpaket einnimmt, um zum Ziel zu gelangen. Man sendet immer wieder IP-Datenpakete an den Ziel Rechner und beginnt mit einer TTL(Time to Live) =1.
Häufige Verwendung des Traceroute besteht darin, das Routing einer bestimmten Verbindung anzuzeigen oder der Auslöser von Verzögerungen zu identifizieren.

Was passiert bei Traceroute?

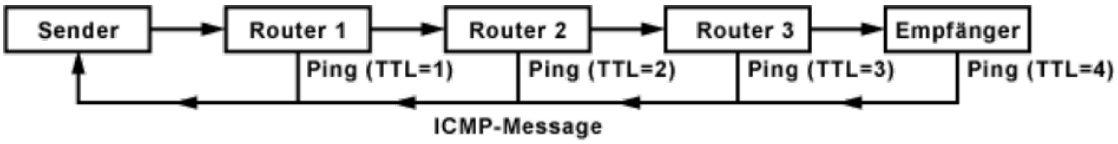


Abbildung 17: Traceroute

Traceroute beginnt mit einer TTL von 1. Dabei sendet er fortlaufend IP-Datenpakete an den Ziel-Rechner. Sobald das erste Datenpaket bei einem Router angekommen ist, der dieses weiterleiten soll, wird die TTL um eins runtergezählt. Da der TTL nun 0 ist, wird dieser verworfen. Anschließend wird eine ICMP-Antwort gesendet vom Typ 11. Nämlich Time exceeded mit dem Code 0: Time to live exceeded in transit an den Absender. Das Datenpaket erhält folglich als Quelladresse die IP-Adresse des Routers. Im Anschluss sorgt Traceroute dafür, dass alle Informationen einschließlich der gesamten Übertragungsdauer aufgezeichnet werden. Danach werden alle Schritte wiederholt mit einer TTL, die um eins erhöht wird. Dies sorgt dafür, dass der nächste Router ermittelt wird. Wenn das Maximum an Hops erreicht wird oder der Zielrechner

erreicht wird, dann hört die Wiederholung auf. Sobald der Zielrechner erreicht wird, sendet er bei ICMP-basiertem Traceroute die ICMP-Antwort Typ 0 ICMP Echo Reply und bei UDP-basiertem Traceroute Destination Unreachable Code 3 Port Unreachable.

Anwendung von Trace Route

Mit Traceroute kann geprüft werden, ob die Datenpakete mit der richtigen Route zum Ziel kommen. Falls dies über einen Umweg läuft, kann daraus schlussgefolgert werden, dass ein Router ausgefallen ist. Zudem kann die Laufzeit zwischen einzelnen Stationen geprüft werden. Falls es dazu kommen sollte, dass ein IP-Paket nicht zum Ziel gelangt, dann kann mit Traceroute die ausgefallene Station ermittelt werden. Wenn mehrere Stationen häufiger vorkommen, könnte die Ursache darin liegen, dass ein Router durch einen fehlerhaften Routing-Eintrag eine Routing-Schleife verursacht.

Domain Name System

Die Hauptaufgabe des Domain Name Systems ist die Beantwortung von Anfragen zur Namensauflösung. DNS wird in vielen IP-basierten Netzwerken verwendet. Jeder Nutzer sendet als Anfrage den Domainnamen übers Internet. Dieser wird vom DNS in die dazugehörige IP-Adresse umgewandelt und kann so einem Rechner zugeordnet werden.

Domain Namensraum

Der Domain Namensraum besitzt eine baumartige Struktur. Dabei nennt man die Blätter und Knoten des Baumes Labels. Will man den kompletten Domainnamen erhalten, so müssen alle Labels desselben Pfades miteinander verkettet werden. Innerhalb einer Domäne kennen die Name-Server nur die Domain-Adressen der direkt höheren oder unteren Nameserver. Zudem bekommt jede Ebene einen eigenen Namen. In Abbildung 10 sind die Domainnamen jeweils mit einem Punkt voneinander getrennt. Die Wurzel repräsentiert immer den DNS-Root.

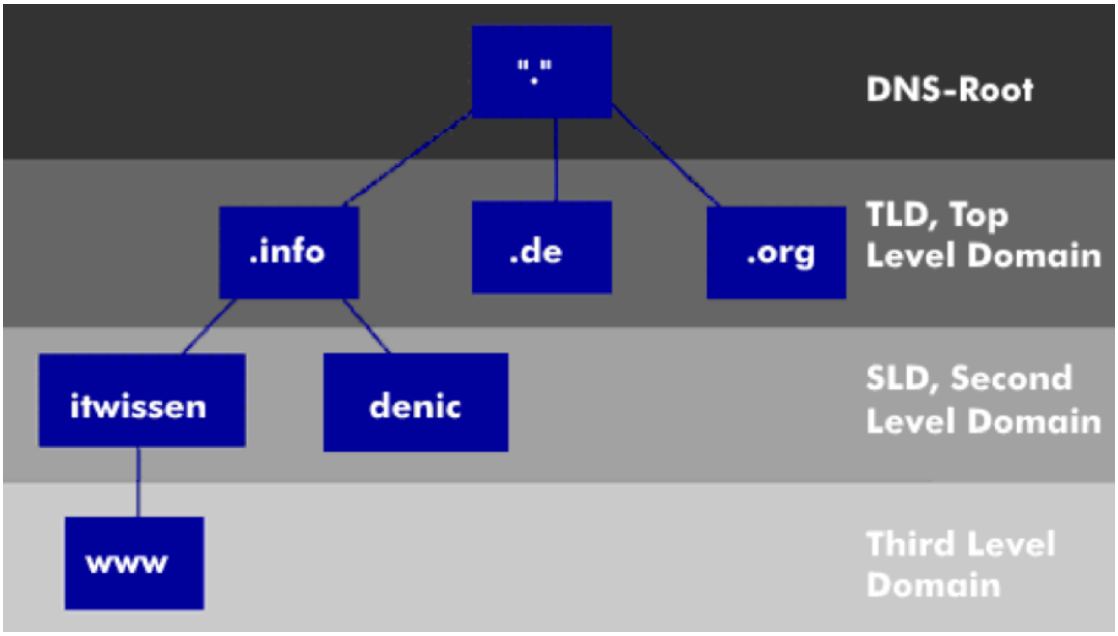


Abbildung 18: Domain Namensraum

Domain Name Server

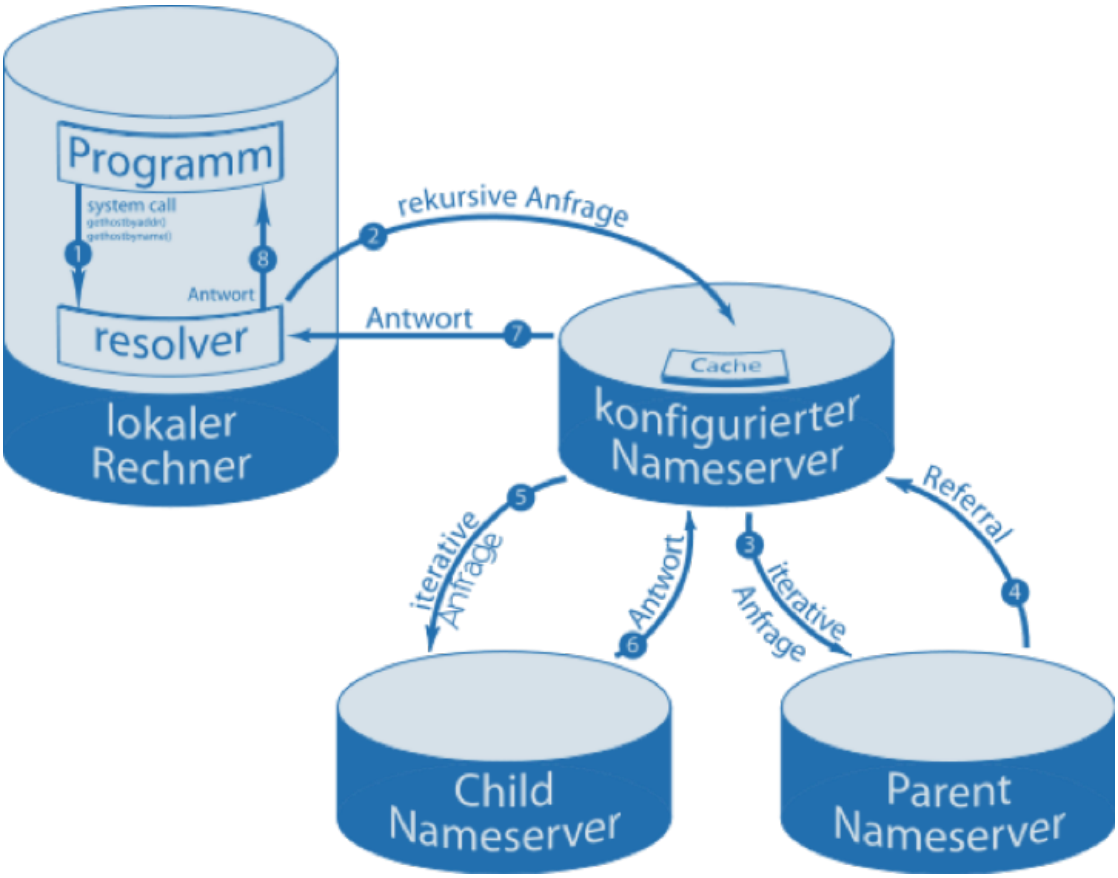


Abbildung 19: Domain Name Server

Jeder DNS-Teilnehmer hat auf seinem eigenen Computer Resolver, die installiert sind. Diese rufen Informationen von Nameservern ab und sind selbst Software-Module. Sie übernehmen die Anfragen der Anwendung und übermitteln diese an einen Nameserver und bilden somit die Schnittstelle. Man unterscheidet zwischen einem rekursiv arbeitenden Resolver und einem iterativ arbeitenden.
Im rekursiven Fall schickt der Resolver eine rekursive Anfrage an einen Nameserver. Dieser schaut im eigenen Datenbestand, ob die benötigten Informationen vorhanden sind. Falls diese nicht vorhanden sind, werden weitere Nameserver kontaktiert. Somit übernehmen die Nameserver die ursprüngliche Aufgabe des Resolvers, da dieser die Anfrage an die Nameserver weiterleitet.

Bei der iterativen Anfrage hingegen bekommt der Resolver entweder den gewünschten Resource Record oder einen Verweis auf weitere Nameserver, die er als nächstes kontaktiert. Dies geschieht solange, bis der Nameserver eine korrekte Antwort bekommt, mit der er arbeiten kann. Der Resolver übergibt die Antwort an ein Programm, welches die Daten angefordert hat. Dies kann zum Beispiel ein Webbrowser sein, der die Anfrage gestellt hat.

Auflösung eines DNS Requests

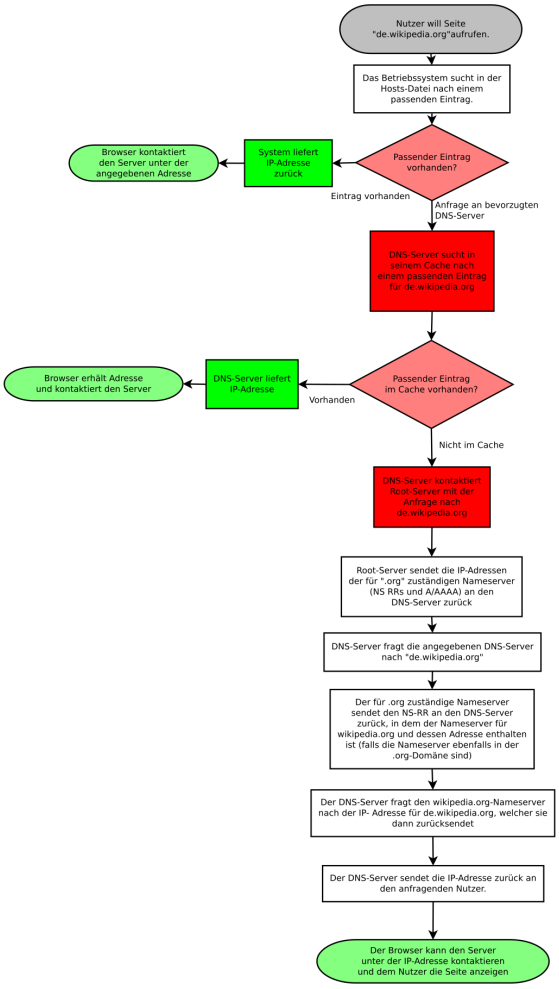


Abbildung 20: Auflösung eines DNS Requests

Bei einer Auflösung eines DNS Requests will ein Rechner eine Verbindung zu einer Seite aufbauen. Dafür benötigt er die IP-Adresse. Dies geschieht mittels Namensauflösung. Dafür müssen folgende Schritte durchlaufen werden. Zunächst sucht der Rechner in seiner eigenen Hosts-Datei, ob die gesuchte IP-Adresse der Webseite schon vorhanden ist. Wenn diese nicht vorhanden ist, fragt dieser einen DNS-Server. Der DNS-Server wird entweder per DHCP automatisch zugewiesen oder der Nameserver ist vorher schon eingetragen. Wenn der DNS-Server die IP-Adresse des angefragten Namens zwischengespeichert hat, liefert er diesen und die Anfrage wird beendet. Ansonsten fragt er einen der 13 Root-Nameservern nach der gesuchten IP-Adresse. Der Root-Nameserver findet zunächst die Zone heraus in welcher sich die Auflösung des Namens befindet. Die Zone ist zunächst die Endung des Namens. In der Abbildung ist dies die org-Zone. Anschließend werden die Namen und die zugehörigen IP-Adressen der entsprechenden Nameserver an den DNS-Server zum Ausgangsrechner gesendet. Dort fragt der DNS-Server den entsprechenden Nameserver für den org-Domain nach der Webseite. Der org-Nameserver sendet alle Namen der Nameserver inklusive der IP-Adressen für die entsprechende Zone. Im Anschluss wird nach der zugehörigen IP-Adresse gefragt, mit welcher an den DNS-Server von dem Ausgangsrechner geantwortet wird. Dieser sendet sie an den Ausgangsrechner, welcher nun seine HTTP-Anfragen an die zugehörige IP-Adresse senden kann.

DNS-Angriffe

Denial of Service (DoS)

DNS Amplification

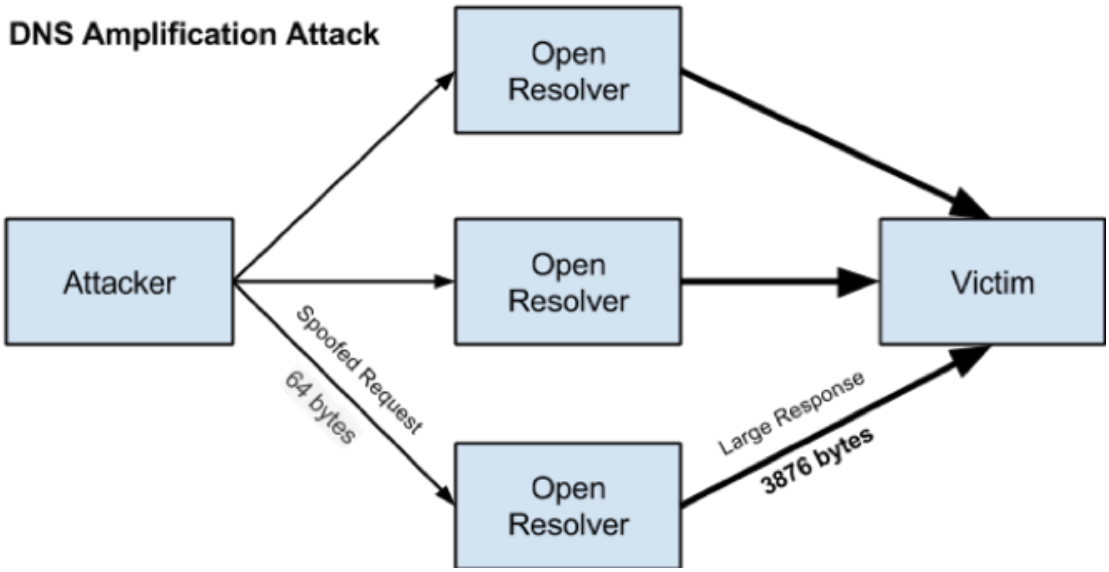


Abbildung 21: DNS Amplification

Spoofing/Phishing

Abbildung 22: Spoofing/Phishing

Cache Poisoning

Fast-Flux DNS

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-kompendium.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-kompendium.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_bedeuten_die_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://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-protokolltyp-feld.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