KAPITEL 3

Internet, Netzwerk und Transportprotokolle

Überblick

In diesem Kapitel erfahren Sie mehr über die folgenden Themen:

Der Erfolg des World Wide Web und des Internet überhaupt ist nicht nur der Attraktivität von Anwendungen wie Webbrowsern und E-Mail-Programmen, sondern auch der Skalierbarkeit und Robustheit der diesen Anwendungen zugrunde liegenden Technologien zuzuschreiben. Bevor es das Internet gab, gab es viele unterschiedliche Netzwerktechnologien, von denen jedoch außer TCP/IP keine über die Eigenschaften verfügte, die für das exponentielle Wachstum des Internet erforderlich waren.

TCP/IP ist (neben UDP) das Protokoll, auf dem der ganze Webverkehr basiert. Insbesondere das Protokoll HTTP baut auf dem Protokoll TCP (Transmission Control Protocol) auf. Ein Großteil des Erfolgs des Internets ist der elementaren Stärke und Skalierbarkeit der Protokolle der unteren Schichten zuzuschreiben. TCP/IP wird häufig als das Schicht-3-Protokoll des Internets bezeichnet, aber eigentlich sind es die beiden Protokolle TCP und UDP, die sich das IP-Protokoll (Internet Protocol) zu Nutze machen. Wenn von TCP/IP als Übertragungsprotokolle des Internets die Rede ist, ist UDP automatisch mitgemeint.

Projekt 3.1: Das Internet und das IP-Protokoll (Internet Protocol)

Nach diesem Kapitel können Sie:

- ✘ Die Organisationen nennen, die für die Registrierung von Domänennamen verantwortlich sind
- ✘ Einen neuen Domänennamen registrieren

Bevor wir uns die technische Seite des Internet Protocol (IP) etwas näher anschauen, sollten wir uns kurz die Geschichte des Internet betrachten. Der Vorläufer des Internet war das ARPANET, das Ende der 60er-Jahre für die Unterstützung von Verteidigungs- und Regierungsprojekten an Forschungsinstituten und Universitäten entwickelt wurde. Die damaligen Nutzungsbedingungen legten fest, dass kommerzielle Anwender im ARPANET bzw. der Vorläuferversion des Internet nicht zulässig waren. In den 80er-Jahren wurden die Nutzungsbestimmungen gelockert und es wurden große Unternehmen zur Nutzung des Netzwerks zugelassen.

Es gab nur wenige größere ISPs, die die erforderlichen Dienste und Verbindungen zur Verfügung stellten. Diese ISPs wurden eingerichtet, um große Unternehmen zu unterstützen. So unterstützte BARRNET (Bay Area Regional Research Network) ursprünglich die Stanford University. Nachdem die Nutzungsbestimmungen gelockert worden und damit Anwender aus der Industrie zulässig waren, erlangten neben anderen Unternehmen aus dem Bereich der neuen Technologien Hewlett-Packard und Amdahl Corporation Zugriff auf das BARRNET. An der Ostküste der USA war BBN (Bolt Beranek und Newman) der größte ISP, der das MIT (Massachusetts Institute of Technology) und andere Universitäten im Raum Boston unterstützte. So wie BARRNET an der Westküste der USA großen Hightech-Unternehmen allmählich den Zugriff auf das Internet gewährte, ermöglichte BBN großen Unternehmen an der Ostküste den Zugriff auf das Internet.

In den 80er-Jahren wurde das Internet um UNIX-Utilities wie E-Mail-Funktionen, FTP und Telnet erweitert. Um eine Telnet- oder FTP-Sitzung zu starten und auszuführen, mussten UNIX-Befehle in die Befehlszeile eingegeben werden. Forscher und Entwickler begannen Such- und Abfrageprogramme wie das an der University of Minnesota entwickelte Gopher und den von Thinking Machines in Boston entwickelte WAIS (Wide Area Information Server) auf der Infrastruktur von UNIX und des Internet aufzusetzen. Bibliothekare, die Zugang zu Forschungs- und anderen Bibliotheksmaterialien bieten wollten, be-

gannen Gopher und WAIS einzusetzen. WAIS wurde als Z39.50-Standard genormt und von Bibliotheken und Informationsdiensten genutzt.

Parallel dazu entwickelte sich das World Wide Web, das als ein Dokumentenverwaltungssystem für Hochenergiephysiker am europäischen Labor für Teilchenphysik, CERN gedacht war. 1993 hatte sich die Nutzung von Gopher und WAIS an Bibliotheken und bei Informationsdiensten bereits durchgesetzt und einige Internetnutzer begannen, Browser mit grafischer Benutzeroberfläche für den Zugriff auf das World Wide Web zu entwickeln und zu nutzen. Im NCSA (National Center for Supercomputing Applications) wurden mehrere Browser entwickelt, darunter auch Mosaic, der bekannteste Browser seiner Zeit. Mosaic bot nicht nur für das HTTP-Protokoll und das World Wide Web, sondern auch für andere Internetprotokolle wie FTP und Telnet eine grafische Benutzeroberfläche. Entwickler schrieben Webschnittstellen für Gopher und WAIS, so dass in Bibliotheken diese Programme weiterhin verwendet werden konnten. Gleichzeitig wurden neue Sammlungen zusammengestellt und im Web über das HTTP-Protokoll verfügbar gemacht. Mit der grafischen Benutzeroberfläche statt der Befehlszeilenmaske, die neue Benutzer meist abschreckte, wurde Mosaic sehr schnell sehr populär. Mosaic wurde dann von Netscape Communications kommerziell eingesetzt, was zum Durchbruch der Browser und des World Wide Web führte. Im Folgenden geht es nun um das Internet und das *Internet Protocol*, die Säulen des World Wide Web.

Das Internet arbeitet mit dem als *IP* oder *Internet Protocol* bekannten Protokoll. IP ist ein auf der dritten Netzwerkschicht angesiedeltes Protokoll. IP beschreibt das Verfahren, mit dem Daten von einem Computer über das Internet an einen anderen Computer gesendet werden. Jeder Internethost verfügt über seine eigene Adresse im Internet. Diese Adresse wird als *IP-Adresse* bezeichnet. Im folgenden Abschnitt geht es nun um IP-Adressen und das IP-Adressierungsverfahren.

Wenn Sie eine Webseite oder eine E-Mail senden oder empfangen möchten, wird die Seite bzw. die E-Mail in so genannte *Pakete* aufgeteilt. Wie im vorhergehenden Kapitel bereits erwähnt, enthält jedes Paket die Internetadresse des Absenders sowie die Internetadresse des Empfängers. Im Internet wird ein Paket zunächst an einen Gatewaycomputer gesendet. Dieser Computer liest die Zieladresse und leitet das Paket an das nächste Gateway weiter. Dieses Gateway liest ebenfalls die Zieladresse des Pakets. Wenn ein bestimmtes Gateway erkennt, dass ein Paket für einen Computer in unmittelbarer Nähe bzw. in einer angrenzenden Domäne bestimmt ist, leitet dieser Computer das Paket direkt an den Computer mit der angegebenen Adresse weiter.

Beim Zerlegen einer Nachricht in Pakete wird jedes Paket mit einer Nummer versehen. Somit kann jedes Paket über einen anderen Pfad im Internet geschickt werden, was einen großen Vorteil darstellt.

Die Aufgabe des IP-Protokolls besteht lediglich darin, die Pakete in der Reihenfolge auszuliefern, in der sie am Ziel ankommen. Es kann also sein, dass die Pakete in einer anderen Reihenfolge ankommen als sie abgeschickt wurden bzw. als in der, in der sie in der abgesendeten Nachricht angeordnet waren. Im Abschnitt über TCP (Transmission Control Protocol) werden Sie erfahren, wie dieses Protokoll dafür sorgt, dass die Pakete wieder in der richtigen Reihenfolge zusammengesetzt werden, so dass die Webseite oder die E-Mail richtig gelesen werden können. Ein weiterer Vorteil des IP-Protokolls besteht darin, dass es sich hierbei um ein verbindungsloses Protokoll handelt. Wenn die Kommunikation erst einmal begonnen hat, gibt es keinen Grund mehr, die Verbindung zwischen den miteinander kommunizierenden Endpunkten aufrecht zu erhalten. Bei der Übertragung der Pakete durch das Internet wird jedes Paket als eine unabhängige Dateneinheit ohne jeden Bezug zu anderen Dateneinheiten behandelt.

Heute gibt es zwei Versionen des IP-Protokolls: IPv4 und IPv6. IPv4, also das Internet Protocol Version 4, ist das allgemein akzeptierte und in Netzwerken von heute verwendete IP-Protokoll. Einige Anbieter beginnen IPv6 zu unterstützen, das ein Verfahren für die Verwaltung längerer Adressen mit sich bringt. Das von IP verwendete Adressierungsverfahren wird im folgenden Abschnitt beschrieben.

Übungen zu 3.1

3.1.1 Die Organisationen nennen, die für die Registrierung von Domänennamen verantwortlich sind

a) Network Solutions ist nicht mehr die einzige Organisation, bei der Domänennamen registriert werden können. Versuchen Sie eine Liste der Organisationen zusammenzustellen, bei denen Domänennamen registriert werden können.

_____

_____

_____

3.1.2 Einen neuen Domänennamen registrieren

b) Lesen Sie bei einem solchen Anbieter nach, wie Sie Ihren eigenen Domänennamen registrieren lassen können.

_____

_____

_____

Lösungen zu den Übungen

Lösung zu 3.1.1

a) Network Solutions ist nicht mehr die einzige Organisation, bei der Domänennamen registriert werden können. Versuchen Sie eine Liste der Stellen zusammen zu stellen, bei denen Domänennamen registriert werden können.

Lösung: ICANN (Internet Corporation for Assigned Names and Numbers) ist die private Organisation, die für die Zuweisung von IP-Adressen, die Zuweisung von Protokollparametern, die Verwaltung des Domain Name System (DNS) und die Verwaltung des Rootserver-Systems gebildet wurde. Auf der Site der ICANN (`www.icann.org`) befindet sich eine Liste der zugelassenen Registrierungsstellen.

Eine aktuelle Liste habe ich unter `http://www.icann.org/registrars/accredited-list.html` gefunden.

Auch auf der Seite der InterNIC finden Sie unter `http://www.internic.net/regist.html` eine Liste der zugelassenen Registrierungsstellen. Eine alphabetisch geordnete Liste gibt es unter `http://internic.net/alpha.html`.

Lösung zu 3.1.2

a) Lesen Sie bei einem solchen Anbieter nach, wie Sie Ihren eigenen Domänennamen registrieren lassen können.

Lösung: Um einen Domänenname registrieren zu lassen, müssen Sie bei der Registrierungsstelle Angaben zu Namen, Wohnort, Telefonnummer, E-Mail-Adresse usw. und natürlich den gewünschten Domänenname angeben. Darüber hinaus müssen Sie noch einige technische Angaben machen. Bei der Registrierungsstelle werden Ihre persönlichen Daten gespeichert und die technischen Angaben werden an das zentrale Verzeichnis mit der Bezeichnung »Registry« gesendet. Hier werden Ihre Angaben, die erforderlich sind, um Ihnen eine E-Mail schicken zu können, oder um Ihre

Website aufrufen zu können, anderen Computern im Internet zur Verfügung gestellt. Sie müssen mit der Registrierungsstelle einen Vertrag abschließen, in dem festgehalten ist, unter welchen Bedingungen Ihre Registrierung akzeptiert wird.

Wiederholungsfragen zu 3.1

Überprüfen Sie Ihr Wissen und versuchen Sie nun, die folgenden Fragen zu beantworten:

1. Zwei Computer können problemlos dieselbe IP-Adresse haben.

   a) Richtig
   b) Falsch

2. Pakete werden in einer Einheit verschickt und können nicht getrennt werden.

   a) Richtig
   b) Falsch

3. Das IP-Protokoll beschreibt das Verfahren, mit dem

   a) E-Mail-Adressen gesucht werden können
   b) Pakete wieder in der richtigen Reihenfolge zusammen gesetzt werden
   c) Daten von einem Computer über das Internet an einen anderen Computer gesendet werden
   d) Keine der genannten Möglichkeiten

4. IP und TCP können unabhängig voneinander arbeiten.

   a) Richtig
   b) Falsch

5. In welcher/n Schicht(en) sind TCP und IP angesiedelt?

   a) TCP in Schicht 2 und IP in Schicht 3
   b) Beide in Schicht 3
   c) TCP in Schicht 3 und IP in Schicht 4
   d) TCP in Schicht 4 und IP in Schicht 3

Die Lösungen befinden sich im Anhang des Buches zum Abschnitt 3.1.

Projekt 3.2: IP-Adressen

Nach diesem Kapitel können Sie:

- ✘ Das IP-Adressierungsverfahren verstehen
- ✘ Einen Domänenname anhand seiner IP-Adresse erkennen

IP-Adressen sind die Namen, die Computer in einem Netzwerk verwenden, um miteinander zu kommunizieren. Im aktuellen IP-Adressierungsverfahren, das als IPv4 (Internet Protocol Version 4) bezeichnet wird, umfasst eine IP-Adresse vier Datenbyte. IPv6 (Internet Protocol Version 6) wurde für längere IP-Adressen und somit für die Zulassung von mehr Hosts entwickelt. Zunächst einmal soll hier nun erläutert werden, wie eine IP-Adresse aufgebaut ist und wie IP-Adressen im Internet verwendet werden. Das Verfahren, mit dem IP-Adressen gebildet werden, ist einer der Gründe dafür, warum das Internet so umfangreich werden konnte, wie es heute ist. Internet-Entwickler hoffen, dass das Internet mit IPv6 noch sehr viel weiter wachsen kann, ohne dass es zu Schwierigkeiten beim Auffinden bestimmter System im Netzwerk kommt.

Eine IP-Adresse kann in unterschiedlichen Formaten dargestellt werden. Das am häufigsten verwendete Format ist das, bei dem die Adresse in vier durch Punkte getrennte Oktette (Bytes) in Dezimalschreibweise dargestellt wird. Ein Beispiel für eine IP-Adresse in diesem Format sieht folgendermaßen aus:

123.234.23.21

Die durch den Punkt getrennte Zahlen liegen im Bereich zwischen 0 und 255. Dies entspricht dem Bereich von 0 bis 2^8 oder 2*2*2*2*2*2*2*2. Sie wundern sich vielleicht, worauf dies zurückzuführen ist. Nun, sagen Ihnen die Begriffe *Bit* und *Byte* etwas?

Ein Bit ist ein Platzhalter für zwei mögliche Werte: entweder 0 oder 1. Ein Byte besteht aus acht Bit.

Bit: 0 oder 1

Byte: 00000000
11111111
10101010
10011001

usw. …

Insgesamt gibt es für ein Byte 2^8 = 2*2*2*2*2*2*2*2 = 256 Kombinationsmöglichkeiten.

Eine IP-Adresse besteht also aus vier Byte bzw. einer Reihe aus 32 Bit. Die Gesamtzahl der möglichen IP-Adressen, die mit IPv4 im Internet verwendet werden können, beträgt somit 2^{32} = 4.294.967.296 oder vier Milliarden.

Das ist etwa 20 % weniger als es zu der Zeit Einwohner auf der Erde gab, als das Internet Protocol entwickelt wurde. Inzwischen ist die Sorge berechtigt, was zu tun ist, wenn die Internetadressen eines Tages ausgehen. Zu Beginn des Internetzeitalters teilte die für die Zuweisung von IP-Adressen an Institutionen zuständige Stelle großzügig ganze IP-Adressräume zu. Heute muss eine Organisation, die IP-Adressen beantragt, jede einzelne Adresse ausführlich rechtfertigen.

Subnetzmaske

Um die Identität eines Computers im Internet bestimmen zu können, sind zwei Angaben erforderlich: die IP-Adresse und die zugehörige Subnetzmaske.

Das Internet besteht aus vielen einzelnen, miteinander verbundenen Netzwerken. Mit Blick auf das Internet werden diese einzelnen Netzwerk als Subnetze bezeichnet. Ein Subnetz ist also ein für sich gesehen komplettes Netzwerk, das jedoch Teil eines größeren Netzwerks, nämlich des Internet ist.

Mit einer IP-Adresse kann sowohl ein einzelner Computer als auch das Subnetz bezeichnet werden, in dem sich der Computer befindet. Um das Auffinden von einzelnen Computern im Internet (die Aufgabe von Routern und Switches) einfacher zu machen, wird zuerst nach dem Subnetz und dann nach dem Computer gesucht.

Eine Subnetzmaske teilt eine IP-Adresse im Prinzip in zwei Teile: die Netzwerknummer (Netzwerk-ID) und die Hostnummer (Host-ID). Ein einfaches Beispiel veranschaulicht diese Aufteilung.

1. Nehmen wir einmal die oben genannte IP-Adresse: 123.234.23.21

   Eine Subnetzmaske kann beispielsweise mit dieser Adresse in Verbindung gebracht werden, um dadurch anzugeben, dass die ersten drei Oktette (123.234.23) für das Netzwerk des Rechners stehen, und dass das letzte Oktett (21) die Host-ID repräsentiert. Dieses Subnetz könnte 255 Hosts umfassen, da das letzte Oktett ausschließlich für die Angabe von Hosts zur Verfügung steht. In diesem Fall würde die Netzwerk-ID folgendermaßen aussehen: 123.234.23.0.

2. Die Subnetzmaske für eine solche Konfiguration sähe wie folgt aus: 255.255.255.0.

   Eine weitere Möglichkeit sieht so aus, dass die ersten beiden Oktette (123.234) ein Netzwerk und die letzten beiden Oktette (23.21) einen Host angeben. In diesem Fall könnten im Subnetz 255x255 bzw. 65025 Hosts angeschlossen sein. Die Netzwerk-ID würde dann folgendermaßen lauten: 123.234.0.0.

3. Die Subnetzmaske für eine solche Konfiguration sähe wie folgt aus: 255.255.0.0.

   Möglicherweise wird nun aber ein Netzwerk benötigt, das kleiner als 65025, aber größer als 255 Hosts ist. In diesem Fall muss das Netzwerk und die Host-ID entlang einer Grenze aufgeteilt werden, die nicht mit den Punkten in der Oktettdarstellung der IP-Adresse zusammenfällt. So hätte ein Subnetz mit 1024 Hosts beispielsweise die Subnetzmaske 255.255.248.0.

4. Denken Sie daran, dass jedes Oktett (die Zahl zwischen den Punkten) ein Byte, d.h. acht Bit darstellt. In unserem Beispiel wurden die ersten beiden Oktette und sechs der acht Bit des dritten Oktetts der Netzwerknummer zugeordnet. Die restlichen zehn Bit (zwei vom dritten Oktett und acht vom letzten Oktett) bilden die Host-ID. Somit kann dieses Subnetz (2*2)*(2*2*2*2*2*2*2*2*2*2) = (4)*(256) = 2^{10} = 1024 Hosts aufnehmen.

   Wie bereits erwähnt, erfolgt das Suchen einer bestimmten IP-Adresse im Internet in zwei getrennten Schritten. Zuerst wird das Netzwerk und dann der Host gesucht. So müssen Internetrouter nicht so viele Informationen speichern und können sich auf die Netzwerk-IDs beschränken. Wenn das »durchschnittliche« Subnetz im Internet 1000 Hosts umfasst, gibt es tausendmal weniger Netzwerke als Hosts und ein Internetrouter muss tausendmal weniger Adressen verwalten.

Übungen zu 3.2

3.2.1 Das IP-Adressierungsverfahren verstehen

Arbeiten Sie mit dem auf Ihrem PC befindlichen Utility *winipcfg*.

a) Ermitteln Sie die IP-Adresse Ihres PC.

_____

_____

_____

b) Wie lautet die Subnetzmaske Ihres PC?

_____

_____

_____

c) Sehen Sie nach, wie Ihr Hostname lautet.

_____

_____

_____

3.2.2 Einen Domänennamen anhand seiner IP-Adresse erkennen

a) Prüfen Sie mit Hilfe des Utility *ping*, ob eine Domäne verfügbar ist. Versuchen Sie es mit einer bekannten Domäne wie `yahoo.com`, `mapquest.com` oder `barnesandnoble.com`. Ermitteln Sie die IP-Adresse jeder Domäne, die Sie prüfen.

b) Suchen Sie nun die IP-Adresse der Website `www.yahoo.com`.

c) Geben Sie die IP-Adresse der Website in Ihrem Webbrowser ein und prüfen Sie, ob Sie so zur Hauptseite der Site gelangen.

Lösungen zu den Übungen

Lösungen zu 3.2.1

Arbeiten Sie mit dem Utility *winipcfg*, das sich auf Ihrem PC befindet.

a) Ermitteln Sie die IP-Adresse Ihres PC.

Lösung: Klicken Sie im Menü START auf AUSFÜHREN. Geben Sie in dem daraufhin erscheinenden Fenster den Befehl `winipcfg`. Danach erscheint ein Fenster, dem Sie die IP-Adresse Ihres Rechners entnehmen können.

b) Wie lautet die Subnetzmaske Ihres PC?

Lösung: In dem Fenster, das erscheint, nachdem Sie den Befehl `winipcfg` ausgeführt haben, wird auch die Subnetzmaske Ihres PCs angezeigt.

c) Sehen Sie nach, wie Ihr Hostname lautet.

Lösung: Wenn Sie auf die Schaltfläche WEITERE INFO klicken, wird Ihr Hostname ebenfalls angezeigt.

Lösungen zu 3.2.2

a) Prüfen Sie mit Hilfe des Utility *ping*, ob eine Domäne verfügbar ist. Versuchen Sie es mit einer bekannten Domäne wie `yahoo.com`, mapquest.com oder `barnesandnoble.com`. Ermitteln Sie die IP-Adresse jeder Domäne, die Sie prüfen.

Lösung: Klicken Sie im Menü START auf AUSFÜHREN. Wenn das Fenster erscheint, geben Sie den Befehl `ping` zusammen mit dem Domänennamen, also z.B. `ping barnesandnoble.com` ein. Als ich diesen Befehl mit yahoo.com ausgeführt habe, wurde die IP-Adresse 216.115.108.232 angezeigt. Es kann jedoch sein, dass die Domäne inzwischen unter einer anderen Adresse erreichbar ist.

b) Suchen Sie nun die IP-Adresse der Website `www.yahoo.com`.

Lösung: Klicken Sie noch einmal im Menü START auf AUSFÜHREN. Geben Sie `ping www.yahoo.com` oder `ping` mit einem anderen Domänennamen ein. Wenn Sie möchten, dass das Fenster länger angezeigt wird, so dass Sie auch lesen können, was dort geschrieben steht, geben Sie den Befehl `ping www.yahoo.com -t` ein. Damit wird der Ping-Prozess fortgeführt. Um diesen wieder zu beenden, drücken Sie die Tasten Strg und C gleichzeitig. Die Adresse, die bei mir nun angezeigt wird, lautet: 204.71.200.75.

c) Geben Sie die IP-Adresse der Website in Ihrem Webbrowser ein und prüfen Sie, ob Sie so zur Hauptseite der Site gelangen.

Lösung: Rufen Sie Ihren Webbrowser auf und geben Sie die IP-Adresse ein, die Sie mit Hilfe von *ping* ermittelt haben. Wenn ich 204.71.200.75

eingebe, erscheint die Hauptseite der Yahoo-Website auf meinem Bildschirm.

Wiederholungsfragen zu 3.2

Überprüfen Sie Ihr Wissen und versuchen Sie nun, die folgenden Fragen zu beantworten:

1. Zur Zeit gibt es ... IP-Adressen.

   a) Zu viele
   b) Zu wenige

2. Wonach wird bei der Suche eines Computers im Internet zuerst gesucht?

   a) Subnetz
   b) Computer
   c) Keines von beidem

3. Wie würde die Subnetzmaske für ein Netzwerk mit 255 Hosts lauten?

   a) 255.0.0.255
   b) 0.0.0.255
   c) 255.255.255.0
   d) 255.255.248.255
   e) 255.0.255.255.255

4. Wie unterscheiden sich IPv4 und IPv6 voneinander? Geben Sie alle zutreffenden Möglichkeiten an.

   a) Bei IPv4 sind mehr Datenbyte zulässig als bei IPv6.
   b) Bei IPv6 besteht eine Adresse aus sechs Gruppen zu je drei hexadezimalen Zeichen.
   c) Bei IPv6 umfasst eine Adresse 16 Byte, während eine IPv4-Adresse aus nur 4 Byte bestehen darf.
   d) Alle genannten Möglichkeiten.

5. Wie viele Zahlenkombinationen können mit einem Byte dargestellt werden?

   a) 8
   b) 64
   c) 128
   d) 256
   e) 512

Die Lösungen befinden sich im Anhang des Buches zum Abschnitt 3.2.

Projekt 3.3: DNS (Domain Name System)

Nach diesem Kapitel können Sie:

- ✘ Verstehen, was Domänen mit IP-Adressen zu tun haben
- ✘ Wie ein Domänenname aufgelöst werden kann

Jeder Internethost verfügt über eine eigene IP-Adresse. Mit Hilfe des DNS (Domain Name System) wird eine Verknüpfung zwischen jedem Namen und einer bestimmten IP-Adresse hergestellt. Wenn Sie den vollständigen DNS-Namen, also beispielsweise `benay.asilomar.dara-abrams.com` oder `drew.africa.drewnet.net` angeben, wird dieser Name einer bestimmten IP-Adresse im Internet zugeordnet. Die IP-Adresse bietet eine Möglichkeit, einen logischen Domänennamen, mit einem Namen, den sich Menschen merken können, in eine physikalische Adresse zu übersetzen, die vom IP-Adressierungsverfahren verwendet werden kann. Wenn Sie einen Domänennamen in einer URL oder in einer E-Mail-Adresse angeben, wird dieser Domänenname, z.B. `prenhall.com`, in eine bestimmte IP-Adresse im Internet übersetzt.

Der Domänenname funktioniert also für eine IP-Adresse wie ein CB-Funknummer. Das DNS-Verfahren stellt für eine IP-Adresse einen logischen Namen zur Verfügung. Es ist jedoch weinig praktisch, eine Liste mit Domänennamen und den dazu gehörenden IP-Adressen zentral zu erstellen und zu verwalten. Wie mit anderen Dingen im Internet wird auch hier die Arbeitslast im Netzwerk verteilt. Eine Liste mit IP-Adressen und den entsprechenden Domänennamen wird in einer Autoritätshierarchie verteilt. Wenn Sie eine Nachricht senden oder empfangen oder Webseiten aufrufen, verwendet Ihr System zum Auflösen von Adressen einen DNS-Server in unmittelbarer Nähe Ihres ISPs. Dieser DNS-Server ordnet Domänennamen in Ihren Internetanforderungen entweder selbst zu oder leitet sie an andere Internetserver weiter.

IP-Adressen sind im Prinzip die Namen, die Computer in einem Netzwerk verwenden, um miteinander zu kommunizieren. Da sich Computer nicht anhand von Eigenschaften wie dem Klang der Stimme oder dem Aussehen erkennen können, braucht jeder Computer im Internet eine eigene IP-Adresse.

Im Gegensatz zu Menschen können sich Computer lange Zahlenreihen problemlos merken. Wir Menschen arbeiten lieber mit etwas besser Vorstellbarem wie z.B. mit Namen. Viele haben einen an ein Netzwerk angeschlossenen Computer auf dem Tisch stehen, der, wenn er über einen Anschluss an das Internet verfügt, auch eine IP-Adresse hat. Aber die wenigsten kennen

diese IP-Adresse. Um die Unterschiede zwischen Menschen und Computern zu überbrücken, wurde das DNS (Domain Name System) entwickelt.

Einfach ausgedrückt, ist DNS für die Verknüpfung von Namen mit IP-Adressen verantwortlich. So können wir unsere Computer nach Stränden in Monterey Bay wie Asilomar, Pebblebeach oder Pajaro benennen. Wie im richtigen Leben sprechen wir die, die uns nahe stehen, häufig nicht mit vollem Namen an. Damit es nicht zu Verwechslungen kommt, muss jedoch der vollständige Name genannt werden. So kann ein bestimmter Computer beispielsweise `pajaro.dara-abrams.brainjolt.com` genannt werden.

`Pajaro` kommt in der Domäne `dara-abrams` nur einmal vor. `Dara-abrams` kommt in `brainjolt` und `brainjolt` in `com` nur einmal vor. Es kann im Internet durchaus mehrere `pajaros` geben, aber `pajaro.dara-abrams.brainjolt.com` gibt es nur einmal.

Übungen zu 3.3

3.3.1 Verstehen, was Domänen mit IP-Adressen zu tun haben

a) Geben Sie in einem UNIX-System den Befehl `nslookup` mit einer beliebigen IP-Adresse ein. Welches Ergebnis erhalten Sie?

3.3.2 Wie ein Domänenname aufgelöst werden kann

a) Suchen Sie mit dem Utility *whois* die IP-Adresse des Namensservers einer bekannten Domäne wie z.B. `amazon.com` oder `yahoo.com`.

Lösungen zu den Übungen

Lösung zu 3.3.1

b) Geben Sie in einem UNIX-System den Befehl `nslookup` mit einer beliebigen IP-Adresse ein. Welches Ergebnis erhalten Sie?

Lösung: Mit dem Befehl `nslookup` wird der Domänennamensserver angezeigt, der für die Suche von IP-Adressen verwendet wird. Außerdem wird der vom Server ermittelte DNS-Eintrag für die von Ihnen angegebene IP-Adresse angezeigt.

Lösung zu 3.3.2

c) Suchen Sie mit dem Utility *whois* die IP-Adresse des Namensservers einer bekannten Domäne wie z.B. `amazon.com` oder `yahoo.com`.

Lösung: Sie können das Utility *whois* auf der InterNIC-Site (`www.internic.net`) verwenden. Wenn Sie den Domänennamen `amazon.com` eingeben (und auf DOMAIN klicken), wird der Namensserver angezeigt. Über den Namensserver habe ich folgende Information erhalten: NS2.PNAP.NET. Als ich den angegebenen Namensserver eingab und auf NAMESERVER klickte, erhielt ich folgende Angaben:

```
Server Name: NS2.PNAP.NET
IP Address: 206.253.194.97
Registrar: NETWORK SOLUTIONS, INC.
Whois Server: whois.networksolutions.com
Referral URL: www.networksolutions.com
```

Somit lautet die IP-Adresse für den primären Namensserver von `amazon.com`: 206.253.194.197.

Wiederholungsfragen zu 3.3

Überprüfen Sie Ihr Wissen und versuchen Sie nun, die folgenden Fragen zu beantworten:

1. Computer sprechen einander mit ... an.

   a) Dem Domänennamen
   b) Der IP-Adresse
   c) Der Subnetzmaske
   d) Allen genannten Möglichkeiten

2. DNS verknüpft ... mit ....

   a) IP-Adresse, Domänenname
   b) IP-Adresse, Subnetzmaske
   c) Domänenname, Subnetzmaske

3. Wenn es einen Computer mit dem Domänennamen `darwin.millenniumpark.org` gibt, kann es dann gleichzeitig einen Computer mit dem Domänennamen `darwin.brainjolt.com` geben?

   a) Ja
   b) Nein

4. Sie können eine Webseite ohne DNS-Adresse nicht finden.

   a) Richtig
   b) Falsch

5. Computernamen müssen eindeutig sein, damit Domänennamen eindeutig sein können.

   a) Richtig
   b) Falsch

Die Lösungen befinden sich im Anhang des Buches zum Abschnitt 3.3.

Projekt 3.4: TCP (Transmission Control Protocol)

Nach diesem Kapitel können Sie:

- ✘ Die Socket-Nummer für »bekannte Dienste« bestimmen
- ✘ Die Verwendung von Ports und Diensten verstehen

Das Protokoll TCP (Transmission Control Protocol) verfügt über Features zum Steuern des Datenflusses (Paketen) zwischen Absender und Empfänger. Diese Flusskontrolle ist mit ein Grund für die exponentielle Ausbreitung des Internet.

Das wichtigste Feature von TCP ist, dass es dafür sorgt, dass jedes Datenpaket an seinem Ziel abgeliefert und angenommen wird. Wenn ein Paket am Ziel nicht ausgeliefert werden kann, wird der Benutzer (ein Protokoll einer höheren Schicht) darüber informiert.

Die ganze Wahrheit

Die folgenden Ausdrücke werden im Zusammenhang mit TCP synonym verwendet:

Socket ist dasselbe wie *Port*

und

Verbindung ist dasselbe wie *Sitzung*

Sockets

TCP steuert die Auslieferung von Paketen, indem es für jede TCP-Kommunikation eine »Verbindung« bzw. »Sitzung« einrichtet. TCP wird als ein »verbindungsloses« Protokoll bezeichnet. Sitzungen in TCP werden zwischen zwei Endpunkten eingerichtet. Die Endpunkte werden anhand der IP-Adresse und Socket-Nummer der Sitzung für jeden Rechner definiert. Jede TCP-Sitzung ist durch diese beiden Parameter eindeutig definiert.

Wenn zwischen zwei Endpunkten eine Sitzung initiiert wird, sendet TCP eine Synchronisierungsanforderung (ein Paket mit der Bezeichnung »syn«) an die Adresse des Rechners, zu dem eine Verbindung hergestellt werden soll. Dieses Paket enthält Informationen über die Socket-Nummer, mit der der erste Rechner eine Verbindung herstellen möchte. Der Zielrechner sendet darauf-

hin eine Bestätigung (»ack« genannt) an den initiierenden Rechner und teilt diesem mit, dass er die »syn« empfangen hat und dass die gewünschte Socket-Nummer verfügbar ist. Darüber hinaus sendet der zweite Rechner (in einer Übertragung) selbst auch eine Synchronisierungsanforderung, in der er die Socket-Nummer angibt, an die er Pakete an den initiierenden Rechner zurückschicken möchte. Dieses Paket hat die Bezeichnung »syn-ack«, weil damit sowohl das erste Paket bestätigt als auch eine Synchronisierung angefordert wird. Schließlich sendet der initiierende Rechner eine Bestätigung an den zweiten Rechner und teilt diesem mit, dass die in der »syn-ack« angeforderte Socket-Nummer für die Verbindung zur Verfügung steht.

Nun ist die TCP-Sitzung eingerichtet. Sie kann anhand der eindeutigen Endpunkte, der IP-Adresse und Socket-Nummer des ersten Rechners und der IP-Adresse und Socket-Nummer des zweiten Rechners erkannt werden. Zu diesem Zeitpunkt gibt es diese Kombination nur einmal.

Die ganze Wahrheit

Wenn ein Client eine HTTP-Verbindung zu einem Server anfordert, richtet er diese Anforderung an die IP-Adresse des Servers an Port 80. Der Server sucht sich dann einen beliebigen Port über 1023 und sendet ein Paket an den anfordernden Client. Damit fragt er, ob Antwortpakete an die IP-Adresse des anfordernden Client am beliebig gewählten Port gesendet werden können. Wenn dieser Port beim Client frei ist, bestätigt er die Anfrage und beginnt den vereinbarten Port abzuhören.

So kann ein Client mehrere TCP-Sitzungen gleichzeitig mit einem bestimmten Server anfordern und dennoch für jede Sitzung eigene IDs verwenden. Der Port, über den der Server mit dem Client kommuniziert, wird beliebig zugewiesen. Wenn beim Client der vom Server vorgeschlagene Port belegt ist, lehnt der Client den Vorschlag des Servers ab. Daraufhin schlägt der Server einen neuen Port vor. Das geht so lange, bis sich die beiden Rechner auf einen Port einigen können.

Beim IP-Protokoll werden zwei Datenbyte für die Definition der TCP-Socket-Nummer (bzw. UDP-Socket-Nummer) verwendet. Das bedeutet, dass es insgesamt $(2^8)*(2^8) = 255 * 255 = 65.025$ Socket-Nummern gibt.

Die Port- bzw. Socket-Nummern 0 bis 1023 sind für die Definition des Prozesses reserviert. Anders ausgedrückt: Ein mit IP arbeitender Rechner darf nur bestimmte Protokolle auf diesen Ports zulassen. Ports über 1023 (von 1024 bis 65025) sind keinen bestimmten Protokollen zugewiesen und können für jedes beliebige Protokoll verwendet werden.