Praktische Übungen zu Computertechnik 2

Versuchsprotokoll

Versuch:

C3 – Rechner-Netzwerke

Versuchsdatum und -zeit:

Donnerstag, 24. Juni 2010, 10-13 Uhr

Betreuer:

Adrian Knoth

Name, Studiengang, Mat.-Nr.:

Ralf Wondratschek, B. Sc. Informatik, 112626

Email:

ralf.wondratschek@uni-jena.de

Name, Studiengang, Mat.-Nr.:

Kerstin Gößner, B. Sc. Informatik, 114656

Email:

kerstin.goessner@uni-jena.de

Vom Betreuer auszufüllen:

Vorbereitung/Kolloquium:

Durchführung:

Protokoll:

Gesamtbewertung:

Gliederung

1. Vorbereitung

Eine der wohl rasantesten Entwicklungen in den letzten Jahrzehnten legte zweifelsfrei das Internet hin. Ziel: jeder Computer soll mit den anderen im weltweiten Netz kommunizieren und Daten austauschen können, Informationen sollen stets abrufbar sein. Um die Daten zwischen Geräten austauschen zu können, dient zurzeit am meisten das Internet-Protokoll Version 4 (IPv4). Jedoch wird diese Version in absehbarer Zeit wegen des Bedarfs an IP-Adressen durch IPv6 abgelöst.

Dieser Versuch soll die grundlegende Funktionalität des Internets mit dem zukünftigen Standard IPv6 vermitteln.

2. Vorgehensweise

Insgesamt stehen drei Rechner zur Verfügung. Der erste Linux Rechner hat die Funktion des Clients, das heißt er symbolisiert den Nutzer, der Daten und Informationen aus dem Internet abrufen will. Der zweite Linux Rechner dient als Router, er kann somit Daten empfangen und entsprechend weiterleiten. Als drittes steht ein grafikfähiger Linux Rechner zur Verfügung.

Als erstes sollen die Rechner für das Netzwerk konfiguriert werden, das heißt man weißt den internen Netzwerkkarten IP-Adressen zu. Da wir Gruppe B waren entstanden demzufolge die IP-Adressen

- 2001:638:906:beef::11:2626 für den Client und
- 2001:638:906:beef::11:4656 für den Router.

Nachdem das Routing auch richtig eingestellt wurde, soll eine Routenverfolgung durchgeführt werden und die DNS abgehört werden. Zum Schluss soll die URL aus den Netzwerk-Dumps extrahiert werden.

In den Vorbereitungsmaterialien sind die entsprechenden Terminal-Befehle vorgegeben, diese werden daher nicht noch einmal extra erwähnt beziehungsweise protokolliert.

3. Erprobung

Wie bei der Vorgehensweise erwähnt, werden dem Client und dem Router die gebildeten Adressen zugewiesen. Zu beachten bei dieser Aufgabe ist der richtige Interface-Name der Netzwerkkarte. Sowohl bei Client als auch bei dem Router wird die Netzwerkkarte ethintern ausgewählt. Damit ist die zugewiesene IP-Adresse nur im internen Netz verfügbar. Beide lokale Adressen waren auch problemlos erreichbar. Die entsprechende Konfiguration vom Client findet man auf Seite A1 und vom Router auf Seite A2.

Das anpingen des Clients vom Router lief auch unproblematisch. Die Grenzen der Header findet man im Anhang auf Seite A3 bis A5. Mit Wireshark ist es auch einfach, die Hardware-Adressen der Netzwerkkarten herauszufinden. Im Protokollstapel von Ethernet II liest man sie einfach unter Destination und Source ab (siehe Seite A6). Im Vergleich zu der Ausgabe von ip addr show erkennt man auch keinen Unterschied. In Wireshark hat das Ziel die Adresse 00:0a:5e:63:cb:e9, was mit „link/ether“ der Netzwerkkarte ethintern vom Client übereinstimmt(siehe A1). Analog hat die Quelle die Adresse 00:c0:26:f1:e0:11, was wieder mit „link/ether“ der Netzwerkkarte ethintern vom Router übereinstimmt (siehe Seite A2). Hierbei handelt es sich um IEEE 8002-Adressen, was ein Standard für die Adressierung von Netzwerkschnittstellen ist. Die einzelnen Ziffern befinden sich in Hexadezimaldarstellung, das bedeutet jede Ziffer hat 4 Bits bzw. ein Block hat 1 Byte. Insgesamt ergeben sich 6 Byte oder umgerechnet 48 Bit. Die ersten 3 Byte dienen zur Firmenkennung, daraus lässt sich schließen, dass alle 3 Netzwerkkarten (eine hat der Client, zwei der Router) von unterschiedlichen Herstellern stammen. Bei den letzten 24 Bit handelt es sich um die Erweiterungskennung, die bei jeder Karte der gleichen Bauart unterschiedlich ist. Somit lässt sich eine Netzwerkkarte anhand ihrer MAC-Adresse stets genau identifizieren. Ein neuer Standard sind IEEE EUI-64-Adressen. Diese haben statt nur sechs insgesamt acht Byte. Die zusätzlichen 16 Bit werden zur Erweiterungskennung hinzugefügt, wodurch sich statt nur 2^{24} 2^{40} Karten adressieren lassen.

Auf Seite A4 sieht man den kompletten IPv6-Header. Die erste Ziffer (6) gibt die IP Versionsnummer an (in dem Fall IPv6). Die nächsten zwei Ziffern (00) stehen für die Traffic Class, was der Prioritätsvergabe entspricht. Die folgenden fünf Ziffern (00000) dienen dem Flow Label. Damit wird entschieden, wie Pakete behandelt werden, sprich Pakete mit dem gleichen Flow Label werden gleich behandelt. Die nächsten vier Ziffern (0040) zeigen die Payload Length (Länge des IPv6-Paketinhaltes in Byte). Danach kommen zwei Ziffern (3a) für den Next Header, womit man den Typ des nächsten Kopfdatenbereiches identifizieren kann. Danach kommen zwei weitere Ziffern (40) für das Hop Limit. Mit dem Hop Limit wird festgelegt, wie viele Stationen ein Paket passieren darf. Bei jedem Durchlaufen eines Routers verringert sich das Hop Limit um eins. Ist das Hop Limit gleich null, wird das Paket verworfen und geht verloren. Zum Schluss kommen noch 64 Zeichen. Die ersten 32 (200106380906beef0000000000114656) stehen für die Source Address und die restlichen für die Destination Address (200106380906beef0000000000112626), was selbsterklärend ist. Jedes Zeichen entspricht vier Bit, da sie sich in Hexadezimaldarstellung befinden. Insgesamt ergeben sich somit 40 Bytes bzw. 320 Bit für den IPv6 Header. Alle Pakete komplett findet man im Anhang auf Seite A7 bis A9.

Die Routingtabelle des Routers findet man im Anhang auf Seite A10. Es ist deutlich zu erkennen, dass die Defaultroute auf fe80::2e0:81ff:fe40:7768 gesetzt ist. Wird eine bestimmte Adresse angesprochen, so wird überprüft,

ob sich diese in der Routingtabelle befindet. Ist dies nicht der Fall, gibt es zwei Möglichkeiten. Bei nichtgesetzter Defaultroute kann die Adresse nicht angesprochen werden und es gibt einen Fehler. Bei gesetzter Defaultroute wird diese angesprochen. Bei der Adresse handelt es sich in der Regel um einen Router höherer Ordnung, der möglichweise mehr Informationen besitzt und eventuell die gesuchte Adresse mit den zugehörigen Schnittstellen kennt.

Der Client bekommt als Defaultroute die Adresse von dem Router. Das bedeutet, dass jede Adresse, die beim Client aufgerufen wird, an den Router weitergeleitet wird. Die Verbindung vom Client zum Router funktionierte vorher bereits problemlos. Nun überprüften wir das Außeninterface des Routers (2001:638:906:2:2e0:7dff:fe8c:416f), was auch sehr gut klappte (siehe Anhang Seite A11). Es traten auch keine Probleme auf, als wir www.kame.net und loris.tv anpingten.

Danach bestimmten wir die Route zum einen zu einen Rechner im Linuxpool, zum anderen zu anderen Rechnern in der Welt. Die Ergebnisse findet man in folgender Reihenfolge im Anhang auf Seite A12 und A13: Linuxrechner, ftp.uni-kl.de, www.prettygoodzero.de,www.kame.net. Der Übergang vom deutschen Forschungsnetz zu einem anderen Netzanbieter ist bei www.prettygoodzero.de von Zeile sechs zu sieben gut erkennbar, denn das das Präfix des Forschungsnetzes beginnt immer mit 2001:638. In Zeile sieben beginnt es mit 2001:6f8, was für den Netzanbieter Easynet steht. Bei www.kame.net erfolgt der Übergang wieder zwischen Zeile sechs und sieben. Zwischen Zeile acht und neun, elf und dreizehn erfolgen weitere Übergänge zwischen Netzbetreibern. Die ersten sechs Schritte der Route sind bei beiden Seiten auch gleich, was normal ist, da dies der typische Weg ist um eine Adresse außerhalb des Netzwerkes anzusprechen.

Im Anhang auf Seite A14 findet man die Hostanfrage an ipv6.google.com. Auf der darauffolgenden Seite steht die DNS-Antwort. Die MAC Adresse ist deutlich ablesbar: 00:e0:7d:8c:41:6f, wobei es sich wieder um eine IEEE 8002-Adresse handelt. Auch der Hersteller Netronix der Netzwerkkarte ist gut lesbar. Wie bereits weiter oben angesprochen, wäre er auch über die Firmenkennung 00:e0:7d identifizierbar. Den kompletten Paketstrom findet man im Anhang ab Seite A16.

Danach haben wir den Youbube Rechner eingerichtet. Das heißt wir gaben der Netzwerkkarte die IP Adresse

- 2001:638:906:beef:11:2627

und setzten die Defaultroute wieder auf den Router. Anschließend öffneten wir Iceweasel und starteten ein Video. Im Anhang auf Seite A22 befindet sich ein Screenshot der HTTP-GET-Anfrage des Youbube Videos. Die URI

- http://www.youtube.com/player_204?sst=10&at=2_1_5&len=550.537&mt=10.201&el=detailpage&art=13.21&event=ad&plid=AASKFka7-Ue2iAkB&v=2EbgsHKBPQw&ad_flags=0&ad_event=3

und der Host

- www.youtube.com\r\n

sind deutlich lesbar.

4. Schlussfolgerungen

Dieser Versuch lieferte einen guten Einblick in die Grundstruktur des Internets und Einrichten eines Netzwerkes. Die meisten Aufgaben verliefen wie geplant. Mit tcpdump und Wireshark ist ein mächtiges Tool gegeben um den Datenverkehr zu verfolgen und Schlüsse zu ziehen. Es zeigt sich auch, dass man beim Surfen durch das Internet keinesfalls anonym ist, so ist man über seine IP-Adresse stets identifizierbar und mit der MAC Adresse gibt man sogar Informationen über die verbaute Hardware preis.

Eine Aufgabe entsprach nicht unseren Erwartungen: URL-Extraktion aus Netzwerk-Dumps. Setzte man den Filter in Wireshark auf http.request.method==GET, so erhielt man 3 Einträge. Der einzige, der infrage kam, lieferte eine URI, die bei erneuter Eingabe im Browser kein Video lieferte, auch war das Video nicht darüber downloadbar. Setzte man den Filter nur auf http, so war die Liste der Einträge wesentlich länger. Dennoch war nirgends ein Eintrag mit .flv oder .mp4 zu finden. Dieser Zusammenhang lässt darauf schließen, dass etwas im Projekt nicht korrekt lief, obwohl das Youtube Video auf dem Rechner korrekt abgespielt wurde und die Route über den Router lief, der den Datenverkehr protokollierte. Vollständigkeitshalber hieß die URL

- http://www.youtube.com/watch?v=2EbgsHKBPQw,

worüber das Video mit JDownloader auch problemlos herunterladbar war.