Rechnernetze, Übungsblatt 6, Sommer 2024

Aufgabe 1

Sliding Window

Würde man nach dem Versenden eines jeden TCP-Pakets auf die Bestätigung des Empfängers warten, bevor man das nächste versendet, könnte man weder die Speicherfähigkeit des Mediums noch die Kapazität des Empfängers optimal auslasten. Um den Datenfluss zu verbessern, lässt der Sender daher die Übertragung einer bestimmten Anzahl an Paketen (Sliding Window) zu, bevor er eine Bestätigung zurückerwartet. Zur Ermittlung der Fenstergröße gibt es verschiedene Methoden

TCP Tahoe

Die Fenstergröße wird mit einem geringen Wert (1) initialisiert (slow start) und wird linear erhöht (AIMD (Addditive Increase / Multiplicative Decrease) bzw. bei einer Überlastung exponetiell gesenkt.

TCP Rheno

Um den Datenfluss weniger einbrechen zu lassen, wird bei einer Überlastung die Fenstergröße im Gegensatz zu TCP Tahoe nur halbiert.

TCP Vegas

TCP Vegas ermittelt die Round-Trip-Time (RTT) der Segmete, d.h. die Zeit, die zwischen dem Versenden und dem Erhalt der Bestätigung vergehen. Weicht die aktuelle Übertragungszeit von der RTT ab, werden Pakete direkt erneut versendet. Die Fenstergröße wird in Abhängigkeit von der RTT berechnet.

ISO/OSI-Modell

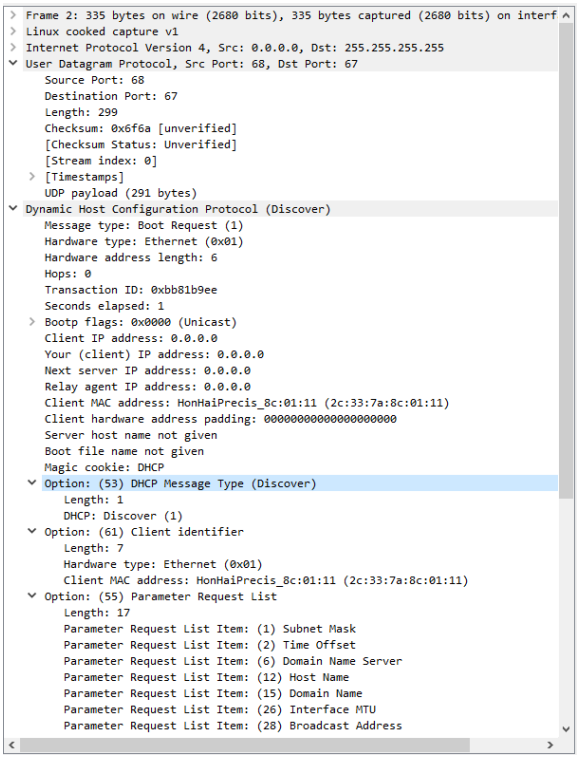
- IP (Internet Protocol): Network Layer, ermöglicht Routing der Pakete
- ICMP: Network Layer, da Bestandteil von IP, wird aber als eigenes Protokoll behandelt
- TCP: Transport Layer, da es eine Ende-zu-Ende-Verbindung zwischen zwei Rechnern ermöglicht und auf IP aufsetzt.
- UDP: Transport Layer, da es eine Ende-zu-Ende-Verbindung zwischen zwei Rechnern ermöglicht und auf IP aufsetzt.
- NTP (Network Time Protokoll): Application Layer, da Synchronisation der Zeit eine ein Anwendungsfall ist.
- ARP bzw. RARP: Link Layer, da für Adressauflösung im Ethernet zuständig

Aufgabe 2

Da DHCP-Pakete über die UDP-Ports 67 (IPv4 Server) und 68 (IPv4 Client) ausgetauscht werden habe ich den Capture-Filter *port 67 or port 68* genutzt. Um das Versenden / Empfangen von DHCP-Pakten zu provozieren, habe ich die WLAN-Verbindung meines PCs aus- und wieder eingeschaltet.

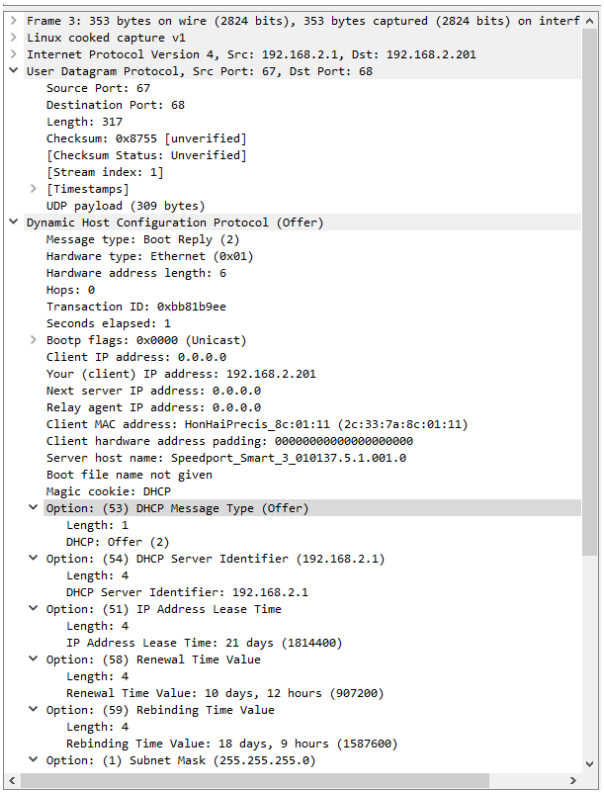
Anhand der Pakete lässt sich folgendes Verhalten nachvollziehen

- **Paket 2**



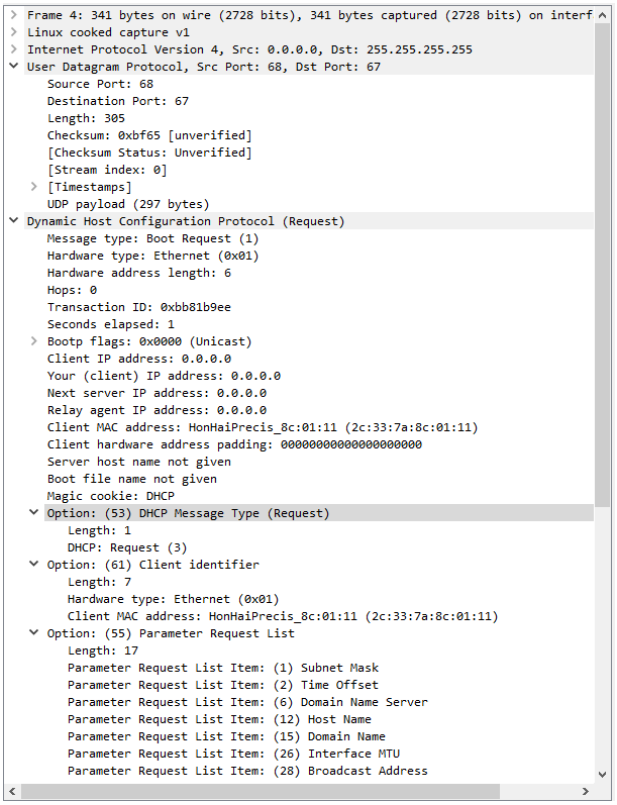
Der PC, der seine IP-Adresse noch nicht kennt (daher die nicht-routingfähige Quelladresse 0.0.0.0), sendet einen Broadcast (Zieladresse 255.255.255.255), um Adressangebote im Netz anzufragen. Diese DHCP-Nachricht ist vom Typ Discover.

- **Paket 3**



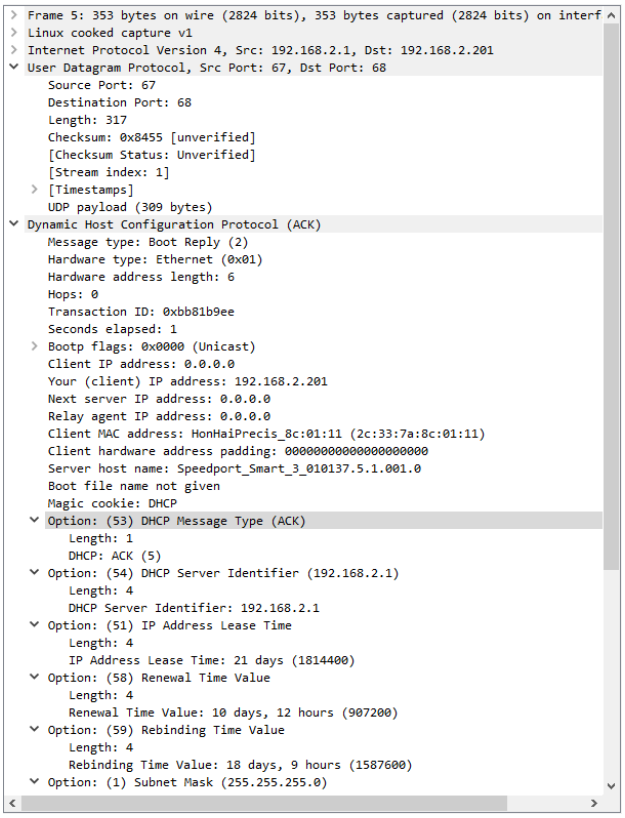
Daraufhin bietet der DHCP-Server dem PC die IP-Adresse 192.168.2.201 an. Diese DHCP-Nachricht ist vom Typ Discover.

- **Paket 4**



Der PC fragt eine Übernahme der angebotenen IP-Adresse beim DHCP-Server an. Diese DHCP-Nachricht ist vom Typ Request.

- **Paket 5**



- Der DHCP-Server bestätigt die Anforderung der IP-Adresse und räumt eine Lease-Zeit von 21 Tagen ein. Diese DHCP-Nachricht ist vom Typ ACK (Acknowledgement).

Aufgabe 3

Teilaufgabe a

```
julian@iupiter:~$ nmap -sP 192.168.2.1/24

Starting Nmap 7.80 ( https://nmap.org ) at 2024-07-17 13:36 CEST

Nmap scan report for speedport.ip (192.168.2.1)

Host is up (0.0018s latency).

Nmap scan report for iupiter (192.168.2.201)

Host is up (0.000045s latency).

Nmap scan report for 192.168.2.204

Host is up (0.085s latency).

Nmap done: 256 IP addresses (3 hosts up) scanned in 2.50 seconds
```

In meinem lokalen Netz befanden sich zu diesem Zeitpunkt drei Hosts. In A3a.pcapng sind massenweise ARP-Requests zu sehen, genauer gesagt eine für jede potentielle IP-Adresse eines Hosts.

Teilaufgabe b

```
julian@iupiter:~$ sudo nmap -O scanme.nmap.org

[sudo] password for julian:

Starting Nmap 7.80 ( https://nmap.org ) at 2024-07-17 13:42 CEST

Nmap scan report for scanme.nmap.org (45.33.32.156)

Host is up (0.18s latency).

Other addresses for scanme.nmap.org (not scanned):
2600:3c01::f03c:91ff:fe18:bb2f

Not shown: 996 closed ports

PORT      STATE SERVICE

22/tcp    open  ssh

80/tcp    open  http

9929/tcp  open  nping-echo

31337/tcp open  Elite

Aggressive OS guesses: HP P2000 G3 NAS device (93%), OpenWrt 12.09-
rc1 Attitude Adjustment (Linux 3.3 - 3.7) (93%), Linux 2.6.32 (92%),
Linux 3.7 (92%), Ubiquiti AirOS 5.5.9 (92%), Ubiquiti Pico Station
WAP (AirOS 5.2.6) (92%), Linux 2.6.32 - 3.13 (92%), Linux 3.13 or
4.2 (91%), Linux 2.6.32 - 3.1 (91%), Infomir MAG-250 set-top box
(91%)

No exact OS matches for host (test conditions non-ideal).

Network Distance: 20 hops
```

```
OS detection performed. Please report any incorrect results at
https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 7.56 seconds
```

Leider konnte Nmap das Betriebssystem nicht eindeutig identifizieren. Da die Vermutung mit der höchsten Wahrscheinlichkeit (NAS) abwegig ist, handelt es sich wohl um ein Linux-System. In A3b.pcapng lässt sich der Austausch diverser TCP-Pakete zwischen meinem PC und scanme.nmap.org (45.33.32.156) beobachten.

Teilaufgabe c

nmap.org wurde laut WHOIS-Daten am 18. Januar 1999 registriert.

Teilaufgabe d

Eine große Menge von IP-Adressen lässt sich mittels folgenden Befehls effektiv auf einen Schlag scannen, wenn sich diese im selben Netzwerk befinden.

```
julian@iupiter:~$ sudo nmap -sS 192.168.2.1/24

[sudo] password for julian:

Starting Nmap 7.80 ( https://nmap.org ) at 2024-07-17 17:48 CEST

Nmap scan report for speedport.ip (192.168.2.1)

Host is up (0.0024s latency).

Not shown: 996 closed ports

PORT     STATE    SERVICE

53/tcp   open     domain

80/tcp   open     http

5060/tcp filtered sip

8443/tcp open     https-alt

MAC Address: 44:FE:3B:74:FC:5A (Arcadyan)


Nmap scan report for 192.168.2.102

Host is up (0.0053s latency).

All 1000 scanned ports on 192.168.2.102 are closed

MAC Address: 88:83:22:97:76:C4 (Samsung Electronics)


Nmap scan report for 192.168.2.104

Host is up (0.012s latency).

Not shown: 995 closed ports

PORT     STATE SERVICE

80/tcp   open  http
```

```
443/tcp  open  https
631/tcp  open  ipp
8080/tcp open  http-proxy
9100/tcp open  jetdirect
MAC Address: F4:39:09:FE:57:6A (Hewlett Packard)

Nmap scan report for 192.168.2.198
Host is up (0.014s latency).
Not shown: 999 filtered ports
PORT     STATE SERVICE
5357/tcp open  wsdapi
MAC Address: 40:1A:58:02:70:80 (Unknown)

Nmap scan report for 192.168.2.204
Host is up (0.0058s latency).
Not shown: 999 closed ports
PORT     STATE    SERVICE
5060/tcp filtered sip
MAC Address: EE:5B:AC:A8:8F:93 (Unknown)

Nmap scan report for iupiter (192.168.2.201)
Host is up (0.0000040s latency).
All 1000 scanned ports on iupiter (192.168.2.201) are closed

Nmap done: 256 IP addresses (6 hosts up) scanned in 40.19 seconds
```

In A3d.pcapng lässt sich nachvollziehen, dass ähnlich wie in Teilaufgabe a ARP-Requests alle IP-Adressen gesendet werden. An alle Hosts, die tatsächlich existieren werden TCP-Requests an deren Ports gesendet.

Teilaufgabe e

Der SYN-Scan wird zum Scannen von TCP-Ports verwendet. Wie sich anhand A3d.pcapng nachvollziehen lässt, ist er effizient, indem er lediglich halbgeöffnete TCP-Verbindungen öffnet. Das heißt, an jedes Port wird ein SYN-Paket gesendet, je nachdem ob ein ACK-, ein RST-Paket oder (nach einer entsprechenden Anzahl von Versuchen) gar keine Antwort folgt, steht fest, ob es sich um einen offenen, geschlossenen oder gefilterten Port handelt.

Teilaufgabe f

- Port 80: http-Anfragen

- Port 443: https Anfragen
- Port 631: IPP (Internet Printing Protokol, dient zum Drucken)
- Port 9100: JetDirect (Protokoll zur Anbindung von Druckern)
- Port 5357: WSD-API (Web Services on Devices, Technologie von Microsoft zum Auffinden und Nutzen von Netzwerkgeräten wie Druckern)
- Port 5060: SIP (Session Initiation Protocol, in der IP-Telefonie genutzt)

Aufgabe 4

Der Algorithmus zur Erstellung der Routingtabellen funktioniert folgendermaßen:

- Im Initialisierungsschritt tut jeder Knoten folgendes:
  - Schreibe für jeden Nachbarknoten N in die Zelle „zu N via N“ die entsprechenden Kosten.
- In den darauffolgenden Aktualisierungsschritten tut jeder Knoten folgendes:
  - Sende die eigene Routingtabelle an jeden Nachbarknoten.
  - Erstelle folgendermaßen eine neue Routingtabelle:
    - Schreibe für jeden Nachbarknoten N in die Zelle „zu N via N“ die entsprechenden Kosten.
    - Für jeden Nachbar X: Schreibe in jede Zelle „zu Y via X“ die Kosten der günstigsten Route von X nach Y zuzüglich der Kosten zu X. Falls die Routingtabelle von X keine Route zu Y kennt, bleibt die Zelle leer.

Im Gegensatz zum Link-State-Verfahren werden Informationen nur zwischen benachbarten Routern ausgetauscht, sodass Änderungen im Netz nur schrittweise propagiert werden. Ändert sich die Topologie eines Netzes häufig, empfiehlt sich hingegen das Link-State-Verfahren. Hierbei speichert jeder Router in einer Datenbank die gesamte Netztopologie. Änderungen werden per Multicast allen Routern mitgeteilt, sodass sie ihre Datenbanken aktualisieren können.

Teilaufgabe a

Von x	Via x	Via y	Via z
Zu x			
Zu y		2	
Zu z			7

Von y	Via x	Via y	Via z
Zu x	2		
Zu y			
Zu z			1

Von z	Via x	Via y	Via z
Zu x	7		
Zu y		1	
Zu z			

Von x	Via x	Via y	Via z
Zu x			
Zu y		2	8
Zu z			7

Von y	Via x	Via y	Via z
Zu x	2		8
Zu y			
Zu z	9		1

Von z	Via x	Via y	Via z
Zu x	7	3	
Zu y	9	1	
Zu z			

Teilaufgabe b

Von x	Via x	Via y	Via z
Zu x			
Zu y		7	
Zu z			7

Von y	Via x	Via y	Via z
Zu x	7		
Zu y			
Zu z			1

Von z	Via x	Via y	Via z
Zu x	7		
Zu y		1	
Zu z			

Von x	Via x	Via y	Via z
Zu x			
Zu y		7	8
Zu z		8	7

Von y	Via x	Via y	Via z
Zu x	7		8
Zu y			
Zu z	14		1

Von z	Via x	Via y	Via z
Zu x	7	8	
Zu y	14	7	
Zu z			

Teilaufgabe c

Im ersten Aktualisierungsschritt nach dem Ausfall, bemerkt C die fehlende Verbindung zu D, wohingegen A und B noch die alte Routing-Tabelle von C erhalten, welche von einer intakten Verbindung zu C ausgeht.

Im darauffolgenden Aktualisierungsschritt erlangen A und B jedoch Kenntnis von dem Ausfall, da sie nun eine Routingtabelle von C erhalten, die keine Verbindung zu D mehr aufführt.