Lukas Kohlhaas 1538421 Rechnernetze Übung 6

Aufgabe 1)

Das Sliding-Window ist ein Grundkonzept der TCP Datenübertragung und beschreibt im Grunde genommen wie viele Pakete der Sender versenden darf, ohne dafür bereits ACK Pakete vom Empfänger zurück bekommen zu müssen. Würde man für jedes einzelne Paket ein ACK Paket zurück bekommen müssen, würde die Datenübertragung zu lange dauern, weswegen ein Sliding-Window von maximal n Paketen gesetzt wird, die der Sender im Vorraus verschicken kann ohne sofort eine Bestätigung für jedes dieser Pakete zu brauchen. Sollten n Packete verschickt aber nicht quittiert worden sein, so blockt der Sender das Versenden der Pakete, bis weitere Quittungen zurück gekommen sind.

TCP Tahoe ist ein früher Ansatz um ein gutes Sliding-Window zu finden. Bekommt man schnell genug ACK Pakete zurück steigert TCP Tahoe die Übertragungsrate linear. Sollten allerdings 3 „Dublicate ACKs“ zurück kommen, wird die Übertragungsrate wieder auf das absolute minimum reduziert und neu hoch skaliert.

TCP Reno macht im Prinzip das Gleiche wie TCP Tahoe, allerdings wird bei 3 „Dublicate ACKs“ die Größe des Sliding-Windows nur halbiert und danach kurz vor der vorherigen Grenze die Fenstergröße nur langsamer erhöht um eine konstantere Übertragungsrate zu gewährleisten.

TCP Vegas verbessert das Protokoll weiter, indem über den Abstand zwischen Send und dem zugehörigen ACK eine Round-Trip-Time (RTT) errechnet wird. Aus dieser RTT wird ein Sliding-Window abgeleitet. Dadurch kann TCP Vegas aus einer aktuell größeren Übertragungszeit als die RTT und einem doppeltes ACK Paket schnell feststellen, dass ein Retransmit nötig ist. Dadurch kann gegenüber TCP Reno etwa 40% mehr Durchsatz gewährleistet werden.

Ich beschränke mich bei den Protokollen auf die, die auch aktiv Bestandteil der Vorlesung waren. http, smtp, ftp und alles was nicht direkt Inhalt der Vorlesung war, aber trotzdem erwähnt wurde, lasse ich entsprechend bewusst weg:

IP: Teil des Network Layers. Jedes Gerät eines Netzwerkes hat eine eindeutige Adresse, die zum Routing verwendet wird.

ICMP: Teil des Network Layers. Verschickt Informative Meldungen und Fehlermeldungen per IP.
(R)ARP: Teil des Network Layers. Nutzt IP Adresse um Netzwerkadresse zu

finden bzw. anders herum bei RARP (Reverse ARP).

UDP: Teil des Transport Layers. Wird verwendet um Datagramme zu verschicken

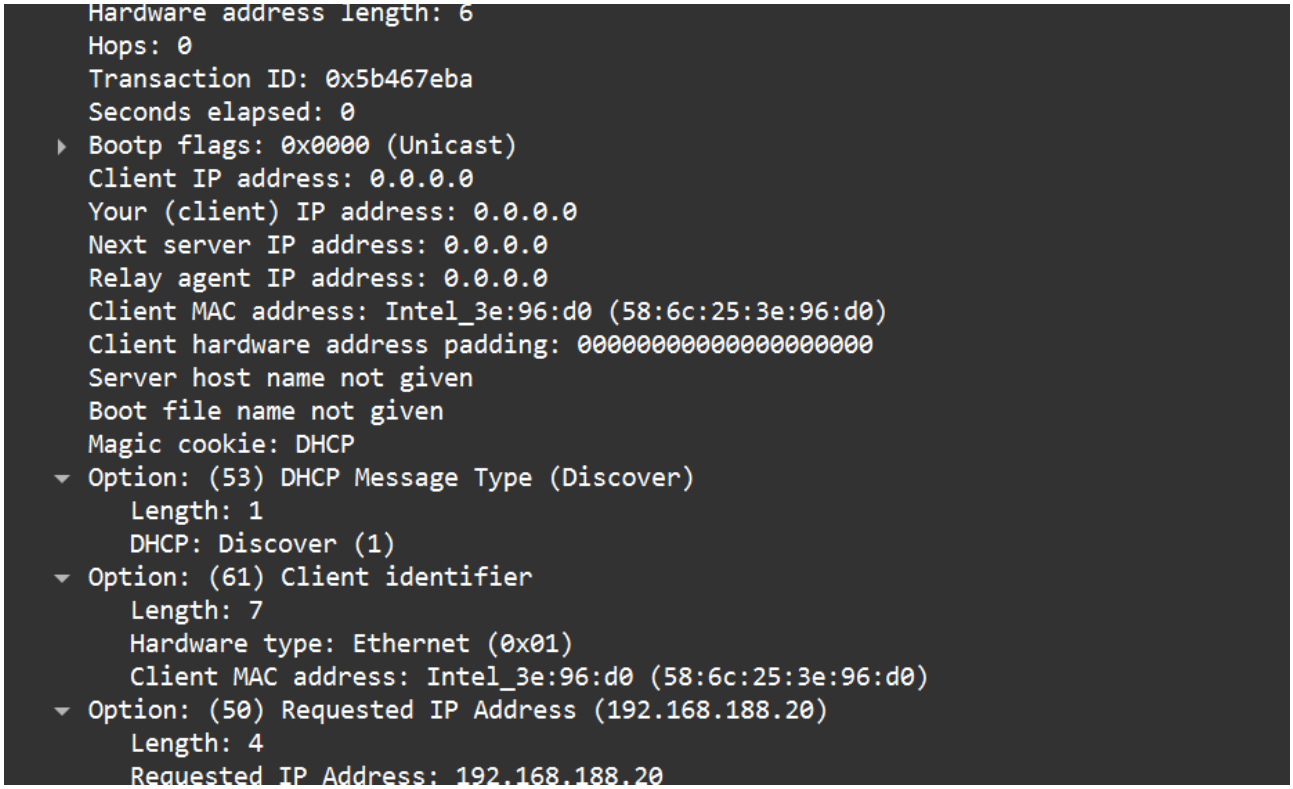
TCP: Teil des Transport Layers. Wird verwendet um eine Verbindung zwischen zwei Geräten aufzubauen und darüber Pakete zu verschicken.

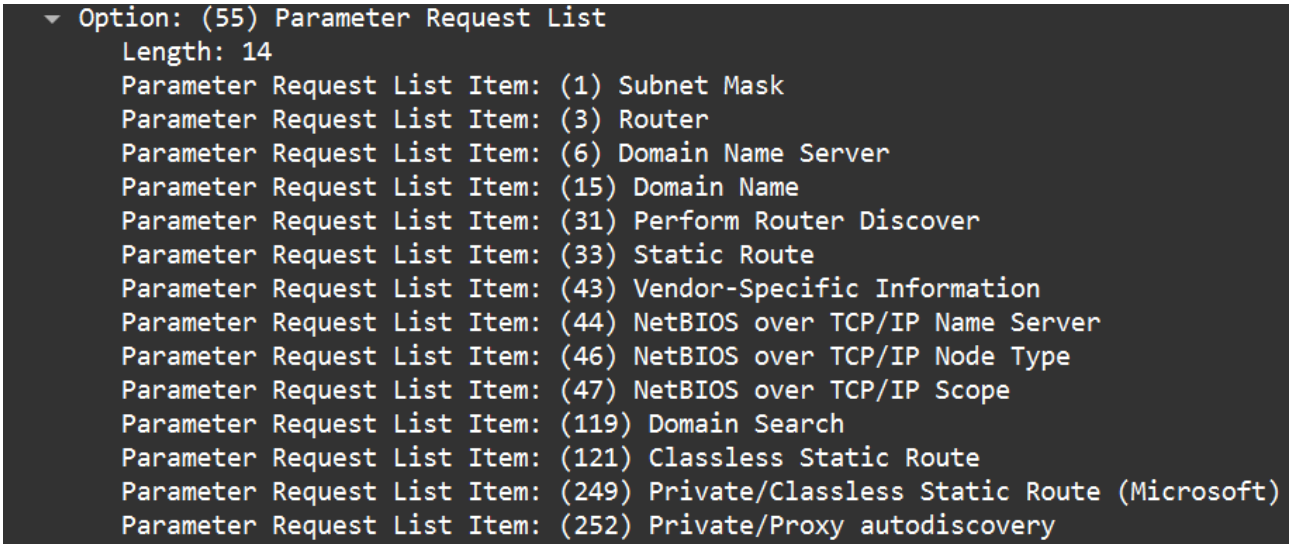
DNS: Entweder Ebene 5 oder 7. Das aufschlüsseln von IP Adressen zu klaren Domain Namen ist ein Fall für das Application Layer, ist aber weniger praktisch in der Verwendung und könnte daher auch ins Session Layer gehören.

DHCP: Ebene 5 oder 7. Ähnlich wie bei DNS ist DHCP klar ein Anwendungsfall aber auch passiver Teil einer Sitzung.

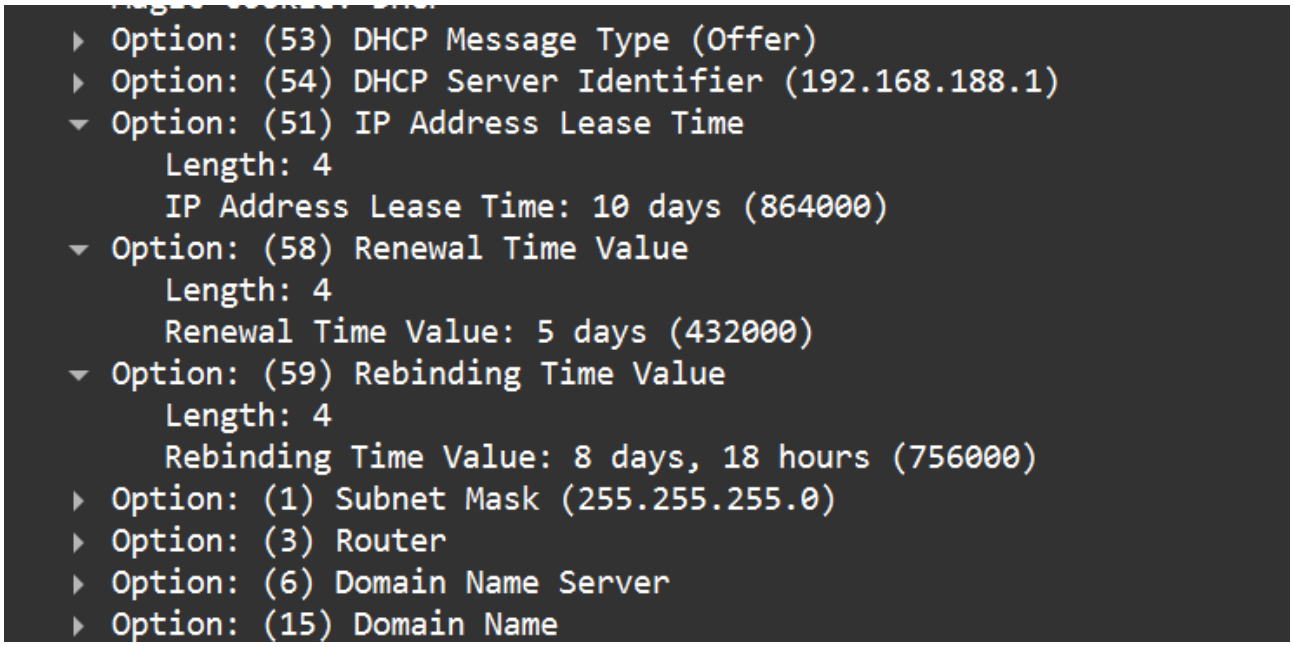
NAT: Network Layer, da IP Adressen für Lokale Netzwerke in den Headern geändert werden

Aufgabe 2) Benutzt man im Terminal eines Gerätes mit Windows Betriebssystem den Command „ipconfig /release“, so gibt das Gerät seine aktuelle IP Adresse im lokalen Netzwerk frei und fragt kurz darauf mit einem DHCP Discover Broadcast ob es im Netzwerk einen DHCP Server gibt, der eine IP Adresse anzubieten hat, sowie nach allen möglichen Diensten, die das Gerät kennen muss, um im Netzwerk zu funktionieren.





Im vom DHCP Server zurück kommenden DHCP Offer Paket befinden sich 3 besonders interessante Werte:



„IP Address Lease Time“ gibt an wie lange das Gerät seine lokale IP Adresse behalten darf, bevor diese frei gegeben wird. Dies kann allerdings verhindert werden indem das Gerät bei Ablauf des „Renewal Time Values“ einen neuen DHCP Request an diesen DHCP Server verschickt. Bei Ablauf des „Rebinding Time Value“ passiert im Grunde das Gleiche, allerdings werden diesmal ALLE verfügbaren DHCP angefragt. Weiterhin werden dem Gerät natürlich auch eine IP Adresse, aber auch ein Router, ein DNS Server etc angeboten. Im darauffolgenden DHCP Request Paket, bestätigt das Gerät das Angebot mit allen gegebenen Parametern, woraufhin der DHCP Server, mit einem DHCP ACK Paket, den Request bestätigt.
(Siehe Wireshark Capture Datei)

Aufgabe 3)

a) Mit nmap -sn 192.168.188.0/24 habe ich mit Ping Scan überprüft wie viele Hosts sich in meinem localen Netzwerk zurück melden. In meinem Fall sind das 8 gewesen.

b) Mit nmap -O scanme.nmap.org kann man den Betriebssystem Scan machen. Dieser hat bei mir eine Vermutung mit 87% Sicherheit ergeben, dass scanme.nmap.org ein Linux System verwendet.

c) Mit whois -v nmap.org kann man sich einige Informationen zu nmap.org ausgeben lassen. Darunter „Creation Date: 1999-01-18T05:00:00.0Z“.

d) Mit nmap -p <Startport>-<Endport> -T5 <IPAdresse> kann man mit der schnellsten Option -T5 mit -p alle ausgewählten Ports scannen.

e) Mit einem SYN Scan verschickt man Verbindungsanfragen an die TCP Ports. Diese Antworten entweder mit ACK oder mit RST. Ein Port der mit ACK antwortet ist mindestens gefiltert oder offen, ein Port der mit RST antwortet ist komplett geschlossen. Dieser Scan ist deutlich schneller als ein kompletter TCP Scan und wird deswegen auch verwendet.

f) Mit nmap -p 1-65535 -v --open <IPAdresse> habe ich einige Systeme im lokalen Netz gescant und habe leider kein eindeutiges Muster bei den geöffneten Ports gefunden mit Ausnahme einiger weniger offener Ports für Microsoft Services.

Aufgabe 4)
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		5	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			

Von x	Via x	Via y	Via z
Zu x			
Zu y		2	8
Zu z		5	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			

b) Ja, der kostengünstigste Pfad von z nach x kostet jetzt 7

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	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	1	
Zu z			

c) Die anderen Router bemerken dass D nicht mehr erreichbar ist, sobald sie die Routingtabellen untereinander abgleichen und aktualisieren. Hierbei bemerkt zuerst C das D nicht mehr erreichbar ist. Bei Deren nächster Aktualisierung nach Cs Aktualisierung, bemerken B und A, dass D nicht mehr erreichbar ist, da sie jetzt beim Abgleichen ihrer Routingtabelle mit der Routingtabelle von C bemerken, dass C D nicht mehr erreicht und Sie deshalb D auch nicht mehr erreichen können.