Rechnernetze - Übung 6: Jonas Bast (1692288)

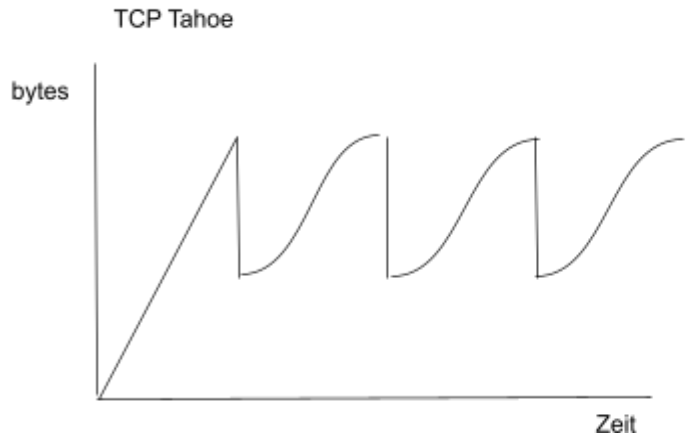
Aufgabe 1:

Sliding-Window:

Das Sliding-Window-Protokoll ist ein Mechanismus in TCP zur Flusskontrolle. Es ermöglicht dem Sender, mehrere Datenpakete ohne sofortige Bestätigung (ACK) zu senden. Die Anzahl der unbestätigten Pakete wird durch das "Fenster" bestimmt. Sobald ACKs empfangen werden, "rutscht" das Fenster weiter, und neue Pakete dürfen gesendet werden. Dies verbessert die Effizienz bei hoher Latenz, da nicht nach jedem Paket auf eine Antwort gewartet werden muss.

TCP Tahoe:

Tahoe ist eine frühe TCP-Variante mit grundlegender Staukontrolle. Nach einem Paketverlust (z.B. durch Timeout) wird das Congestion Window auf 1 reduziert (Slow Start), und das Netzwerk wird langsam wieder "aufgefüllt". Tahoe nutzt Slow Start, Congestion Avoidance und einen Timeout-basierten Rückfall.



TCP Reno:

Reno erweitert Tahoe um "Fast Retransmit" und "Fast Recovery". Wenn drei gleiche ACKs empfangen werden, interpretiert Reno das als Paketverlust und sendet das vermisste Paket sofort erneut (Fast Retransmit), ohne auf einen Timeout zu warten. Danach reduziert es das Fenster halbiert (Fast Recovery), anstatt ganz zurückzusetzen.

TCP Vegas:

Vegas versucht, Überlastung zu vermeiden, bevor Verluste auftreten. Es misst die RTT (Round Trip Time) und vergleicht die Erwartete mit der tatsächlichen Durchsatzrate. Ist die tatsächliche Rate deutlich kleiner, deutet das auf Stau hin. Vegas passt das Fenster also proaktiv an und reagiert sensibler auf Verzögerungen statt nur auf Paketverluste.

Zweck dieser Techniken:

Alle genannten Verfahren dienen der effizienten Nutzung des Netzwerks unter gleichzeitiger Vermeidung von Überlastung. Sliding-Window erhöht die Ausnutzung der Leitungskapazität, die TCP-Varianten steuern das Sendeverhalten in Abhängigkeit von Netzwerkbedingungen.

Liste der Protokolle und ihre OSI-Schicht:
- Ethernet - Schicht 2 (Data Link): regelt MAC-Zugriff, Rahmenstruktur
- IP (IPv4) - Schicht 3 (Network): logische Adressierung, Routing
- ICMP - Schicht 3 (Network): Fehlerdiagnose (Ping, Traceroute)
- ARP/RARP - Schicht 3 (Network): Adressauflösung (MAC <-> IP)
- UDP - Schicht 4 (Transport): verbindungslos, minimaler Overhead
- TCP - Schicht 4 (Transport): verbindungsorientiert, zuverlässig
- DNS - Schicht 7 (Application): Namensauflösung
- DHCP - Schicht 7 (Application): automatische IP-Konfiguration
- NAT - Schicht 3 (Network, nicht standardkonform): IP-Adressübersetzung

Aufgabe 2:

a) Befehl: nmap -sn 192.168.1.0/24
Ausgabe: NMAP done: 256 IP addresses (0 hosts up) scanned in 239.25 seconds

b) Befehl: sudo nmap -O scanme.nmap.org
Ausgabe: Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.19

c) Befehl: whois nmap.org
Ausgabe: Creation Date: 1999-01-18T05:00:00.0Z

d) Befehl: nmap -sS -T4 -p 1-1000 192.168.1.0/24
Erklärung: -sS: SYN-Scan – schnell und unauffällig (siehe Teil e).
-T4: Timing-Stufe 4 – aggressiver Scan, schneller als Standard.
-p 1-1000: Scan nur der ersten 1000 Ports (häufig genutzte Ports).
192.168.1.0/24: Scan des gesamten Subnetzes.

e) Befehl: nmap -sS <Addresse>
Erklärung: SYN-Scan ist ein halb-offener Scan (auch "stealth scan" genannt).
Er sendet ein SYN-Paket an einen Port.
- Antwort ist SYN/ACK → Port offen.
- Antwort ist RST → Port geschlossen.
- Keine Antwort oder ICMP → evtl. gefiltert.
Verbindung wird nicht vollständig aufgebaut (kein ACK), daher schwerer zu erkennen in Logs

f)

Häufigste Offene Ports	Service
TCP	ssh http

	nping-echo Elite

Aufgabe 3:
Da DHCP nicht ständig im Netzwerk läuft, musste ich einen DHCP-Prozess auslösen, indem ich die WLAN-Anbindung meines Laptops aus- und angeschaltet habe. Um nur DHCP-Pakete aufzufangen, habe ich als capture-filter (port 67 or port 68) genutzt, da diese UDP Protokolle immer über Port 67 oder Port 68 kommunizieren.

Paket 1:
Der Client (02:ac:d0:1e:0c:57) hat eine DHCP Offer-Nachricht mit der IP-Adresse 192.168.178.66 erhalten und sendet nun diese Request-Nachricht, um die IP zu reservieren. Die IP-Adresse ist im Requested IP-Feld eingetragen. Die Quelladresse 0.0.0.0 zeigt, dass der Client noch keine eigene IP besitzt. Gesendet wird an die Broadcast-Adresse, weil die Kommunikation mit dem Server noch nicht direkt möglich ist.
Die Transaction ID verknüpft das Paket logisch mit den anderen DHCP-Paketen. Der Client fordert zusätzlich bestimmte Parameter vom Server an (z. B. DNS, Gateway), die später in der ACK-Nachricht bestätigt werden.

Paket 2:
Dieses DHCP ACK-Paket ist die letzte Phase der Adressvergabe. Mein Computer bekommt vom DHCP-Server die Adresse 192.168.178.66 zugewiesen, zusammen mit wichtigen Netzwerkparametern wie Subnetzmaske, Gateway und DNS-Server. Die Kommunikation läuft über Broadcasts und dedizierte DHCP-Ports (UDP 67/68). Die Transaktions-ID verbindet alle zugehörigen Pakete logisch miteinander.