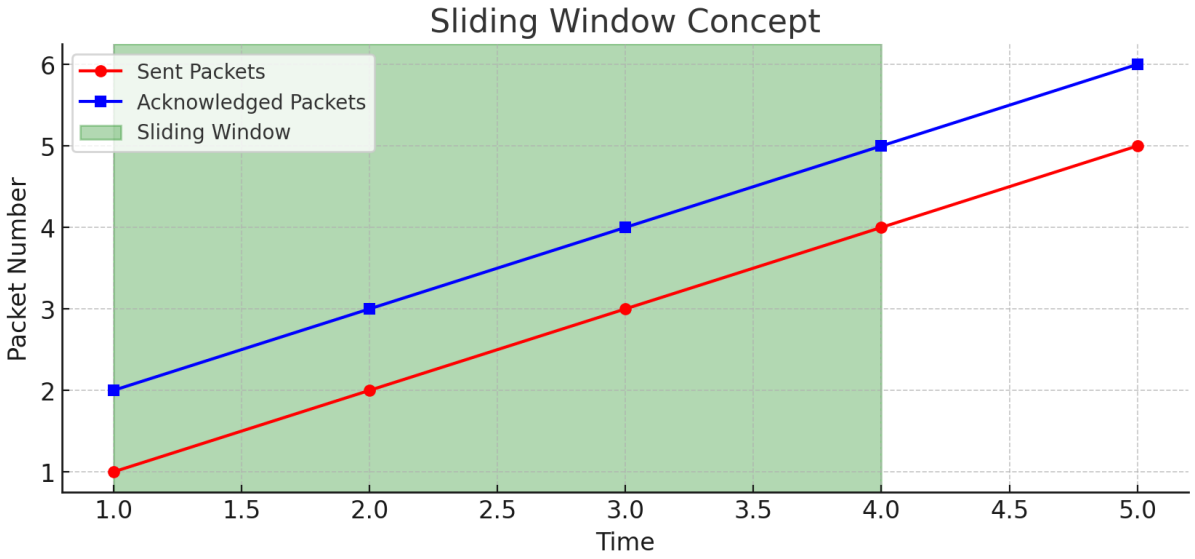
Rechnernetze Übung 06 – Philipp Seibel 1296632

Aufgabe 1

Sliding Window ist ein Mechanismus zur Flusskontrolle in TCP, der es dem Sender erlaubt, mehrere Pakete zu senden, bevor eine Bestätigung empfangen wird. Dies erhöht den Durchsatz, indem es die Wartezeit auf Bestätigungen reduziert.



TCP Tahoe verwendet Slow Start (Größe des Sende-Fensters erhöht sich exponentiell), Congestion Avoidance (verlangsamt Wachstum des Fensters auf lineare Rate, um Überlastungen zu vermeiden) und Fast Retransmit (ermöglicht schnelles Wiederholen von Paketen, wenn ein Verlust erkannt wird). Bei Paketverlust setzt es das Congestion Window zurück und beginnt erneut mit Slow Start.

TCP Reno erweitert Tahoe um Fast Recovery. Bei drei doppelten ACKs halbiert es das Congestion Window statt es auf 1 zu setzen und überspringt Slow Start. Dies führt zu einer schnelleren Wiederherstellung der Sendeleistung.

TCP Vegas führt eine Überlastungserkennung ein. Es überwacht die Round-Trip Time (RTT) von Paketen, um die optimale Fenstergröße zu berechnen. Durch frühzeitige Erkennung von Überlastungen kann Vegas die Fenstergröße anpassen, bevor es zu Paketverlusten kommt.

Protokolle und ISO/OSI-Modell:

- Schicht 1: Physical Layer
    - In der Vorlesung genannte Beispiele:
        - V.24, RS-232
- Schicht 2: Link Layer
    - Ethernet (LAN-Protocol)
        - Stellt den Rahmen für physikalische Übertragung der Daten bereit
    - Weitere in der Vorlesung genannte Beispiele:
        - CSMA/CD
        - HDLC
- Schicht 3: Network Layer
    - IP (Internet Protocol)
        - Grundlegendes Protokoll des Internets, sorgt für Adressierung und Routing von Paketen zwischen Computernetzwerken
            - Warum Schicht 3? Nutzt Ethernet und ist ein Host-to-Host Protokoll
- Schicht 4: Transport Layer
    - TCP (Transmission Control Protocol)
        - Zuverlässige, verbindungsorientierte Datenübertragung
            - Warum Schicht 4? Nutzt IP und erweitert um TCP-Portnummern
    - UDP (User Datagram Protocol)
        - Verbindungsloses Protokoll mit schneller, unzuverlässiger Datenübertragung
            - Warum Schicht 4? Nutzt IP und erweitert um UDP-Portnummern
    - ICMP (Internet Control Message Protocol)
- Schicht 5: Session Layer
    -
- Schicht 6: Presentation Layer
    - In der Vorlesung genannte Beispiele:
        - XDR (SUN-RPC), ASN.1, SOAP, JSON
- Schicht 7: Application Layer
    - DNS (Domain Name System)
        - DNS wandelt menschenlesbare Domainnamen in IP-Adressen um und erleichtert so die Navigation im Internet
    - DHCP (Dynamic Host Configuration Protocol)
        - Ermöglicht automatisierte IP-Vergabe in einem Netzwerk
            - Warum Schicht 7? DNS und DHCP haben anwendungsorientierte Funktionen und arbeiten unabhängig von unteren Schichten
    - Weitere in der Vorlesung genannte Beispiele:
        - FTP (File Transfer Protocol)
        - SSH (Secure Shell)
        - NFS (Network File System)
        - NIS (Network Information System)
        - SMTP (Simple Mail Transfer Protocol), X.400, POP.3, IMAP
        - HTTP (Hypertext Transfer Protocol)

Aufgabe 2: DHCP

Um DHCP-Pakete zu erzeugen, kann man die Netzwerkverbindung trennen und erneut verbinden. Hauptsächlich gibt es dabei 4 Transaktionen:

- DHCP Discover: Der Client sucht nach einem DHCP-Server (Broadcast-Anfrage)
    - Auffälligkeit: Client IP Address: 0.0.0.0 (Client hat noch keine IP-Adresse)
    - Weitere Informationen: eindeutige Transaction ID und Hardware-MAC-Adresse
- DHCP Offer: Der Server bietet eine IP-Adresse an
    - Auffälligkeit: Server bietet Client eine IP-Adresse an (yiaddr)
    - Weitere Informationen: IP-Adresse des DHCP-Servers und Lease Time
- DHCP Request: Der Client akzeptiert die angebotene IP-Adresse
    - Auffälligkeit: Der Client fordert die IP-Adresse explizit an
    - Weitere Informationen: DHCP-Server-Adresse und Client MAC Address
- DHCP Acknowledge: Der Server bestätigt die IP-Zuweisung
    - Auffälligkeit: Es werden auch Subnet Mask und Standard-Gateway angegeben
    - Weitere Informationen: Lease Time und die Client-IP-Adresse

Aufgabe 3:

a) Wie viele Hosts befinden sich in ihrem lokalen Klasse-C-Netz?
   nmap -sn 192.168.1.0/24
   Nmap done: 256 IP addresses (256 hosts up) scanned in 64.84 seconds
b) Welches Betriebssystem wird von scanme.nmap.org verwendet?
   nmap -O scanme.nmap.org
   Aggressive OS guesses: Linux 2.6.32 (88%), Ubiquiti WAP (Linux 2.6.32) (88%), Netgear ReadyNAS 3200 NAS device (Linux 2.6) (87%), F5 3600 LTM load balancer (85%), Linux 2.6.11 - 2.6.18 (85%), Netgear WNDAP660 WAP (Linux 2.6.36) (85%)
   No exact OS matches for host (test conditions non-ideal).
c) An welchem Datum wurde die Webseite nmap.org registriert?
   whois nmap.org
   Creation Date: 1999-01-18T05:00:00Z
d) Wie kann man möglichst effektiv eine größere Menge an Adressen nach offenen TCP-Ports scannen?
   Argumente: -T4 (aggressives Timing), -A (Erkennung OS & Dienste), -v (ausführliche Ausgabe)
e) Wie funktioniert der SYN-Scan und für was kann man ihn verwenden?
   Nmap -sS: halboffener Scan, wenn der Port offen ist, antwortet der Host mit SYN-ACK, Nmap sendet RST-Paket, um Verbindung zu beenden, ohne vollständige TCP-Verbindung aufzubauen
f) Welches sind die offenen Ports, die bei ihren bisherigen Nmap-Scans am häufigsten auftreten, und wofür werden sie verwendet?
   80 (http) und 443 (https), aber auch 22 (ssh), 25 (SMTP – Mails) und 53 (DNS)

Aufgabe 4:

a)

Von x	Via x	Via y	Via z	Von y	Via x	Via y	Via z	Von z	Via x	Via y	Via z
Zu x				Zu x	2			Zu x	7		
Zu y		2		Zu y				Zu y		1	
Zu z			7	Zu z			1	Zu z			

Von x	Via x	Via y	Via z	Von y	Via x	Via y	Via z	Von z	Via x	Via y	Via z
Zu x				Zu x	2		8	Zu x	7	3	
Zu y		2	8	Zu y				Zu y	9	1	
Zu z		3	7	Zu z	9		1	Zu z			

Von x	Via x	Via y	Via z	Von y	Via x	Via y	Via z	Von z	Via x	Via y	Via z
Zu x				Zu x	2		8	Zu x	7	3	
Zu y		2	8	Zu y				Zu y	9	1	
Zu z		3	7	Zu z	9		1	Zu z			

b)

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

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

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

c)

Es fällt erst auf, wenn man Router D erreichen möchte. In einer Routing-Tabelle wird kein anderer über D angesteuert bzw. bildet den kürzesten Pfad.