

Übung Netzwerk-, Transport- und Applikationsschicht

1. Transportschicht

- (1.1) (2 Punkte) Was sind die Eigenschaften der verbindungsorientierten Kommunikation im Vergleich zur verbindungslosen Kommunikation?

- (1.2) (3 Punkte) Ordnen Sie den folgenden Protokollen die Eigenschaften verbindungslos oder verbindungsorientiert zu, indem Sie genau ein Kreuz in der entsprechenden Spalte einer jeden Zeile setzen:

Protokoll	verbindungslos	verbindungsorientiert
IP		
TCP		
UDP		

- (1.3) (5 Punkte) Ordnen Sie den folgenden Anwendungen ein geeignetes Transportprotokoll (TCP/UDP) zu. Bei einigen Fällen ist die Entscheidung u. U. nicht eindeutig. Begründen Sie daher kurz Ihre Wahl!

Anwendung	TCP/UDP	Begründung
Versand eines Bildes per Messenger		
Webseite abrufen		
Online-Videos anschauen		
LAN-Spiel		
Domain Name Service		

2. Transportschicht - Sliding-Window

Es werde eine Verbindung zwischen zwei Rechnern aufgebaut. Der Empfangsrechner habe eine Fenstergröße von 4 Frames ($W_r = 4$). Gehen Sie davon aus, dass alle Pakete korrekt empfangen werden und das Sliding- Window-Verfahren verwendet wird, um einen maximalen Durchsatz zu erreichen.

(2.1) (6 Punkte) Zeichnen Sie bitte ein Nachrichtendiagramm für den Versand eines Datenstromes der aus insgesamt 8 Frames besteht inklusive Verbindungsaufbau und -abbau. Fügen Sie die folgenden Daten zu den einzelnen Nachrichten des Nachrichtendiagrammes hinzu:

- Handelt es sich um ein SYN, ACK oder FIN-Paket?
- Geben Sie jeweils die Sequenznummern der Pakete hinzu.

- (2.2) (4 Punkte) Beschreiben Sie kurz anhand von zwei Verfahren, wie im o.g. Beispiel mit Problemen bei fehlerhaftem Datenempfang umgegangen werden kann.

- (2.3) (3 Punkte) Die Definition der Größe des Empfangswindows durch den Empfänger ist eine Methode der Flusskontrolle. Begründen Sie dies kurz. Wo liegt der Unterschied zur Staukontrolle?

3. Network Address Translation

Gegeben ist der folgende Paket-Anfang beginnend mit dem Header des Network Layers.

0	3	4	7	8	15	16	23	24	31
4	5	0x00			0x3c				
0x4068					0	1	0	0x00	
0x40		0x06			0x8c2b				
192.168.91.200									
193.98.144.85									
45138					25				
0xe428c3be									
0x00000000									
0xa	0x00		0	0	0	0	1	0	0xfaf0
0x6e57					0x0000				
Daten									
...									

- (3.1) (3 Punkte) Nachdem der NAT-Router mit der öffentlichen IP 139.30.5.23, der dieses Paket in das Internet weiterleitet, das Paket herausgeschickt hat, befinden sich folgende Einträge in seiner NAT-Tabelle:

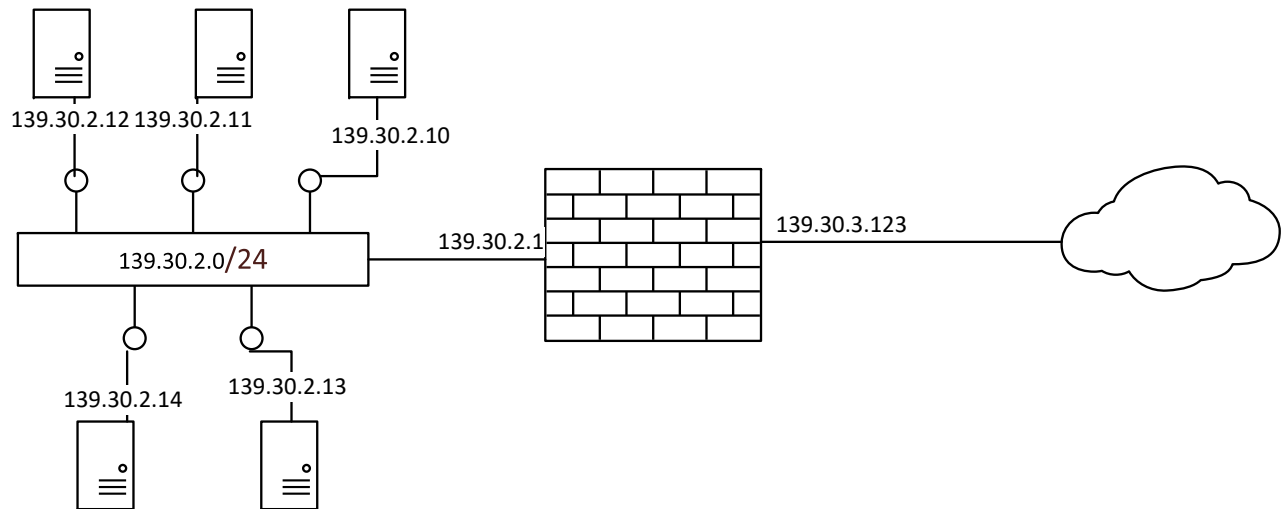
Lokale IP	Lokaler Port	Globaler Port
192.168.91.199	15645	51800
192.168.91.200	45137	51801
192.168.91.200	45138	51802

Welche Paketfelder hat der Router wie vor dem Versenden wie geändert? Ignorieren Sie bitte die Checksummen.

- (3.2) (7 Punkte) Wie könnte das Antwortpaket zu diesem Paket aussehen, das der Router empfangen wird?

4. Firewalls

Sie administrieren ein Netz, das wie folgt aufgebaut ist:



Nun sollen Sie eine Firewall anlegen, die nach dem Statefull Packet Inspection (SPI) Prinzip arbeitet.

(4.1) (1 Punkt) Welche Portnummer verwendet SSH?

(4.2) (9 Punkte) Ihre Aufgabe ist, Regeln zu erstellen, die von außen nur SSH-Requests durchlassen. Alle Pakete aus dem lokalen Netz dürfen ungehindert passieren.

Source IP	Source Port	Destination IP	Dest. Port	Protokoll	State	Allow / Block

5. HTTP

(5.1) (3 Punkte) Erklären Sie kurz wesentliche Unterschiede in der Kommunikation zwischen den HTTP-Versionen 1.0, 1.1 und 1.1 inkl. Pipelining.

(5.2) (3 Punkte) Vergleichen Sie kurz den GET, HEAD und POST-Request in HTTP.
