

Aufgabe 01

1. Wozu dienen IP-Adressen?

Die Internet Protocol Address, kurz IP-Adresse, ist eine Netzwerkadresse, die für jedes Gerät in einem Netzwerk nur einmal vergeben werden darf. Das ist notwendig, damit Datenpakete richtig adressiert und zugestellt werden können.

Eine IP-Adresse ist das eindeutige Identifikationsmerkmal eines Computers, um den Standort im Internet zu definieren. Sie zeigt auf welcher Provider dabei verwendet wird. Die 32-Bit IP-Adresse (auch IPv4 genannt) besteht aus vier Zahlenblöcken von 0 bis 255.

2. Wie ist eine IPv4- und eine IPv6-Adresse aufgebaut? Wieviele Adressen gibt es theoretisch in jeder Version? Wer ist die Standardisierungsorganisation? In welchen Dokumenten ist IPv4 und IPv6 standardisiert?

IPv4: 192.168.2.1 -> 32 bit -> 2^{32}
 IPv6: 1234:5678:90BC:DEFG:0000:0000:0000:2345 -> 64 bit (hexadezimal) -> 2^{64}

Eine IP-Adresse besteht aus zwei Teilen. Dem vorderen Teil, der Netzwerkadresse, und dem hinteren Teil, der Hostadresse. Die Netzwerkadresse ist vorallem für das IP-Routing wichtig wogegen die Hostadresse für den Router, in dessen Netz sich der Host befindet, von Bedeutung ist.

Internet Engineering Task Force (IETF) ist die "Standardisierungsorganisation" und hat unter anderem TCP/IP, BGP, DNS, http, VoIP und TLS entworfen.

3. Wie ist ein IPv4- und ein IPv6-Paket grob aufgebaut? („Grob“ heißt, sie brauchen nicht wissen, was die Bedeutung eines jeden einzelnen Flags ist. Allerdings sollten Sie den Aufbau des Kopfbereiches zeigen.) Was sind die Veränderungen zw. den Versionen?

Der IPv4-Kopfdatenbereich umfasst 20 Byte plus bis zu 40 Byte optionale Felder, die Länge des Kopfes darf 60 Byte nicht überschreiten. Der IPv6-Header ist 40 Byte lang. Optionen werden hier in eigenen Erweiterungsheadern dargestellt.

4. Auf welcher Schicht des OSI-Referenzmodells befindet sich das IP-Protokoll und was ist die Hauptaufgabe dieser Schicht? Von welchem Netzgerät wird diese Aufgabe durchgeführt?

- Schicht 3 – Der Network Layer oder die Vermittlungsschicht
- Hauptaufgabe: Vermittlung der Pakete zum nächsten Netzknoten
- Hardware auf dieser Schicht: Router

5. Auf welcher Schicht im OSI-Referenzmodell befindet sich das TCP-Protokoll? Was sind die Hauptaufgaben dieser Schicht?

- Schicht 4 Transport
- Erweiterung der Basisfunktionen der Vermittlungsschicht

- Erste Schicht die ausschließlich Ende-zu-Ende arbeitet, d.h. es gib in der Regel keine Protokollinstanzen im Netz
 - Zu den Aufgaben der Transportschicht zählen die Segmentierung des Datenstroms, die Stauvermeidung und die Zuteilung von Daten
6. Was sind die Eigenschaften von TCP? (Sie brauchen nicht erklären können, wie jede Eigenschaft umgesetzt wird. Allerdings sollten Sie ein Verständnis davon haben, was die Bedeutung jeder Eigenschaft ist.)

TCP ist ein zuverlässiges, verbindungsorientiertes Protokoll zur fehlerfreien Ende-zu- Ende-Übertragung eines Datenstroms.

- Ende-zu-Ende-Transportprotokoll im Internet
- Zuverlässig, verbindungsorientiert, paketvermittelt
- Bidirektional, d.h. Übertragung in beide Richtungen
- Flusskontrolle vermeidet Überlastung des Empfängers
- Staukontrolle drosselt die Übertragung bei (angeblicher) Überlastung des Netzes
- Fehlerkontrolle ermöglicht Wiederübertragung bei fehlerhaften oder verlorenen Segmenten
- Sender: Unterteilt den eingehenden Datenstrom auf mehrere Segmente und übergibt sie der Internetschicht
- Empfänger: Setzt die eingehenden Segmente in der ursprünglichen Reihenfolge zu einem Ausgabestrom zusammen und übergibt ihn der Anwendungsschicht

7. Die Alternative zur Verwendung von TCP ist UDP. Vergleichen Sie die Eigenschaften beider Protokolle. Wie ist ein UDP-Paket aufgebaut?

UDP ist ein unzuverlässiges, verbindungsloses Protokoll zur schnellen, aber unzuverlässigen Ende-zu-Ende-Kommunikation. Das bedeutet, der Absender weiß nicht, ob seine verschickten Datenpakete angekommen sind.

Während TCP Bestätigungen beim Datenempfang sendet, verzichtet UDP darauf. Das hat den Vorteil, dass der Paket-Header viel kleiner ist und die Übertragungstrecke keine Bestätigungen übertragen muss.

UDP hat die selbe Aufgabe wie TCP, nur das nahezu alle Kontrollfunktionen fehlen, dadurch schlanker und einfacher zu verarbeiten ist. So besitzt UDP keinerlei Methoden die sicherstellen, dass ein Datenpaket beim Empfänger ankommt. Ebenso entfällt die Nummerierung der Datenpakete. UDP ist nicht in der Lage die Datenpakete in der richtigen Reihenfolge zusammenzusetzen. Statt dessen werden die UDP-Pakete direkt an die Anwendung weitergeleitet. Für eine sichere Datenübertragung ist deshalb die Anwendung zuständig. In der Regel wird UDP für Anwendungen und Dienste verwendet, die mit Paketverlusten umgehen können oder sich selber um das Verbindungsmanagement kümmern. UDP eignet sich auch für Anwendungen, die nur einzelne, nicht zusammenhängende Datenpakete transportieren müssen.

Die Gemeinsamkeit von UDP und TCP ist die Port-Struktur, die mehreren Anwendungen gleichzeitig mehrere Verbindungen über das Netzwerk ermöglicht.

8. Wozu dienen Ports? In welchem Protokoll wird die Port-Nummer übermittelt?

Lokale Hausnummer innerhalb eines Rechners zur Adressierung einer bestimmten Anwendung. Hinter einem Port befinden sich Anwendungen oder ein Dienst, die diesen Port abhören und die Daten entgegennehmen.

Gültige Portnummern: 0-65535.

- Systemports: 0-1023, reserviert für bestimmte Dienste, Standardisierung durch die IETF.
- Registrierte Ports: 1024-49151, reserviert für registrierte Dienste, Zuweisung ohne IETF (veraltet).
- Dynamische Ports: 49152-65536, Vergabe durch das Betriebssystem.

9. Was ist Network Address Translation (NAT)? Welches Gerät ist dafür zuständig? Auf welche Netzwerkschichten muss dafür zugegriffen werden?

NAT wandelt die private IP-Adresse in die öffentliche IP-Adresse damit über das Heimnetzwerk hinaus unter anderem Daten ausgetauscht werden können, E-Mails verschickt/empfangen werden können und das WWW erreicht werden kann. NAT ist im Router implementiert. Schicht 3, da es den IP-Header verändert sowie IP Checksummen und Schicht 4 TCP/UDP Ports und Checksummen.

10. Was sind die standardmäßigen Portnummern und Transportprotokolle folgender Anwendungsschicht-Protokolle: HTTP, HTTPS, SMTP, DNS, Telnet, SSH, IMAP?

HTTP: 80 **Hypertext Transfer Protocol**

HTTPS: 443 **Hypertext Transfer Protocol over SSL/TLS**

SMTP: 25 **Simple Mail Transfer Protocol** - wird für die E-Mail-Übermittlung zwischen E-Mail-Servern genutzt und findet sehr breite Unterstützung.

DNS: 53 **Domain Name System** - meist ueber UDP

Telnet: 23 **Telnet** - unverschlüsseltes Textprotokoll, z. B. für Fernwartung (ähnlich SSH, mit telnetd) oder manuelle Kommunikation über Textprotokolle wie HTTP

SSH: 22 **Secure Shell** - wird für verschlüsselte Fernwartung und Dateiübertragung genutzt (scp, sftp) sowie für getunnelte Portweiterleitung

IMAP: 143 **Internet Message Access Protocol** - Mail-Management