Zusammenstellung der wichtigsten Netzwerk-Begriffe

Keine Garantie für Vollständigkeit!

Nach Ansicht des Autors müsste man mit Kenntnis der unterstrichenen Begriffe gut durch das NRW-Abi kommen...

Client-Server-Prinzip	Clients verbinden sich mit dem Server; die Kommunikation zwischen den Clients läuft über den Server und wird vom Server verwaltet.
Client	Software! Programm, das mit einem Server kommuniziert.
Server	Software! Programm, das einen Dienst anbietet für alle Clients, die sich am Server anmelden
Host	Hardware! Maschine, auf dem der Server läuft.
Dämon	Hintergrundprozess; die meisten Server sind Dämons; sie warten im Hintergrund, bis sich ein Client bei ihnen anmeldet und werden dann aktiv
Port	„Türe“, an dem der Server auf Anfragen von Clients wartet. Die Clients müssen wissen, welchen Port sie am Host ansprechen müssen, um mit dem Server zu kommunizieren. Bestimmte Dienste haben feste Ports, z.B. hat der Pop3-Server immer Port 110.
Socket	Software! „Steckdose“: Ende einer Kommunikationsverbindung
Peer-to-Peer-Verbindung	Direkte Verbindung zwischen zwei Computern im Internet, eher ungewöhnlich.
Protokoll	Protokolle sind das Rückgrat der Kommunikation in Computernetzwerken. Sie legen für einen Kommunikationszweck (z.B. Versenden von Mail) eine Abfolge von Request-Response-Schritten, in der Regel zwischen Client und Server, fest. Protokolle stellen sicher, dass Computer auf unterschiedlichen Plattformen miteinander kommunizieren können. Bekannte Protokolle sind: - HTTP: für unverschlüsselte Websites - HTTPS: für verschlüsselte Websites - FTP: für die Übermittlung von Dateien - SMTP: für den Versand von Mails - POP3 und IMAP: für den Empfang von Mails - TCP: Für den zuverlässigen Transport von Datenpaketen durch das Internet.
DNS	Domain-Name-System; das DNS kann IP-Adressen und Hostnames einander zuordnen
Namensauflösung	Beschreibt das Auffinden einer IP-Adresse zu einem Hostname
Nameserver	Server, auf dem die Informationen für die Namensauflösung gespeichert sind. Der Nameserver kann von Rechnern aus dem Internet „um Rat“ gefragt werden.
Root-Nameserver	Letzte Instanz der Namensauflösung: Wenn ein Nameserver nicht Bescheid weiß, dann fragt er bei einem von ca. 15 Root-Nameservern nach.
IP-Adresse	z.B. 192.168.100.100; eindeutige Adresse eines Computers (die Adressen 192.168.x.x sind für lokale Netzwerke reserviert; die meisten anderen Ips sind im ganzen Internet gültig)
Hostname	z.B. sibi-honnef.de; eindeutiger Name eines Hosts
URL	Adresse einer Ressource auf einem Host, inklusive Angabe des Protokolls, z.B. http://sibi-honnef.de/vertretungsplan/index.php
Netzroute	Weg vom eigenen Computer zu einem Zielcomputer im Internet; auf der Netzroute werden mehrere Knoten durchlaufen. Es gibt grundsätzlichmehrere Netzrouten zu einem Zielcomputer.

Schichtenmodell	Erklärt, wie die Kommunikation im Internet realisiert wird. Es gibt 4 Schichten: – Highlevel-Protokolle (z.B. http oder smtp) – TCP – IP – Netzzugangsschicht
TCP	Transmission Control Protocol; garantiert eine „sichere“ Kommunikation. Sicher heißt hierbei: – fehlerfrei – verlustfrei Wenn Fehler/Verluste auftreten, dann werden Pakete nochmals angefordert. Wenn das nicht gelingen sollte, werden beide Seiten informiert.
UDP	User Datagram Protocol: ungesicherte Kommunikation. Beim Senden der Daten wird keine Rücksicht darauf genommen, ob die Daten vollständig und fehlerfrei beim Empfänger ankommen. Schneller als TCP; wird vor allem für Streaming (z.B. bei Videos) genutzt.
IP-Datagramm	Grundelement der Internet-Datenkommunikation. Besteht immer aus einem Header und dem eigentlichen Datenteil. Fast alle Daten, die über das Internet verschickt werden, werden in IP-Datagramme zerlegt und auf den Weg geschickt.
Header	Enthält Informationen über die Daten, über Zielport und Ursprungsport etc.
Ursprungsport	„Türe“, aus dem das IP-Datagramm den absendenden Computer verlassen hat.
Zielport	„Türe“, durch den das IP-Datagramm in den Zielcomputer hineingehen soll.
Sequenznummer	Große Datenmengen werden in viele IP-Datagramme zerlegt; mit der Sequenznummer wird die richtige Reihenfolge der IP-Datagramme festgelegt. Das ist wichtig, weil IP-Datagramme auf dem Weg durch das Internet unterschiedlich schnell sein können, d.h. ein früheres IP-Datagramm kann von einem späteren überholt werden. Mit der Sequenznummer kann die ursprüngliche Reihenfolge wiederhergestellt werden.
Bestätigungsnummer	Dient dazu, dass der Empfänger dem Sender den korrekten Empfang von Datenpaketen bestätigt; wird der Empfang nicht bestätigt, werden die Daten nochmal gesendet.
Prüfsumme	Dient dazu, die Unversehrtheit der Daten zu prüfen: Aus den Daten wird eine Prüfsumme berechnet, ungefähr wie eine Quersumme. Diese wird mit den Daten mitgeschickt. Der Empfänger berechnet seinerseits die Prüfsumme aus den Daten und vergleicht mit der mitgeschickten Prüfsumme.
Time-To-Live	Wird beim Durchlauf durch jeden Internet-Knoten eins runtergezählt. Wenn TTL gleich 0 wird, dann wird das Datenpaket gelöscht. Dient dazu, dass Datenpakete, die den Weg zum Empfänger nicht finden, nicht ewig im Internet kreisen.

Intranet	Lokales Netzwerk, z.B. in einer Schule, einer Firma oder auch zuhause
LAN	Local Area Network: lokales Netzwerk, meist kabelgebunden
DHCP	Dynamic Host Configuration Protocol: Mithilfe dieses Protokolls kann man dafür sorgen, dass jeder Rechner in einem lokalen Netzwerk eine eindeutige IP-Adresse (z.B. 192.168.100.100) bekommt. Diese IP-Adresse kann bei jedem Rechnerstart anders sein.
DHCP-Server	Software, die das DHCP-Protokoll verwaltet. Jeder Rechner im lokalen Netzwerk muss sich beim Start am DHCP-Server anmelden und bekommt eine (dynamische) IP-Adresse zugewiesen.
Gateway	Verbindung zwischen Rechnernetzen, die auf unterschiedlichen Protokollen basieren, z.B. eMail → SMS-Gateway oder LAN → WLAN-Gateway
Proxy	„Vermittler“ von Kommunikation: regelt i.A. die Kommunikation von innerhalb eines lokalen Netzwerkes nach draußen. Zweck: Filtern von unliebsamen Inhalten, Zwischenspeichern von häufig abgefragten Inhalten (=die müssen dann nicht jedes Mal aus dem Internet geladen werden)
Proxy-Server	Software, die diesen Vermittlungsdienst anbietet.
Firewall	Sicherungssystem, das ein Rechnernetz (oder einen einzelnen Rechner) vor ungewünschtem/schädlichem Zugriff aus dem Internet schützt.
DMZ	Die De-Militarized Zone hat Firewalls sowohl in Richtung Internet, aber das lokale Netzwerk ist auch mit einer Firewall gegen die DMZ geschützt. Zweck: Hier stehen Services, die viel Kommunikation mit dem Internet haben müssen, von denen deswegen eine Gefahr für das lokale Netzwerk ausgehen könnte. Z.B. Mailserver, Webserver
VPN	Virtual Private Network: Ermöglicht den gesicherten Zugriff auf ein Intranet *durch das Internet.* Dazu wird die Kommunikation verschlüsselt. VPN wird genutzt, damit Mitarbeiter von zuhause aus sicher auf das Firmennetzwerk zugreifen können; mit Hilfe von VPN ist der Rechner zuhause in das Firmennetzwerk einbezogen.
WLAN	Wireless Lan
Switch	Hardware! Verteiler; kann im lokalen Netzwerk mehrere Computer miteinander verbinden.
Bridge	Verbindet Teilnetze
Router	Hardware: Geräte, die Datenpakete zwischen Netzwerken weiterleiten können. Z.B. hat man zuhause einen Router, der die Daten aus dem öffentlichen Netzwerk (= der „Dose“) in das lokale Netzwerk weiterleitet.
Access-Point	Gerät für die Verbindung zwischen drahtgebundenem und drahtlosem Netzwerk.
WLAN-Router	Kombination aus Router und Access-Point
WEP	Veralteteter Verschlüsselungsstandard für WLAN; inzwischen geknackt
WPA2	Aktueller Verschlüsselungsstandard für WLAN