Aufgaben XV Netzwerktechnik

Aufgabe 1: Ping und traceroute/tracert benutzen ICMP. Wie unterscheiden sich die beiden Protokolle dabei und welche ICMP-Typen werden bei IPv6 und bei IPv4 benutzt?
Antwort: Ping fragt nur einmal mit einem hohen hop Limit/TTL das Ziel ab. Traceroute setzt das hope limit bzw. das TTL ab dem Wert 1 nach und nach hoch und pingt somit das Ziel solange an, bis die Anfrage das Ziel erreicht. Da die Router eine ICMP-Nachricht bei Verirrung des Netzes (=0) schicken, kann man den Pfad mit den dabei empfangenen IP's gut nachvollziehen. Es ist kein 100% Pfad, da jedes Paket im Internet einen anderen Weg nehmen kann.
Die ICMP-Typen sind bei IPv6 128 (Echo Request) und 129 (Echo Reply), Typ 3 kommt zurück, wenn das hop limit erreicht ist.
Bei IPv4 lautet die Typnummer 8 (Echo Request) und 0 (Echo Reply), Typ 11 Code0 ist TTL abgelaufen.
Aufgabe 2: Bei WLAN werden CSMA/CA genutzt. Nach welchen Regeln arbeitet es und welche grundlegenen Unterschiede gibt es zu CSMA/CD?
Antwort: 1.) Abhorchen, 2.) Zufällige Zeit warten und abhören, falls belegt →1, 3.) Daten senden, 4.) Empfänger wartet und sendet Ack 5.) Wenn kein Ack korrekt empfangen -> 1, 6.) Nach einer Anzahl Versuchen → Timeout
CSMA/CD kann Kollision erkennen, /CA nicht. /CA hat mehr Wartezeiten, bei /CA ist der Sender auf die Reaktion des Empfängers angewiesen, bei /CD nicht. Verfahren /CD kann nicht den Empfang garantieren, das Lösen höhere Schichten. Beide reagieren auf Kollisionen, können sie aber nicht ausschliessen (dann timeout)
Aufgabe 3: Welche Fehler behandelt das TCP-Windowing und wie behandelt es diese? Wann kann der Sender seinen Arbeitsspeicher für die einzelnen Datensegmente freigeben? Wie sollte das windowsize (Anzahl von Pakete,…) abhängig von der Übertragungsgeschwindigkeit gewählt werden?
Antwort: 1.) Paketverlust, 2.) Paketverdopplung, 3.) Reihenfolgen vertauscht.
Bei 1.) wird das Paket vom Sender nochmals verschickt, weil der Empfänger in vertretbarer Zeit kein Ack gesendet hat. 2.) und 3.) wird durch die Sequencenumber erledigt, anhand dieser Nummer wird das Paket gespeichert.
Das Windowsize sollte bei Störung vermindert und bei einem störungsfreien Betrieb erhöht werden. Hohe Übertragungswerte geben ein hohes Windowsize, es soll ja die Zeit, bis das Ack zurückkommt optimistisch mit Datenübertragung belegt werden. Die Geschwindigkeit wird reduziert, wenn der Sender auf Ack's wartet und dabei nicht sendet. Die notwendigen Speicherbelegung für das Bereithalten der noch nicht bestätigten Pakete ist dagen nicht so hoch.
Aufgabe 4: Wann wurde IP, wann TCP und wann OSI standardisiert? Wann kam IPv6 dazu?
Antwort: IP: RFC 791 – 1981; TCP: RFC793 – 1981; UDP: RFC 768 – 1980; OSI: X.200 – ITU – 1983, 7498 – ISO/DIN – 1984; IPv6: RFC 2460 – 1998, RFC 8200 2017
Aufgabe 5: Es sollen Pakete an fd00:1:2:bad::33 und an 10.5.191.5 mit den Subnetzadressen /56 und /19 verschickt werden. Dazu sind folgender Ausschnitt aus der Routingtabelle gegeben. Welches Gateway wird dabei benutzt und welche Maske dient dabei zur Maskierung?

Netzwerkziel	Gateway	Ziel	Subnetmaske	Gateway
fd00:1:3::/48	fd00:8:7::edda	10.5.8.0	255.255.0.0	178.19.1.5
fd00:1:2:bcd::/56	fd00:8:7::abba	10.5.128.0	255.255.128.0	178.19.1.1
fd00:1:2:bad::/64	fd00:8:7::affe	10.5.224.0	255.255.192.0	178.18.1.1

Antwort: fd00:1:2:bad::33 durch 3. Zeile (1.Abfrage) – sonst auch 2. Zeile zutreffend! 10.5.191.5 durch 2. Zeile.
Aufgabe 6: Was wird bei NAT und was bei PAT vom NAT/PAT-Router ausgetauscht? Welche der beiden Adressen Ziel/Absender weden bei DNAT und bei SNAT ausgetauscht? Wie und mit welchem kann man damit ganze Netzwerke im Internet „verstecken". Was bringt es?

Antwort: Bei NAT wird eine IP-Adressen ausgetauscht, bei PAT sowohl eine IP-Adressen als auch ein Port. Der Austausch erfolgt immer beim 1.Paket, bei den Paketen auf dem Rückweg ist es dann genau die andere Adresse, die zurückgetausch wird. SNAT wird dabei bei ausgehenden Verbindungen benutzt, wobei es durch PAT auch für mehrere Computer im lokalen Netz benutzt werden kann, wo i.d.R. deren privaten Absenderadressen durch die eine öffentliche Adresse ersetzt wird und so alle Computer ins Internet kommen. Bei DNAT wird die öffentliche Zieladresse durch die privat des Servers ersetzt, ein privater Server ist aus dem Internet erreichbar, entweder für alle Ports (DNAT) oder nur für einige Ports, deren Nummern auch verändert werden können (DPAT). Also SNAT → privates Netz mit einer öffentlichen IP vor dem Internet verstecken und DNAT den Zugriff auf einen oder mehreren private (und damit versteckten) Server realisieren.

Aufgabe 7: Bei einem Windowing von 22 werden Pakete verschickt. Das 5. kommt doppelt, das (magische) 13. geht verloren und das 17. wird verstümmelt. Wieviel Pakete sind verschickt, wenn auf die Fehler vom diesen Paketen vom Absender reagiert wird?

Antwort: doppelte Pakete sind problemlos, das 2. Paket überschreibt das 1. oder das 2. Wird fallengelassen (Problematisch ist nur, wenn beim Überschreiben des 1. Paketes festgestellt wird, dass das 2. Fehlerhaft ist. Sollte nicht vorkommen, kann durch Wiederholung der Übertragung gelöst werden) kommt das 13. Nicht an, so wartet der Empfänger so eine Zeit, dass der Sender nicht in Timeout für die ersten 12 Pakete läuft und quitiert die ersten 12 Pakte. Dann läuft der Absender mit dem 13. Ins Timeout, hat aber vielleicht schon bis Paket 34 gesendet und wieder holt jetzt Paket 13, weil er keine Quittung dafür hat. Verstümmelte Paket werden entfernt, es ist also ein Paket das verloren ist. Der Sender kann bis Paket 39 schon senden (Windowsize, Puffergröße). Der Absender sollte die ersten 16 Pakete (also 4 weitere Pakete) in einem Rutsch rechtzeitig quittieren (ACK) sonst kommen diese nochmal.

Aufgabe 8: Es sind im Internet bei IPv4 3,5 Milliarden Adressen verfügbar. Wie groß ist bei 32 bit die mögliche Anzahl und warum ist sie so viel größer?

Class D (Multicast) und Class f (for future use – also wohl kein use mehr) belegen jeweils mit einem Adressumfang von 28 bit jeweils ca. 250 Millionen Adressen. Bei 32 Bit Adressen abzüglich den 0,5 Milliarden sind also nur 3,5 Milliarden möglich (Korrekt: 4 Gibiadr. (4.294.967.296) – 500 Mebiadr. (536.870.912) ergibt 3.758.096.384. Da Netzwerksegmentadressen und Broadcastadressen nicht nutzbar sind, sind die Zahlen noch kleiner. Umso höher der Anteil von kleinen Subnetzen ist, um so mehr IPv4-Adressen für Computer werden vergeudet!