NVS Aufgabenblock 5

Abgabe von David Pape, 01634454. Ausarbeitung hat ca. 2 Stunden in Anspruch genommen.

Aufgabe 19

Wenn das Ziel "unreachable" ist, dann konnte keine Route zu dem Ziel gefunden werden. Dies kann entweder in einem lokalen oder in einem entfernten Router passieren. Die Antwort "Destination Host Unreachable" besagt, dass die Antwort aus dem lokalen Netzwerk kommt; wenn ein entfernter Router keine Route finden kann, dann lautet die Antwort "Reply from $IP: Destination Host Unreachable."

Aufgabe 20

Ein Timeout geschieht, wenn das Ziel nicht unerreichbar ist, aber trotzdem keine Antwort (keine ICMP Typ *Echo Reply* Nachrichten) empfangen wurde. Das Standard-Timeout ist dabei eine Sekunde.

Ein solches Timeout kann z.B. passieren, wenn das Ziel keine Route hat, die wieder zur Quelle geht. Alternativ kann das Netzwerk zu stark belastet oder das Paket irgendwo gefiltert werden.

Wie in der letzten PS-Aufgabe gesehen, gehen viele Hosts nicht auf Ping-Nachrichten ein. Im Falle einer zu hohen Netzwerkauslastung kann es Abhilfe schaffen, das Timeout hinaufzustellen, z.B. auf 5 Sekunden.

Quelle zu Aufgaben 19 und 20: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-2000-server/cc940095(v=technet.10)?redirectedfrom=MSDN

Aufgabe 21

Den vorangegangenen Beobachtungen entsprechend gibt `ping` unterschiedliche Fehlermeldungen, wenn das Ziel wirklich nicht erreichbar ist und wenn das Ziel nur keine Antwort gibt.

Wenn man keinen Fehler "Destination Host Unreachable" bekommt, sondern einen Timeout, dann stehen die Chancen gut, dass das Ziel erreichbar ist und nur nicht auf `ping`-Anfragen antwortet.

Mit anderen Protokollen kann man auch Erfolg haben; wenn das Ziel z.B. einen Webserver hostet, dann kann man sinnvollerweise Antworten auf HTTP-Requests erwarten.

Aufgabe 22

Der ICMP-Header sieht wie folgt aus:

Byte	Funktion
0	Typ
1	Code
2-3	Checksum
4-12	je nach Typ

Einige ICMP-Nachrichten:

Nachricht	Typ	Code	Bemerkung
Echo Reply	0	0	Antwort auf `ping`
Echo Request	8	0	`ping`-Anfrage
	3	0	Dest. network unrachable
	3	1	Dest. host unrachable
Destination Unreachable	3	2	Dest. protocol unrachable
	3	3	Dest. port unrachable
	3	15	Precedence cutoff in effect
Redirect	5	0	Network redirect (if a direct route is available)
	5	1	Host redirect
Time exceeded	11	0	TTL expired
	11	1	Fragment reassembly time exceeded

Quelle: https://en.wikipedia.org/wiki/Internet_Control_Message_Protocol

Aufgabe 23

`traceroute` "missbraucht" den time-to-live counter von Paketen. TTL existiert eigentlich, um Endlosschleifen im Routing von Paketen zu vermeiden; bei jedem Router wird der TTL-Counter um 1 reduziert und wenn TTL=0, dann sendet der Router, bei dem das Paket gerade ist, eine Benachrichtigung an den Host, um ihn zu informieren, dass das Paket einen timeout erlitten hat.

Setzt man TTL=1, dann wird einem der erste Router auf der Strecke antworten; ebenso mit TTL=1 und TTL=2 usw., bis man am Ziel angelangt ist. Man muss anmerken, dass die Route nicht unbedingt konstant zwischen allen Paketen bleibt. Weiters liefern einige Betreiber gar keine TTL-Benachrichtigungen und/oder filtern `traceroute`-Anfragen per Firewall, vielleicht damit ihre interne Netzwerkinfrastruktur unbekannt bleibt. Bei solchen Hops zeigt `traceroute` dann nur `* * *`.

Aus jenem Grund kann `traceroute` mit TCP, UDP und ICMP verwendet werden. Der Unix-Default UDP erfordert keine besonderen Rechte, anders als ICMP, allerdings kann es gut sein, dass die UDP-Ports, die `traceroute` verwendet, gefiltert werden; daher bleibt die Option ICMP (und auch TCP). Sporadische

Praxistests ergaben auch weniger `* * *` bei Verwendung von `-I` und `-T`, wobei nur bei `-T` `sudo`-Rechte gebraucht wurden.

Quelle: https://stackoverflow.com/questions/10312344/why-traceroute-sends-udp-packets-and-not-icmp-ones