Hochauflösende Netzwerküberwachung mit Pings

Mit Pings Aufspüren von Switchen und transparenten Bridges, Messen von Kabellängen und Entfernungen, Detektieren von Unterbrechungen und beschädigten Datenpaketen

Dr. Rolf Freitag, 2014-03

Ping-Elend

Schon beim klassischen ICMP-Ping sind Ausreißer ein großes Problem:

...
64 bytes from 192.168.1.1: icmp_req=66 ttl=64 time=0.209 ms
64 bytes from 192.168.1.1: icmp_req=64 ttl=64 time=0.158 ms
64 bytes from 192.168.1.1: icmp_req=65 ttl=64 time=508 ms
64 bytes from 192.168.1.1: icmp_req=66 ttl=64 time=0.204 ms
64 bytes from 192.168.1.1: icmp_req=67 ttl=64 time=0.166 ms
--- 192.168.1.1 ping statistics ---
100 packets transmitted, 100 received, 0% packet loss, time 98998ms
rtt min/avg/max/mdev = 0.097/5.297/508.262/50.549 ms

D. h. 1 % Ausreißer verschieben den Mittelwert, hier bei 0,2 ms, um weit mehr als 1000 % und zudem stark verrauscht.
Der statistische Ansatz, mit Mittelwert und Standard- Abweichung, passt weil die allermeisten Netze, auch Ethernet, stochastische Zugangsverfahren verwenden, aber es zeigt sich meist eine Summe mehrer Verteilungsfunktionen, von denen meist nur eine benötigt wird.

Programm Pinger

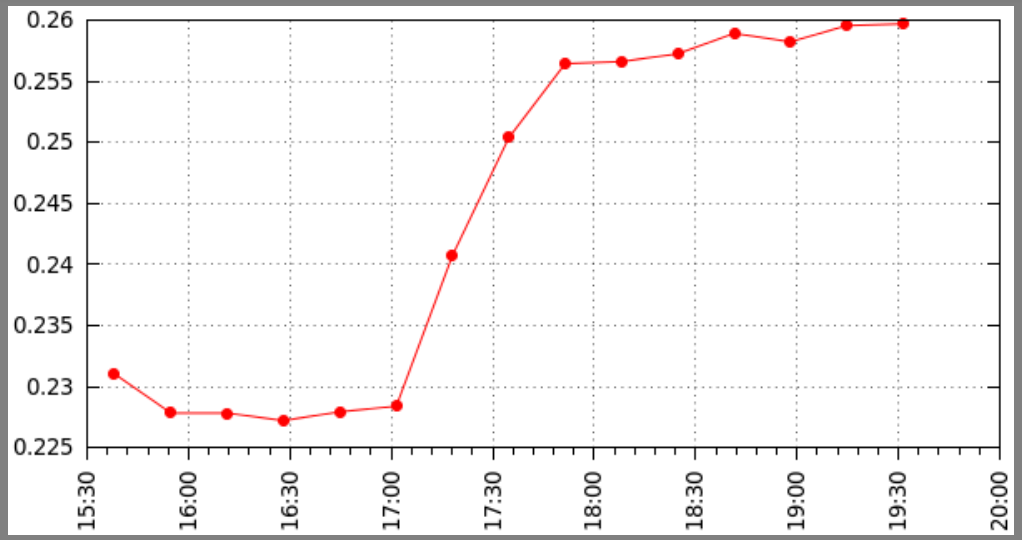
- Ausfiltern von Ausreißern mit einem Ausreißer-Test, im einfachsten Fall cutoff (Abschneiden) mit einem festen Wert
- Exponentiell gleitende Mittelung über n=10, 1000, 86400 RTTs und Rückgabewerte (0, 1, 2)
- Ausgabe der Mittelwerte in je eine Datei und auch eine Statistik über minimale/maximale RTT, Prozentsatz Ausreißer etc.
- Grobstruktur: Ein koordinierender und auswertender Main-Thread und 10 Ping-Threads, die einmal pro Sekunde Pingen, mit einer 128 Bit Zufallszahl und dem don't fragment-Flag
- Passend zu den Dateien mit den Mittelwerten gibt es ein Skript zur ersten Auswertung in Form eines Plots

RTT-Resultate

Netzwerkbestandteile mit einer RTT-Erhöhungen von 0,2, 5, 500, und circa 20.000 ns

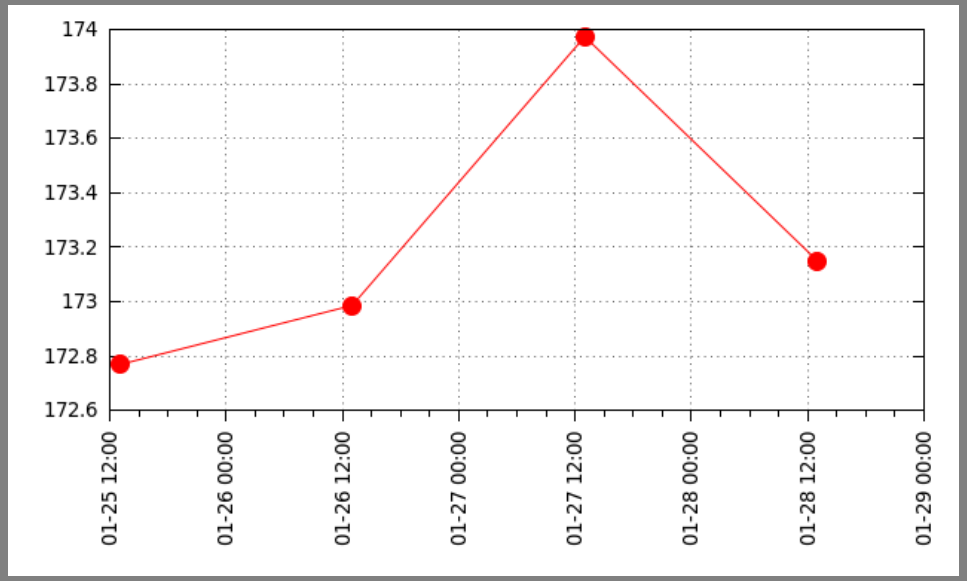
Wird einer der kleinen GB-Switche für einige Stunden entfernt, zeigt sich das bei den 1000 s Mittelwerten von 44 Byte kleinen Pings an einer Stufe mit -30 µs

RTT-Resultate

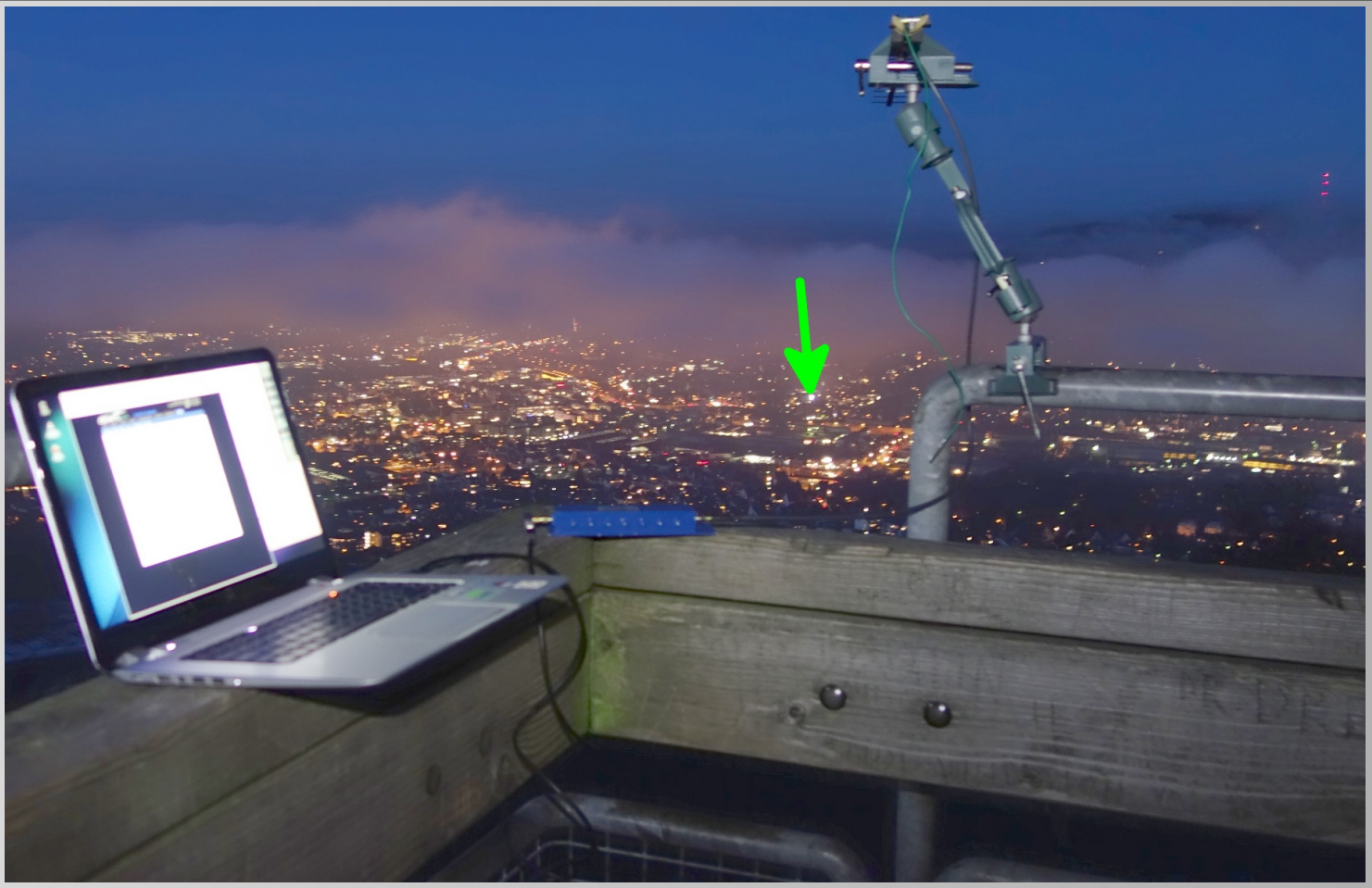


Beim großen Switch zeigt sich ein Warmlaufen und erst mit 1500 Byte großen Pings eine deutliche RTT-Erhöhung

Der Austausch eines 0,5 m Kabel durch ein 50 m Kabel erhöht die RTT um 0,5 µs, aber bei den einfachen Tagesmitteln ist das Rauschen gleich groß. Die 2-Tage-Mittelwerte zeigen einen Unterschied von 685 ns



RTT-Resultate



WLAN-Messung mit 2,5 km statt 0,7 m Distanz, zwei 1000 s RTT-Mittelwerte: Theoretisch zusätzliche 16,7 µs, Messwert 36,8 µs

Schluss

- Noch höhere Genauigkeit ist möglich mit a) häufiger Pingen, b) Pingen mit Echtzeit, c) Echtzeit auch hinter/vor der Netzwerk-Buchse durch Echtzeit-Netzwerke wie Echtzeit-Ethernet, d) Differenzmessung
- Einige WLAN-Standards bestimmen die Entfernung über Zeitstempel, nicht RTTs
- Pinger wurde unter Linux mit ICMP-Ping entwickelt, läuft aber auch unter MS-Windows (mit Cygwin) und mit anderen Pings, z. B. Arping
- Spionage-Boxen die die RTT erhöhen, z. B. IMSI-Catcher, sind leicht aufspürbar
- Durch Messung der Abhängigkeit der RTT von der Paketlänge kann man auch unterscheiden zwischen der Latenz durch Kabel/Distanzen und der durch Geräte wie Switche

URL:

https://sslsites.de/www.true-random.com/homepage/projects/pinger/

Übliche Ping-Messung mit MRTG: RTT in blau, Packet Loss [%] in grün