Next Level Ping Nerdery

Netzwerk-Monitoring mit Meshping

Das Internet Control Message Protocol, kurz ICMP, ist eines der grundlegendsten Protokolle unserer modernen Netzwerke. Wie der Name schon andeutet dient es zum Versenden von Steuerungs-Nachrichten (Control), und agiert daher meist unbemerkt im Hintergrund: Es wird nicht vom menschlichen Anwender genutzt, sondern ermöglicht den IP-Stacks der jeweiligen Netzwerkteilnehmer den Austausch von Informationen über das Netzwerk.

Ping

Die wohl bekannteste Anwendung dieses Protokolls dürfte zweifelsohne der Ping sein. Das `ping`-Kommando ermöglicht das Senden einer Nachricht an einen anderen Teilnehmer, welcher den Ping beantwortet. Dies ermöglicht uns zu prüfen ob überhaupt eine Verbindung besteht, sowie eine Abschätzung über die Paketlaufzeit indem wir die Antwortzeit messen. Ping-Nachrichten können allerdings noch deutlich mehr, wenn wir sie mit anderen Funktionen kombinieren.

Traceroute

Ebenfalls weit bekannt ist das `traceroute`-Kommando (von manchen Betriebssystemen auch `tracert` genannt). Dieses Kommando legt offen, welche Router ein Paket auf seinem Weg von der Quelle zum Ziel passiert. Technisch wird dies umgesetzt, indem die `Time to live` der Ping-Pakete geschickt verwendet wird: Jedes Paket enthält einen Zähler, wieviele Router es noch passieren darf, bevor es verworfen wird. Indem wir diesen Zähler zunächst auf 1 setzen, wird das Paket vom ersten Router verworfen, der dann eine ICMP-Nachricht zurücksendet um den Fehler zu melden. Indem wir den Prozess mit höherer TTL wiederholen, können wir nacheinander alle Router identifieren. Bekommen wir statt einem Fehler eine Antwort, so ist das Ziel erreicht und der Prozess abgeschlossen.

Erkennung der Pfad-MTU (Path MTU Discovery)

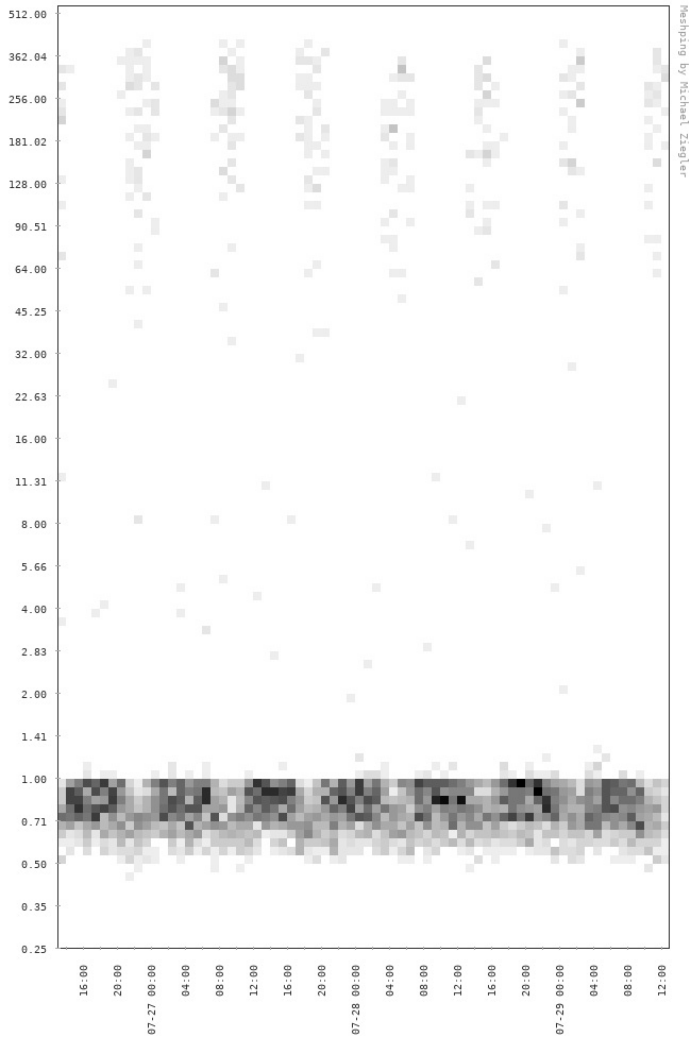
Zu guter Letzt bietet ICMP auch eine Möglichkeit, die maximale Paketgröße zu ermitteln, welche zwischen Quelle und Ziel ausgetauscht werden kann. Diese Größe kann beispielsweise bei DSL-Anschlüssen oder VPN-Verbindungen reduziert sein, wodurch unter anderem Remote-Desktop-Verbindungen in Mitleidenschaft gezogen werden: Werden RDP-Pakete größer als ein Router auf der Strecke damit umgehen kann, so kann es vorkommen dass ein Router auf der Strecke das Paket verwirft. RDP quittiert dies durch einen Verbindungsabbruch und anschließendes Neu-Verbinden, was für den Benutzer sehr störend ist. Wie kann nun geprüft werden, ob die MTU der Auslöser für dauernde Verbindungsabbrüche sein könnte?

Dazu kann man erneut ein Ping senden und diesen Fehler bewusst provozieren. Das `ping`-Paket darf in ICMP beliebig groß werden, begrenzt nur durch die MTU. Außerdem gibt es ein Flag im IP-Header, über welches man einem Router signalisiert, dass Pakete nicht fragmentiert werden dürfen. Kann ein Router ein solches Paket aufgrund einer kleineren MTU auf der folgenden Strecke nicht weiterleiten, so muss er das Paket verwerfen und dem Absender mit einer ICMP-Nachricht die neue MTU mitteilen. Sendet man nun also ein ausreichend großes Ping-Paket bei dem man das `don't fragment`-Flag gesetzt hat, so bekommt man entweder eine Antwort vom Ziel (wenn es keine MTU-Probleme gibt), oder eine ICMP-Nachricht mit der passenden MTU. Wiederholt man diesen Prozess so lange bis man eine Antwort bekommt, so hat man die MTU des gesamten Pfades ermittelt.

Fazit

In Unternehmensnetzwerken ist es üblich, dass mehrere Netzbereiche über Standorte hinweg miteinander kommunizieren. Diese Tools zu kennen ermöglicht einem Administrator die gezielte Fehlersuche bei Problemen: Ist mein Ziel überhaupt erreichbar? Falls nicht, welchen Weg nehmen meine Pakete, und wie weit kommen sie? Gibt es ein Problem wenn sie zu groß werden? Wie groß dürfen sie maximal sein?

Ich entwickle ein Tool namens Meshping, welches diese Informationen für konfigurierbare Ziele kontinuierlich sammelt und in einer Web-Oberfläche darstellt. Die Latenzen werden als Heatmap dargestellt, wodurch auch kleine Ausreißer sehr deutlich erkennbar werden:



Die Ausreißer wurden durch eine unserer Firewalls verursacht, welche einen Teil der Pakete verzögert hat. Der durchschnittliche Ping betrug zwar nur 7ms, die einzelnen verzögerten Pakete hatten jedoch eine Latenz von über 300ms und die Nutzer hatten häufig Verbindungsabbrüche.

Im Vortrag zeige ich wie man die Informationen mit dem `ping`-Kommando manuell sammeln kann und gebe eine kurze Vorstellung von Meshping.