Netzwerk-Protokolle
Hinter die Kulissen geblickt: Traceroute/Ping

Marvin Ekmekci

Gliederung

- Ping
  - Wofür?
  - Geschichte
  - Wie?
  - Beispiel
- Traceroute
  - Wofür?
  - Geschichte
  - Wie?
  - Beispiel

Ping – Wofür?

- Test auf Erreichbarkeit eines Hosts
- Messung der round-trip time (RTT)
- Aufzeichnung der verlorenen Packete
- Missbrauch möglich!
  - Denial of service (dos) attack per z.B. ping flood
  - Ping of death: zu großes Packet wird verschickt und sorgt evtl. für overflows und crashes

Ping – Geschichte

- Entwickelt von Mike Muuss im Dezember 1983
- Benannt nach dem Sonar Geräusch
  - IP/ICMP echo request und reply um Distanz zu schätzen
  - oft auch Packet InterNet Grouper

Ping – Wie?

- Ping verschickt ein ICMP echo request Paket und wartet auf ein entsprechendes echo reply
- RFC1122 definiert, dass jeder Host Funktion für Annahme und Versendung von ICMP Paketen bereitstellen muss

Ping - ICMP Paket

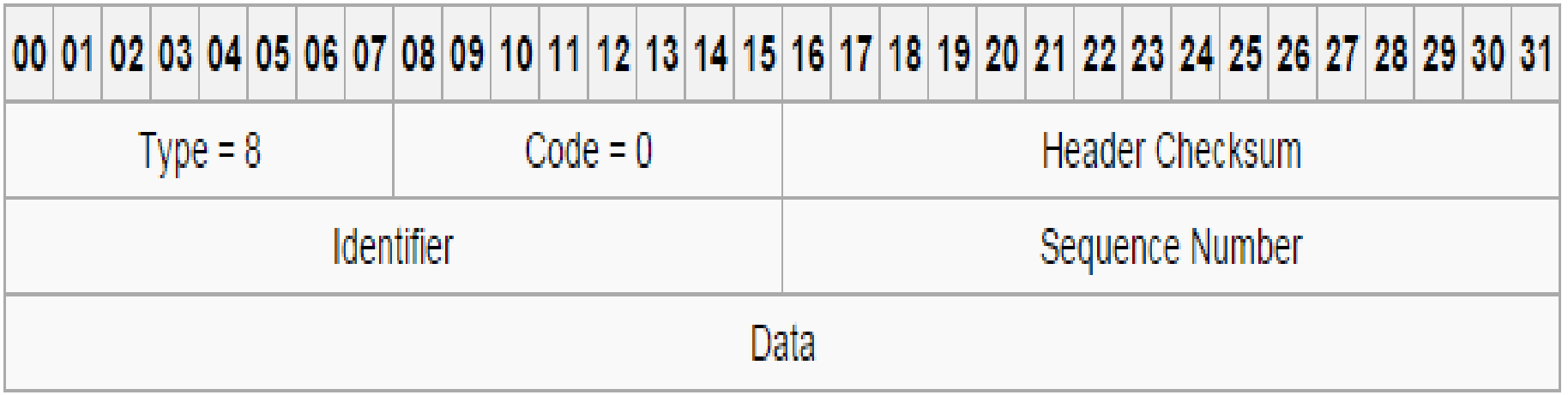
IP Datagram

	Bits 0–7	Bits 8–15	Bits 16–23	Bits 24–31
IP Header (20 bytes)	Version/IHL	Type of service	Length	
	Identification		*flags* and *offset*	
	Time To Live (TTL)	Protocol	Checksum	
	Source IP address			
	Destination IP address			
ICMP Header (8 bytes)	Type of message	Code	Checksum	
	Header Data			
ICMP Payload (*optional*)	Payload Data			

- Protocol 1 für ICMP und Type of Service 0

Ping – ICMP Header

- Echo request (ping):



- Identifier und sequence number dienen dazu requests und replies zusammenzuführen
- Empfangene Daten müssen unverändert zurückgeschickt werden

Ping – ICMP Header

- Echo reply (pong):

00 01 02 03 04 05 06 07	08 09 10 11 12 13 14 15	16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
Type = 0	Code = 0	Header Checksum
Identifier		Sequence Number
Data		

- Type und Code werden auf 0 gesetzt

Ping – Mögliche Antworten

- Bei Fehler wird ICMP Error Message verschickt
  - Fehler beinhaltet ersten 8 Bytes der Original Nachricht, was Zuordnung zum Request ermöglicht

- H, !N, or !P – host, network or protocol unreachable
- S – source route failed
- F – fragmentation needed
- U or !W – destination network/host unknown
- I – source host is isolated
- A – communication with destination network administratively prohibited
- Z – communication with destination host administratively prohibited
- Q – for this ToS the destination network is unreachable
- T – for this ToS the destination host is unreachable
- X – communication administratively prohibited
- V – host precedence violation
- C – precedence cutoff in effect

Ping – Payload Data

- Enthält ASCII characters

```
16:24:47.966461 IP (tos 0x0, ttl 128, id 15103, offset 0, flags [none],
proto: ICMP (1), length: 60) 192.168.146.22 > 192.168.144.5: ICMP echo request,
id 1, seq 38, length 40
        0x0000:  4500 003c 3aff 0000 8001 5c55 c0a8 9216  E..<:.....\U....
        0x0010:  c0a8 9005 0800 4d35 0001 0026 6162 6364  ......M5...&abcd
        0x0020:  6566 6768 696a 6b6c 6d6e 6f70 7172 7374  efghijklmnopqrst
        0x0030:  7576 7761 6263 6465 6667 6869            uvwabcdefghi
```

- Enthält einen Zeitstempel, der zur Berechnung der Pingzeit verwendet wird

Ping - Beispiel

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Alle Rechte vorbehalten.

C:\Users\Marvin>ping www.google.com

Ping wird ausgeführt für www.google.com [2a00:1450:4008:801::1012] mit 32 Bytes
Daten:
Antwort von 2a00:1450:4008:801::1012: Zeit=24ms
Antwort von 2a00:1450:4008:801::1012: Zeit=25ms
Antwort von 2a00:1450:4008:801::1012: Zeit=24ms
Antwort von 2a00:1450:4008:801::1012: Zeit=24ms

Ping-Statistik für 2a00:1450:4008:801::1012:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0
    (0% Verlust),
Ca. Zeitangaben in Millisek.:
    Minimum = 24ms, Maximum = 25ms, Mittelwert = 24ms

C:\Users\Marvin>_
```

Traceroute – Wofür?

- Anzeigen des Pfades eines Pakets
- Messung der Übertragungszeiten
- Zeigt Netzwerk Probleme

Traceroute – Geschichte

- Van Jacobson
- Erste Version funktionierte nicht wirklich
  - Schickte ICMP Pakete, doch RFC 791 verbot es ICMP Errors als Antwort auf ein ICMP Paket zu schicken
- Daraufhin nutzte neue Version UDP Pakete
- Aussage von RFC 791 wurde später aber abgeschwächt

Traceroute – Wie?

- Unix basierende Systeme:
  - UDP Pakete
- Windows:
  - ICMP Pakete
- Einige spezielle Programme:
  - TCP SYN Pakete
- Paket wird mit Time to live 1 losgeschickt
- Router dekrementiert TTL um 1
- Bei TTL 0 wird ICMP Time Exceeded Error zurückgeschickt
- Paket wird mit TTL 2 losgeschickt
- Usw…
- Ziel Router schickt ICMP Echo Reply

Traceroute - Beispiel

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Alle Rechte vorbehalten.

C:\Users\Marvin>tracert google.com

Routenverfolgung zu google.com [2a00:1450:4008:800::1004] über maximal 30 Abschn
itte:

  1    <1 ms    <1 ms    <1 ms  p2003007A8E21D3E1D62122FFFE5270C0.dip0.t-ipconne
ct.de [2003:7a:8e21:d3e1:d621:22ff:fe52:70c0]
  2     *        *        *     Zeitüberschreitung der Anforderung.
  3    20 ms    20 ms    20 ms  2003:0:1501:8318::2
  4    24 ms    25 ms    25 ms  2003:0:1001:4000::1
  5    76 ms    80 ms     *     2001:4860:1:1:0:cf8:0:9
  6    25 ms    24 ms    24 ms  2001:4860::1:0:6e0f
  7    29 ms    24 ms    24 ms  2001:4860:0:1::4b
  8    24 ms    24 ms    25 ms  ber01s08-in-x04.1e100.net [2a00:1450:4008:800::1
004]

Ablaufverfolgung beendet.
```

- i.d.R. 3 Pakete pro Host
  - Sternchen zeigen packet-loss an