Internet Control Message Protocol (ICMP)

Netzwerkgrundlagen (NWG2)

Markus Zeilinger[1]

[1]FH Oberösterreich
Department Sichere Informationssysteme

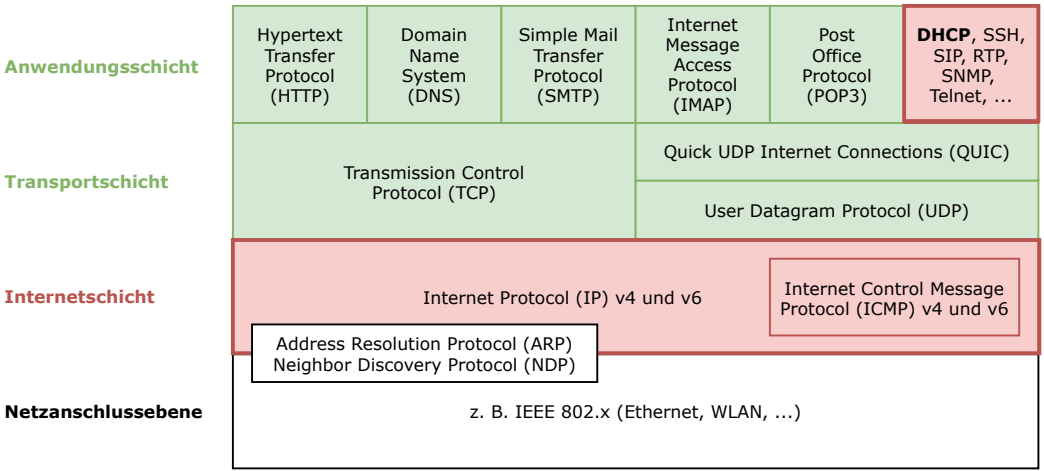
Sommersemester 2023

FH OBERÖSTERREICH
UNIVERSITY OF APPLIED SCIENCES UPPER AUSTRIA

Wichtiger Hinweis

Alle Materialien, die im Rahmen dieser LVA durch den LVA-Leiter zur Verfügung gestellt werden, wie zum Beispiel Foliensätze, Audio-Aufnahmen, Übungszettel, Musterlösungen, ... dürfen ohne explizite Genehmigung durch den LVA-Leiter NICHT weitergegeben werden!

Internetschicht in der TCP/IP Protokollfamilie



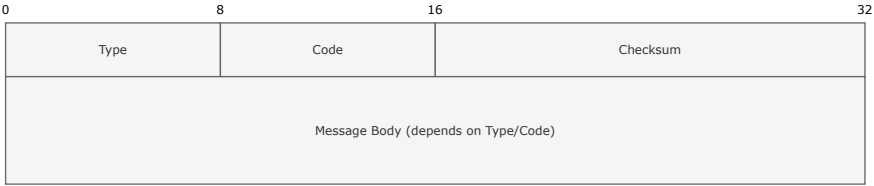
Internet Control Message Protocol

Basics

- Internet Control Message Protocol v4 (ICMPv4, RFC 792)
- Internet Control Message Protocol v6 (ICMPv6, RFC 4443)
- Erweiterbares Protokoll-Framework für Test-, Diagnose- und Fehlermeldefunktionen in/für IP.
- Sender von ICMP Nachrichten: Endsysteme, Router
- ICMP kennt Error und Informational/Query Nachrichten (Verwaltung durch die IANA [v4, v6]):
  - Message Type = Klasse/Typ einer ICMP Nachricht + Message Code = spezifiziert den Type der Nachricht genauer.
- ICMPv4 Nachrichten werden in IPv4 Paketen, ICMPv6 Nachrichten in IPv6 Paketen übertragen.

Internet Control Message Protocol

Header



- Type
  - Typ der ICMP Nachricht (maximal $2^8 = 256$ verschiedene Typen möglich).
- Code
  - Subtyp der ICMP Nachricht (spezifiziert den Type genauer) (maximal $2^8 = 256$ verschiedene Subtypen möglich)
- Der Inhalt des Message Bodies hängt von Type und Code der Nachricht ab.
  - Error Nachrichten enthalten den kompletten IPv4 Header und mind. die ersten 8 Byte der IP Payload des ursprünglich auslösenden IP Pakets.

Type	Beschreibung	Code	Beschreibung
0	Echo Reply	0	Echo Reply (Antwort auf Echo [Request])
3	Destination Unreachable	0	Destination network unreachable
		1	Destination host unreachable
		2	Destination protocol unreachable
		3	Destination port unreachable
		4	Fragmentation needed and DF set
5	Redirect	0	Redirect datagrams for the network
		1	Redirect datagrams for the host
8	Echo (Request)	0	Echo (Request) (Antwort durch Echo Reply)
11	Time Exceeded	0	TTL expired in transit
		1	Fragment reassembly time exceeded

Internet Control Message Protocol

ICMPv6 - Wichtige Types und Codes (unvollständig)

Type	Beschreibung	Code	Beschreibung
1	Destination Unreachable	0	No route to destination
		3	Address unreachable
		4	Port unreachable
2	Packet Too Big	0	Packet Too Big (Fragmentierung)
3	Time Exceeded	0	Hop limit exceeded in transit
		1	Fragment reassembly time exceeded
128	Echo Request	0	Echo Request (Antwort durch Echo Reply)
129	Echo Reply	0	Echo Reply (Antwort auf Echo Request)
133	Router Solicitation	0	Router Solicitation (SLAAC)
134	Router Advertisement	0	Router Advertisment (SLAAC)
135	Neighbor Solicitation	0	Neighbor Solicitation (NDP)
136	Neighbor Advertisements	0	Neighbor Advertisements (NDP)

Internet Control Message Protocol

ping I (Wiederholung)

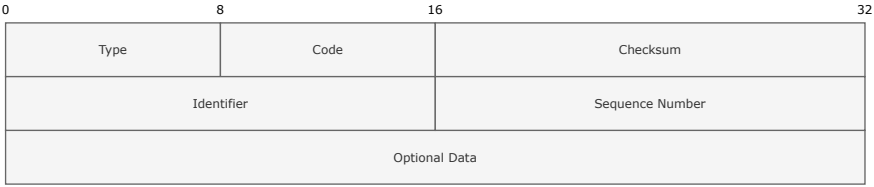
- ping ist ein Tool zum Feststellen, ob ein System "up" ist (d. h. läuft, verfügbar ist; eigentlich ob unter einer IP-Adresse ein System "up" ist).
- Verwendung von ICMPv4/v6 Echo Request und Echo Reply Nachrichten.

```
[redacted]:~$ ping -c 4 www.fh-ooe.at
PING web11.fh-ooe.at (78.46.220.229) 56(84) bytes of data.
64 bytes from www.fh-ooe.at (78.46.220.229): icmp_seq=1 ttl=58 time=22.6 ms
64 bytes from www.fh-ooe.at (78.46.220.229): icmp_seq=2 ttl=58 time=22.7 ms
64 bytes from www.fh-ooe.at (78.46.220.229): icmp_seq=3 ttl=58 time=22.7 ms
64 bytes from www.fh-ooe.at (78.46.220.229): icmp_seq=4 ttl=58 time=22.7 ms

--- web11.fh-ooe.at ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 7ms
rtt min/avg/max/mdev = 22.566/22.661/22.699/0.119 ms
```

```
[redacted]:~$ ping -6 -c 4 www.heise.de
PING www.heise.de(www.heise.de (2a02:2e0:3fe:1001:7777:772e:2:85)) 56 data bytes
64 bytes from www.heise.de (2a02:2e0:3fe:1001:7777:772e:2:85): icmp_seq=1 ttl=54 time=13.5 ms
64 bytes from www.heise.de (2a02:2e0:3fe:1001:7777:772e:2:85): icmp_seq=2 ttl=54 time=13.7 ms
64 bytes from www.heise.de (2a02:2e0:3fe:1001:7777:772e:2:85): icmp_seq=3 ttl=54 time=13.5 ms
64 bytes from www.heise.de (2a02:2e0:3fe:1001:7777:772e:2:85): icmp_seq=4 ttl=54 time=13.5 ms

--- www.heise.de ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 8ms
rtt min/avg/max/mdev = 13.474/13.533/13.683/0.166 ms
```

Internet Control Message Protocol

ping II (Wiederholung)



- Type (Code immer 0):
  - IPv4: 0 = Echo Reply, 8 = Echo (Request)
  - IPv6: 128 = Echo Request, 129 = Echo Reply
- Identifier identifiziert eine "Ping Session", Sequence Number identifiziert eine Echo Request Nachricht in einer "Ping Session".

- Mit `traceroute` kann ermittelt werden, über welche Router Pakete vom aufrufenden System (Quelle) aus zu einem bestimmten Ziel übertragen werden.
- Zweck: Bestimmen, wo am Wege von Quelle zum Ziel das/ein Problem (z. B. Loss, Verzögerung peakt) passiert.
- Wichtig!
  1. Mit `traceroute` kann immer nur der Weg von Quelle zu Ziel aber nicht umgekehrt bestimmt werden (warum?)!
  2. Das Ergebnis eines `traceroute`-Aufrufs ist von der Position der Quelle abhängig (vgl. Routenplanung)!

- Funktionsweise (Prinzip, im Detail komplizierter):
  1. *step* = 1
  2. Schicke eine IP Pakets mit Time to Live bzw. Next Header Wert *step*.
  3. System/Router *step* Hops entfernt verwirft das Paket + schickt eine ICMP Time Exceeded Nachricht
  4. Stammt ICMP Time Exceeded Nachricht vom Ziel? Wenn ja → ENDE, wenn nein → erhöhe *step* um 1 und setze bei Schritt 1 fort.
- Viele verschiedene Varianten: per ICMP Echo, UDP oder TCP SYN, Paris-Traceroute, Dublin-Traceroute

Internet Control Message Protocol

traceroute II (Wiederholung)

```
[redacted]:~$ sudo traceroute -I vu.nl
traceroute to vu.nl (37.60.194.64), 30 hops max, 60 byte packets
 1  185.252.74.1 (185.252.74.1)  0.290 ms  0.278 ms  0.232 ms
 2  192.168.255.1 (192.168.255.1)  0.356 ms  0.345 ms  0.303 ms
 3  83.164.137.141 (83.164.137.141)  1.821 ms  1.820 ms  1.794 ms
 4  openpeering-fra.peering.cz (91.213.211.18)  21.135 ms  21.135 ms  21.108 ms
 5  nikhef-cr.openpeering.nl (217.170.0.241)  28.175 ms  28.177 ms  28.132 ms
 6  openpeering.nikhef.jointtransit.nl (82.150.153.90)  36.777 ms  31.127 ms  31.102 ms
 7  gi2-24.sara-r9-alm.com.sara.nl (217.170.10.220)  27.743 ms  27.741 ms  27.701 ms
 8  ae1-0.vancis-asd01-r01.vancis.net (85.90.64.14)  27.910 ms  28.223 ms  28.179 ms
 9  po12-5.vancis-asd01-r02.vancis.net (85.90.64.21)  28.369 ms  28.418 ms  28.504 ms
10  isp-uplink-1458.vancis-fwc08.vancis.net (37.60.197.228)  27.918 ms  28.190 ms  28.137 ms
11  37.60.197.6 (37.60.197.6)  28.644 ms  28.566 ms  28.575 ms
12  37.60.194.64 (37.60.194.64)  28.178 ms  28.152 ms  28.067 ms
```

Internet Control Message Protocol

`traceroute` III (Wiederholung)

```
[redacted]:~$ sudo traceroute -I vu.nl
traceroute to vu.nl (37.60.194.64), 30 hops max, 60 byte packets
 1  static.209.26.46.78.clients.your-server.de (78.46.26.209)  0.479 ms  0.475 ms  0.473 ms
 2  core23.fsn1.hetzner.com (213.239.229.113)  26.841 ms  26.850 ms  26.848 ms
 3  core1.fra.hetzner.com (213.239.203.153)  4.927 ms  4.936 ms  4.935 ms
 4  * * *
 5  nikhef-cr.openpeering.nl (217.170.0.241)  18.256 ms  18.267 ms  18.266 ms
 6  * * *
 7  gi2-24.sara-r9-alm.com.sara.nl (217.170.10.220)  12.074 ms  12.250 ms  12.250 ms
 8  ae1-0.vancis-asd01-r01.vancis.net (85.90.64.14)  11.375 ms  11.405 ms  11.402 ms
 9  po12-5.vancis-asd01-r02.vancis.net (85.90.64.21)  11.381 ms  11.508 ms  11.890 ms
10  isp-uplink-1458.vancis-fwc08.vancis.net (37.60.197.228)  12.133 ms  12.120 ms  12.093 ms
11  37.60.197.6 (37.60.197.6)  12.574 ms  12.570 ms  12.549 ms
12  37.60.194.64 (37.60.194.64)  12.574 ms  12.304 ms  12.173 ms
```

traceroute IV (Wiederholung)

```
[redacted]:~$ sudo traceroute -6 -T vu.nl
traceroute to vu.nl (2001:4d60:12::64), 30 hops max, 80 byte packets
 1  2a0c:2344::1 (2a0c:2344::1)  0.387 ms  0.322 ms  0.299 ms
 2  fc00::1 (fc00::1)  45.279 ms  45.253 ms  87.313 ms
 3  2a00:1860:100:1004::1 (2a00:1860:100:1004::1)  88.005 ms  130.811 ms  172.395 ms
 4  r11-te1-5-16.core.lnz.net.lagis.at (2a00:1860:0:4::2)  214.414 ms  172.313 ms  171.534 ms
 5  2001:7f8:30:0:2:1:0:6939 (2001:7f8:30:0:2:1:0:6939)  258.269 ms  258.261 ms  258.178 ms
 6  * * *
 7  100ge14-2.core1.fra2.he.net (2001:470:0:2ef::1)  305.746 ms  53.094 ms  179.668 ms
 8  e0-32.core2.ams2.he.net (2001:470:0:489::2)  84.133 ms  229.352 ms  178.050 ms
 9  * * *
10  ae1-0.vancis-asd01-r01.vancis.net (2001:4d60:0:1029::1)  76.005 ms  35.372 ms  35.359 ms
11  po12-5.vancis-asd01-r02.vancis.net (2001:4d60:0:1030::2)  29.386 ms  29.191 ms  29.110 ms
12  isp-uplink-1458.vancis-fwc08.vancis.net (2001:4d60:0:1008::4)  35.293 ms  35.846 ms  35.289 ms
13  2001:4d60:12:ffff::1 (2001:4d60:12:ffff::1)  30.756 ms  30.692 ms  30.619 ms
14  2001:4d60:12::64 (2001:4d60:12::64)  29.691 ms  29.865 ms  37.243 ms
```

traceroute V (Wiederholung)

```
[redacted]:~$ sudo traceroute -6 -T vu.nl
traceroute to vu.nl (2001:4d60:12::64), 30 hops max, 80 byte packets
 1  * * *
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * *^C
```

- Viele Systeme/Netzwerke filtern/blocken ICMP Nachrichten aus Sicherheits- und/oder aus Performance-Gründen (Router-Belastung reduzieren).
  - IPv4: Generell möglich, IPv4 + TCP/UDP "funktioniert" auch ohne ICMP.
  - IPv6: Generell nicht möglich, ICMPv6 wichtig für NDP und SLAAC[1]
- Zumeist geht es dabei um Blocken von `ping` und `traceroute` (v4 Type 0, 8 und 11, v6 Type 3, 128 und 129)
  - Pro: Macht Systeme "unsichtbar" $\rightarrow$ schwieriger anzugreifen
  - Contra: Vorhandensein von Systemen auf anderen Ebenen (Schicht-2 und -4) testbar, was nicht einfach geblockt werden kann, Blocking erschwert Netzwerk-Management

[1] Enno Rey, Local Packet Filtering with IPv6, RIPE Labs, Juli 2017

- Es kommt auch stark darauf an, WO und VON WO NACH WOHIN ICMP Blocking durchgeführt wird!
- Das Blocken von ICMP Error Nachrichten versucht auf jeden Fall mehr Schaden als Nutzen (z. B. PMTUD)!
- In jedem Fall eine Never-Ending Discussion[2] [3] [4] [5]!

[2] Enno Rey, Local Packet Filtering with IPv6, RIPE Labs, Juli 2017
[3] Twitter Feed Enno Rey, Juni 2020
[4] Stack Exchange, Is it a bad idea for a firewall to block ICMP?, Oktober 2012
[5] http://shouldidisableicmp.com/, http://shouldiblockicmp.com/


Fragen
Ceisteanna
Froen
Vragen
Spørgsmål
Preguntas
Pitanja
Questions
Quaestiones
Domande
Kérdések
Vprašanja
Cwestiynau
Frågor
Spurningar
Galderak
Kysymykset
Mistoqsijiet