Internet Control Message Protocol (ICMP)

Einführung

Das *Internet Control Message Protocol* (ICMP) dient dem Zweck der Übertragung von Statusinformationen und Fehlermeldungen der Protokolle IP, TCP und UDP zwischen IP−Netzwerkknoten.
ICMP nutzt das *Internet Protocol* (IP) als wäre es selber in einer höheren Schicht als IP angesiedelt. Tatsächlich ist ICMP ein wesentlicher Teil von IP und muß von jedem IP−Modul eingebunden werden. ICMP ist zusammen mit IP im OSI−Schichtenmodell in der Vermittlungsschicht (Schicht 3) angesiedelt.

ICMP wurde definiert, da IP selber keine Funktion zur Status− oder Fehlerübermittlung vorsieht. Ein Sender, der ein Datagramm (Paket) per IP überträgt haben weder Anspruch darauf, daß das Paket ankommt, oder falls es ankommt, daß es korrekt übertragen wurde. Auch wird er nicht darüber informiert, wenn letzterer Fall eintritt. An diesem Punkt setzt ICMP an.

ICMP wurde im September 1981 im *Request For Comments* (RFC) Nummer 792 von der *Network Working Group* auf Basis des IPv4 beschrieben. Mit der Spezifizierung des *Internet Protocol Version 6* (IPv6) wurde auch ICMP für IPv6 (kurz ICMPv6) im RFC 1885 vom Dezember 1995 von der *Network Working Group* neu definiert.
Für ICMPv4 wurden im Nachhinein noch diverse Erweiterungen definiert, die sich jedoch in den seltensten Fällen wirklich durchgesetzt haben.

Im folgenden wird das zur Zeit noch weit verbreitete ICMPv4 näher erläutert. Interessenten an ICMPv6 werden auf die RFC 1885 verwiesen.

ICMPv4

Da von Sender oder Empfänger ein aufgetretener Fehler bei der Übertragung festgestellt wird, ist es sinnvoll diese Information auch zu verwenden. Die Hauptaufgabe von ICMP ist nun eben diese Übertragung von Fehlerinformationen. Weitere Funktionen sind vor allem die Übermittlung von Informationen zu Diagnose− oder Optimierungszwecken. Es können auch jederzeit neue Funktionalitäten in ICMP eingebaut werden, so daß eine Anpassung an neue Anforderungen ohne Einführung eines neuen Protokolls möglich ist.

Trigger

ICMP−Nachrichten verschicken sich nicht einfach selbst, sondern es braucht einen Auslöser. Die Ursache für das Versenden einer ICMP−Nachricht kann recht vielfältig sein, die wichtigsten Ursachen sind:

- Fehler beim Weiterleiten eines Pakets durch einen Router
  z.B.: der Router hat keine Informationen, wohin das Paket weitergeleitet werden soll oder es wurde fehlerhaft übertragen
- Fehler bei der Verarbeitung eines Pakets durch den Empfänger
  z.B.: Fehlerhafte Übertragung, das übergeordnete Protokoll ist unbekannt oder ein fragmentiertes Paket ist unvollständig
- Suboptimaler Zustand
  z.B.: falsches Routing, Überlastung eines Links
- Aufruf eines ICMP−Requests
  z.B.: Programm ‚ping'
- an den Rechner adressierter Request
  z.B.: durch ‚ping' ausgelöster *Echo−Request*

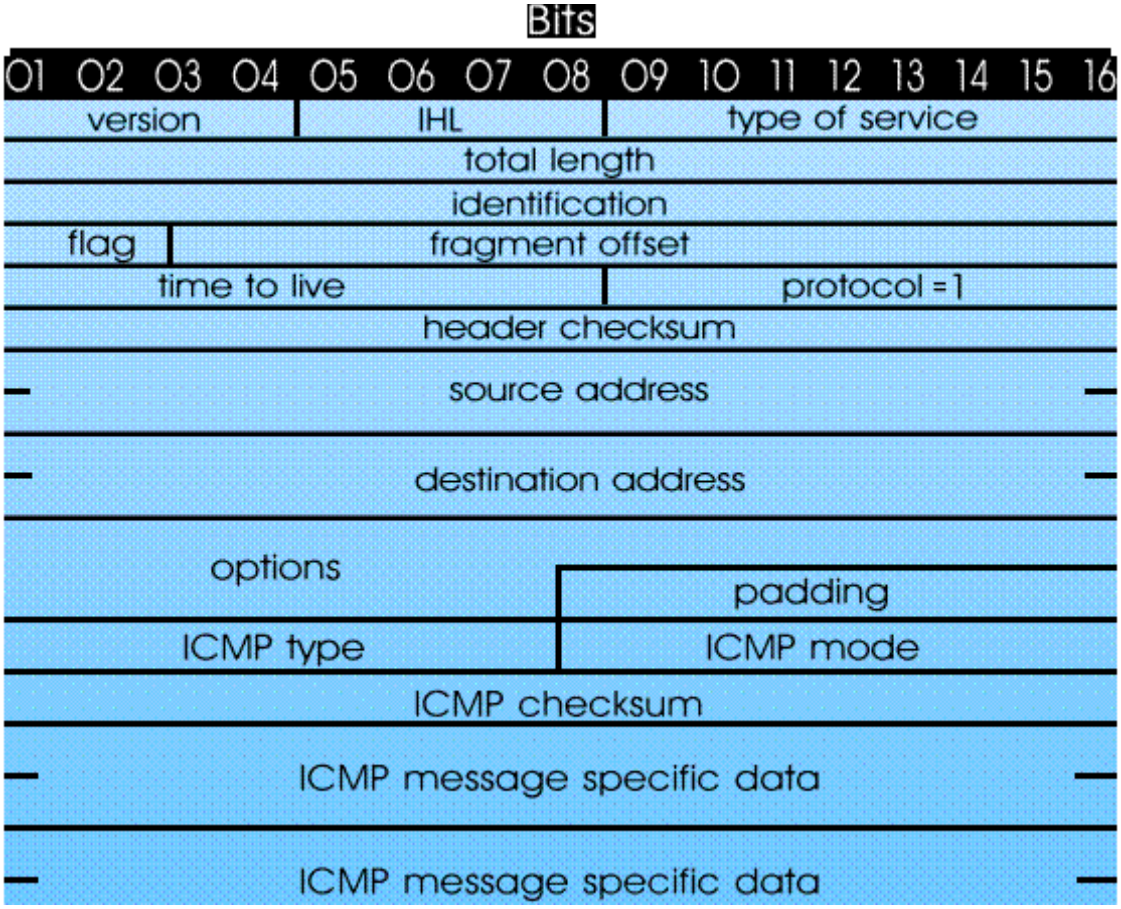
Weiterhin existieren einige Einschränkungen, damit das Netz nicht durch zu viel ICMP−Verkehr belastet wird:

- Vermeidung von Schleifen
  Wenn der Trigger eine andere ICMP−Nachricht ist, wird keine ICMP−Nachricht ausgesandt
- Einschränkung der Bandbreite
  Es wird vorgeschlagen maximal 1 ICMP−Nachricht pro Sekunde zu versenden oder maximal 2% der Bandbreite für ICMP−Nachrichten zu verwenden
- Unterscheidung von Fragmenten
  Ist ein Fragment der Trigger, wird nur dann eine ICMP−Nachricht verschickt, wenn es sich um das erste Fragment (Offset=0) handelt.

Diese Einschränkungen gelten nicht für Antworten auf ICMP−Requests.

Kein Rechner ist verpflichtet, ICMP−Nachrichten zu versenden, mit einer Ausnahme: Jeder Rechner muß auf ein *Echo−Request* immer mit einem *Echo−Reply* antworten (auch *Ping* und *Pong* genannt).

Nachrichtenformat



Der ICMP−Header ist als eine Erweiterung des IP−Headers anzusehen. Daher setzt sich der ICMP−Header auch aus einem IP−Header mit nachfolgenden ICMP−Daten zusammen.
Der *Type of Service* indiziert bei ICMP−Nachrichten eine 'Routine'−Nachricht ohne spezielle Anforderungen. Weiterhin identifiziert *protocol* mit dem Wert 1 den Inhalt als ICMP−Paket. Die anderen Felder werden vom System wie bei jedem anderen IP−Paket ausgefüllt, bis auf den ICMP−Header, der bei *ICMP type* beginnt.

Unter dem ICMP−Protokoll wurden 15 verschiedene Pakettypen festgelegt. Die wesentlichen Felder des ICMP−Headers sind das Typfeld (*ICMP type*) und das Codefeld (*ICMP mode*), beide jeweils 8 Bit lang. Sie bestimmen gemeinsam die Funktionalität der einzelnen ICMP−Pakete. Die eigentlichen Informationen werden im Nachrichtenfeld (*ICMP message specific data*) eingetragen, dies kann dann auch noch einmal weitere Felder beinhalten.

Die wichtigsten ICMP−Pakettypen werden im folgenden näher betrachtet. Weitere Einzelheiten sind bei Interesse den RFCs zu entnehmen.

Pakettypen

Typ	Code	Bedeutung
0		Echo Reply
3		Destination unreachable
3	0	net unreachable
3	1	host unreachable
3	2	protocol unreachable
3	3	port unreachable

3	4	fragmentation needed and DF set
3	5	source route failed
4	0	Source Quench
5		Redirect Message
5	0	Redirect datagrams for the Network
5	1	Redirect datagrams for the Host
5	2	Redirect datagrams for the Type of Service and Network
5	3	Redirect datagrams for the Type of Service and Host
8		Echo Request
11		Time Exceeded
11	0	time to live exceeded in transit
11	1	fragment reassembly time exceeded
12		Parameter Problem
12	0	pointer indicates the error
13		Timestamp Request
14		Timestamp Reply
15		Information Request
16		Information Reply

Empfängt ein Rechner also eine Nachricht mit Typ=3 und Code=2, so kann er bei Kenntnis von Type und Code recht genau bestimmen, was die Ursache des Fehlers ist, in diesem Fall daß der Absender das vorher angesprochene Protokoll nicht kannte. Kennt er den Code nicht, so weiß er nur, daß der Absender aus irgendeinem Grund nicht erreichbar war. Wenn er auch den Typ nicht kennt, kann er mit der Nachricht natürlich gar nichts anfangen. Die oben aufgeführten Nummern sind allerdings wahrscheinlich allen Rechnern bekannt, aber bei den vielen Erweiterungen muß das nicht der Fall sein.
Wenn wir uns das obige Beispiel ansehen, so stellt sich z.B. die Frage, auf welches Paket und welches Protokoll sich die Fehlermeldung bezog. Abhängig vom Typ (und manchmal auch Code) haben die Nachrichten noch entsprechende Informationen im Nachrichtentext. Bei Fehlermeldungen sind dies 32 Bit für weitere Felder und anschließend der IP−Header und die ersten 64 Bit des verursachenden Pakets, aber bei anderen Nachrichten kann man die Nachrichtentexte nur auswerten, wenn man den Typ (und den Code) kennt. Die Checksumme dient dazu die Korrektheit der Nachricht zu gewährleisten.

Destination Unreachable

Type	Code	Checksum
unused		
Internet Header + 64 bits of Original Datagram		

Eine ’Destination Unreachable’−Nachricht wird verschickt, wenn ein Paket nicht zugestellt werden kann, weil der Empfänger nicht erreichbar ist. Die Ursachen können sehr vielfältig sein, z.B. daß der Empfänger nicht existiert, kein passendes Protokoll geladen ist oder das Routing nicht geklappt hat.

Packet Too Big

Type	Code	Checksum
unused		
Internet Header + 64 bits of Original Datagram		

Eine ’Packet Too Big’−Nachricht wird versandt, wenn ein Paket nicht weitergeleitet werden konnte, weil sie zu lang war, aber nicht fragmentiert werden durfte. Diese Nachricht ist Grundlage für PMTU−Discovery, ein

Verfahren um automatisch die ideale MTU−Größe (Maximum Transfer Unit − Größe der einzelnen Paketfragmente) zu ermitteln.

Time Exceeded

Type	Code	Checksum
unused		
Internet Header + 64 bits of Original Datagram		

Befindet sich eine Nachricht so lange im Netz, daß die 'Time To Live' abgelaufen ist, so wird eine 'Time Exceeded'−Nachricht verschickt. Eine andere Ursache ist das Ausbleiben von Fragmenten einer Nachricht.

Parameter Problem

Type	Code	Checksum
Pointer	unused	
Internet Header + 64 bits of Original Datagram		

Es ist ein Problem beim Auswerten der Nachricht aufgetreten, das auf fehlerhafte oder unbekannte Parameter zurückzuführen ist. Der Pointer ist hierbei ein Zeiger auf die Position an der das Problem auftrat.

Source Quench

Type	Code	Checksum
unused		
Internet Header + 64 bits of Original Datagram		

Hat ein Rechner Probleme, die ankommenden Pakete rechtzeitig zu verarbeiten, so sendet er eine 'Source Quench'−Nachricht. Diese veranlaßt den Sender, die Rate seiner Pakete zu vermindern. Dieses Verfahrens ist jedoch angeblich viel zu ineffizient, so daß andere Methoden zur Staukontrolle und −vermeidung bevorzugt werden sollten.
Da ein Router diese Nachricht auch schon bei hoher Auslastung verschicken kann, ohne daß das Paket verloren geht, kann nicht entschieden werden, ob es sich um einen wirklichen Fehler (Verlust des Paketes) oder nur um eine Information handelt.

Redirect

Type	Code	Checksum
Gateway Internet Address		
Internet Header + 64 bits of Original Datagram		

Bemerkt ein Router, daß es für eine Nachricht einen besseren Weg gibt, als über diesen Router, so kann er eine Empfehlung verschicken, weitere Nachrichten zum gleichen Ziel, über die angegebene Gateway−Adresse zu routen.
Da das Paket nicht verloren geht, handelt es sich um eine reine Informationsnachricht.

Echo Request / Reply

Type	Code	Checksum
Identifier		Sequence Number
Data		

Die wohl bekannteste Anwendung, die auf ICMP basiert ist 'ping', ein Programm zum versenden von Diagnose−Nachrichten. Hierbei wird von dem Programm ein Echo−Request ausgelöst und zum anderen Rechner geroutet. Dieser **muß** auf den Request mit einem Reply antworten. Erhält der erste Rechner die Antwort, so erhält der Benutzer eine entsprechende Ausgabe (z.B. rechner2 is alive, ggf. mit Angabe einer Round Trip Time).
Ein Echo Request ist die einzige ICMP−Nachricht, auf die jeder IP−fähige Rechner antworten muß.

Timestamp Request / Reply

Type	Code	Checksum
Identifier		Sequence Number
Originate Timestamp		
Receive Timestamp		
Transmit Timestamp		

Die ’Timestamp Request’− und ’Timestamp Reply’−Nachrichten ermöglichen die Zeitsynchronisation zweier Rechner. Da jedoch weitere Protokolle wie NTP oder SNTP eingeführt wurden, ist dieser Nachrichtentyp überflüssig geworden.

Information Request / Reply

Type	Code	Checksum
Identifier		Sequence Number

Dieser Nachrichtentyp ermöglicht es einem Host, seine Netz−Adresse zu erfahren.

Quellenangaben

Achim Thesmann, "Internet Control Message Protocol (ICMP) und Path−MTU Discovery bei IPv4 und IPv6" 19.02.1997
[http://www.uni−koblenz.de/~thesmann/ICMP/ICMP.html]

Internet Control Message Protocol
[http://www.snutz.de/computer/icmp.htm]

NetworkWorld Germany − Glossar:ICMP−Protokoll
[http://www.gateway.de/knowledge/lexikon/docs/5/F005395.HTM]

NetworkWorld Germany − Glossar:ICMP−Header
[http://www.gateway.de/knowledge/lexikon/docs/1/F009301.HTM]

NetworkWorld Germany − Glossar:ICMP−Pakettypen
[http://www.gateway.de/knowledge/lexikon/docs/5/02005395.HTM]

NetworkWorld Germany − Glossar:Aufbau des ICMP−Datenrahmens
[http://www.gateway.de/knowledge/lexikon/docs/5/01005395.HTM]

J. Postel, "RFC 792 − Internet Control Message Protocol", 01.09.1981
[http://www.uni−koblenz.de/~thesmann/ICMP/rfc792.txt]

A. Conta, S. Deering, "RFC 1885 − Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6)",04.01.1996
[http://www.uni−koblenz.de/~thesmann/ICMP/rfc1885.txt]