23. Trainer – OSI-Schicht 3

- ICMP (Internet Control Message Protocol)

ICMP (Internet Control Message Protocol)

ICMP einfach erklärt

ICMP steht für **Internet Control Message Protocol**.

ICMP ist ein Kontroll- und Fehlerprotokoll der Internetprotokollfamilie. Es wird nicht wie TCP oder UDP verwendet, um normale Nutzdaten zwischen Anwendungen zu übertragen, sondern um Statusinformationen, Fehlermeldungen und Diagnoseinformationen im IP-Netzwerk zu senden.

Kurz gesagt:

```
TCP  = zuverlässige Datenübertragung zwischen Anwendungen
UDP  = schnelle, verbindungslose Datenübertragung zwischen Anwendungen
ICMP = Kontroll- und Fehlermeldungen im IP-Netzwerk
```

Wofür wird ICMP verwendet?

ICMP wird verwendet, um Netzwerkprobleme zu melden oder die Erreichbarkeit von Geräten zu prüfen.

Typische Einsatzbereiche:

```
- Erreichbarkeit eines Hosts prüfen
- Netzwerkfehler melden
- Routing-Probleme anzeigen
- Zeitüberschreitungen melden
- Paketgrößenprobleme melden
- Diagnosewerkzeuge wie ping und traceroute ermöglichen
```

ICMP ist also eher ein Hilfsprotokoll für IP-Netzwerke.

ICMP ist kein normales Transportprotokoll wie TCP oder UDP

TCP und UDP transportieren Daten zwischen Anwendungen.

Beispiele:

- HTTPS
- SSH
- DNS
- VoIP
- Streaming
- Online-Gaming

ICMP macht das normalerweise nicht.

ICMP wird eher verwendet, damit Geräte im Netzwerk melden können:

- Ziel nicht erreichbar.
- Paket konnte nicht zugestellt werden.
- Zeit wurde überschritten.
- Paket ist zu groß.
- Host antwortet auf Ping.

Merksatz:

TCP und UDP übertragen Anwendungsdaten.
ICMP meldet Netzwerkzustände und Fehler.

Beispiel: Ping mit ICMP

Das bekannteste Beispiel für ICMP ist **ping**.

Mit ping prüft man, ob ein Gerät im Netzwerk erreichbar ist.

Beim klassischen ping wird ICMP verwendet.

Bei IPv4:

ICMP Echo Request
ICMP Echo Reply

Bei IPv6:

ICMPv6 Echo Request
ICMPv6 Echo Reply

Ablauf vereinfacht:

```
Dein PC                    Zielhost

ICMP Echo Request  --------->

ICMP Echo Reply    <---------
```

Das bedeutet:

```
Echo Request = Bist du erreichbar?
Echo Reply   = Ja, ich bin erreichbar.
```

Wenn eine Antwort zurückkommt, weiß man:

```
Der Zielhost ist grundsätzlich erreichbar.
```

Wenn keine Antwort zurückkommt, kann das verschiedene Gründe haben:

```
- Zielhost ist ausgeschaltet
- Netzwerkweg ist unterbrochen
- Firewall blockiert ICMP
- Zielhost antwortet nicht auf Ping
- Routing-Problem liegt vor
```

Wichtig:

```
Wenn ping nicht funktioniert, heißt das nicht automatisch,
dass der Host komplett offline ist.
```

Ein Gerät kann erreichbar sein, aber ICMP blockieren.

Nutzt Ping immer ICMP?

Das klassische Betriebssystem-Tool **ping** nutzt normalerweise ICMP.

Also zum Beispiel:

```
Windows ping
Linux ping
macOS ping
```

Diese klassischen ping-Befehle senden ICMP Echo Requests und erwarten ICMP Echo Replies.

Prüfungssicher gesagt:

```
Klassisches ping = ICMP Echo Request und ICMP Echo Reply
```

Aber:

```
Der Begriff "Ping" wird im Alltag nicht immer ausschließlich für ICMP verwendet.
```

Manchmal sagen Menschen auch "Ping", wenn sie allgemein eine Erreichbarkeit oder Antwortzeit testen.

Beispiele:

```
- TCP-Ping
- UDP-Ping
- HTTP-Ping
- Game-Ping
```

Das ist dann oft kein echtes ICMP-Ping, sondern ein anderer Latenz- oder Erreichbarkeitstest.

Beispiele:

```
TCP-Ping prüft, ob ein bestimmter TCP-Port erreichbar ist.
HTTP-Ping prüft, ob ein Webserver antwortet.
Game-Ping zeigt oft die Antwortzeit zum Spielserver.
UDP-Ping kann mit eigenen UDP-Anfragen und Antworten arbeiten.
```

Wichtige Unterscheidung:

```
Klassisches ping-Tool = ICMP
Umgangssprachlicher Ping = manchmal auch anderer Verbindungstest
```

Ist ICMP nur für Ping da?

Nein.

ICMP wird nicht nur für Ping verwendet.

Ping ist nur eine bekannte Anwendung von ICMP.

ICMP kann auch viele andere Kontroll- und Fehlermeldungen übertragen.

Beispiele:

```
- Destination Unreachable
- Time Exceeded
- Fragmentation Needed
- Redirect
```

Also:

```
Ping nutzt ICMP.
Aber ICMP ist nicht nur Ping.
```

Merksatz:

```
Klassisches ping nutzt ICMP.
ICMP wird aber nicht ausschließlich für ping verwendet.
```

ICMP arbeitet nicht mit Ports

Ein wichtiger Unterschied zu TCP und UDP ist:

```
TCP und UDP verwenden Ports.
ICMP verwendet keine Ports.
```

Beispiele für TCP und UDP:

```
TCP 443 = HTTPS
TCP 22  = SSH
UDP 53  = DNS
```

```
UDP 123 = NTP
```

ICMP hat keine Portnummern.

Stattdessen arbeitet ICMP mit **Typen** und **Codes**.

Merksatz:

```
TCP/UDP = Ports
ICMP    = Typen und Codes
```

ICMP-Typen und Codes

ICMP verwendet Typen und Codes, um verschiedene Meldungen zu unterscheiden.

ICMP-Meldung	Bedeutung
Echo Request	Anfrage bei ping
Echo Reply	Antwort auf ping
Destination Unreachable	Ziel nicht erreichbar
Time Exceeded	Zeit überschritten
Redirect	Hinweis auf besseren Weg
Fragmentation Needed	Paket ist zu groß und müsste fragmentiert werden

Die genaue Bedeutung wird über ICMP-Typ und ICMP-Code festgelegt.

Beispiel:

```
Echo Request = Ping-Anfrage
Echo Reply   = Ping-Antwort
```

Merksatz:

```
TCP/UDP nutzen Ports.
ICMP nutzt Typen und Codes.
```

Beispiel: Destination Unreachable

Eine typische ICMP-Fehlermeldung ist:

```
Destination Unreachable
```

Auf Deutsch:

```
Ziel nicht erreichbar
```

Das kann passieren, wenn ein Paket nicht zugestellt werden kann.

Mögliche Gründe:

```
- Zielnetz ist nicht erreichbar
- Zielhost ist nicht erreichbar
- Port oder Dienst ist nicht erreichbar
- Firewall blockiert den Verkehr
- Routing fehlt oder ist falsch
```

Vereinfacht gesagt meldet ein Router oder Zielsystem:

```
Ich kann dieses Paket nicht zustellen.
```

Beispiel: Time Exceeded

Eine weitere wichtige ICMP-Meldung ist:

```
Time Exceeded
```

Auf Deutsch:

```
Zeit überschritten
```

Das hängt mit dem TTL-Wert zusammen.

TTL steht für:

```
Time To Live
```

Jedes IP-Paket hat einen TTL-Wert. Dieser Wert wird bei jedem Router um 1 verringert.

Wenn der TTL-Wert bei 0 angekommen ist, wird das Paket verworfen.

Dann kann eine ICMP-Meldung zurückgesendet werden:

```
Time Exceeded
```

Das bedeutet:

```
Das Paket hat sein Ziel nicht rechtzeitig erreicht.
Es wurde unterwegs verworfen.
```

Diese Funktion wird zum Beispiel bei traceroute genutzt.

ICMP und traceroute

Traceroute zeigt, über welche Router ein Paket zum Ziel läuft.

Dafür nutzt traceroute unter anderem ICMP-Time-Exceeded-Meldungen.

Vereinfacht:

```
1. Das erste Paket bekommt TTL 1.
2. Der erste Router verringert TTL auf 0.
3. Der Router verwirft das Paket.
4. Der Router sendet ICMP Time Exceeded zurück.
5. Dadurch erkennt traceroute den ersten Router.
6. Danach wird TTL erhöht.
7. So werden die nächsten Router sichtbar.
```

Dadurch kann man den Weg durch das Netzwerk nachvollziehen.

Merksatz:

```
Ping prüft, ob ein Ziel antwortet.
Traceroute zeigt den Weg zum Ziel.
```

ICMP und Paketgröße

ICMP kann auch melden, dass ein Paket zu groß ist.

Das ist wichtig für die sogenannte Path MTU Discovery.

MTU steht für:

```
Maximum Transmission Unit
```

Die MTU beschreibt, wie groß ein Paket auf einem Netzwerkabschnitt maximal sein darf.

Wenn ein Paket zu groß ist und nicht fragmentiert werden darf, kann eine ICMP-Meldung zurückkommen:

```
Fragmentation Needed
```

Das bedeutet:

```
Das Paket ist für diesen Netzwerkweg zu groß.
Der Absender soll kleinere Pakete senden.
```

Wichtig:

```
Wenn solche ICMP-Meldungen blockiert werden,
kann es zu Verbindungsproblemen kommen.
```

Zum Beispiel können Webseiten teilweise laden oder VPN-Verbindungen Probleme machen.

ICMP im Vergleich zu TCP und UDP

Merkmal	TCP	UDP	ICMP
Voller Name	Transmission Control Protocol	User Datagram Protocol	Internet Control Message Protocol
Hauptaufgabe	zuverlässige Datenübertragung	schnelle Datagramm-Übertragung	Kontroll- und Fehlermeldungen
Verbindungsaufbau	Ja, 3-Wege-Handshake	Nein	Nein
Ports	Ja	Ja	Nein
Arbeitet mit	Ports, Sequenznummern, ACKs	Ports, Datagrammen	Typen und Codes
Zustellgarantie	Ja, eingebaut	Nein	Nein
Reihenfolgekontrolle	Ja	Nein	Nein

Merkmal	TCP	UDP	ICMP
Typische Nutzung	HTTPS, SSH, E-Mail	DNS, VoIP, Streaming	ping, traceroute, Fehlermeldungen
Nutzdaten von Anwendungen	Ja	Ja	Normalerweise nein

TCP, UDP und ICMP einfach unterschieden

TCP:

TCP baut zuerst eine Verbindung auf.
TCP überträgt Daten zuverlässig.
TCP bestätigt empfangene Daten.
TCP sendet verlorene Daten erneut.
TCP nutzt Ports.

UDP:

UDP baut keine Verbindung auf.
UDP sendet Daten direkt los.
UDP hat weniger Verwaltungsaufwand.
UDP garantiert keine Zustellung.
UDP nutzt Ports.

ICMP:

ICMP überträgt normalerweise keine Anwendungsdaten.
ICMP meldet Fehler und Zustände im Netzwerk.
ICMP wird für Diagnose genutzt.
ICMP nutzt keine Ports.
ICMP arbeitet mit Typen und Codes.

ICMP und Firewall

Firewalls können ICMP erlauben oder blockieren.

Beispiele:

- Ping erlauben
- Ping blockieren
- bestimmte ICMP-Fehlermeldungen erlauben
- bestimmte ICMP-Typen blockieren

Wichtig:

ICMP komplett zu blockieren ist nicht immer sinnvoll.

Warum?

Bestimmte ICMP-Meldungen sind wichtig für die korrekte Funktion von Netzwerken.

Beispiele:

- Destination Unreachable
- Time Exceeded
- Fragmentation Needed

Wenn diese Meldungen blockiert werden, kann die Fehlersuche schwieriger werden oder bestimmte Verbindungen können Probleme machen.

Prüfungssicherer Gedanke:

ICMP sollte nicht blind komplett blockiert werden.
Besser ist es, gezielt festzulegen, welche ICMP-Typen erlaubt oder blockiert werden.

Ist ICMP gefährlich?

ICMP ist nicht automatisch gefährlich.

Es kann aber für Angriffe oder Informationsgewinnung missbraucht werden.

Beispiele:

- Ping-Scans zur Erkennung erreichbarer Hosts
- ICMP-Flooding als DoS-Angriff
- Netzwerkaufklärung durch traceroute

Deshalb wird ICMP in vielen Netzwerken eingeschränkt.

Aber:

> ICMP hat auch wichtige Diagnose- und Fehlerfunktionen.

Deshalb ist die beste Lösung meistens nicht:

> Alles blockieren.

Sondern besser:

> Nur benötigte ICMP-Typen erlauben.
> Unnötige oder gefährliche ICMP-Nutzung einschränken.

Wichtige ICMP-Begriffe

Begriff	Bedeutung
ICMP	Internet Control Message Protocol
ICMPv6	ICMP für IPv6
Echo Request	Ping-Anfrage
Echo Reply	Ping-Antwort
Destination Unreachable	Ziel nicht erreichbar
Time Exceeded	Zeit überschritten
TTL	Time To Live
MTU	Maximum Transmission Unit
Typ	Art der ICMP-Meldung
Code	genauere Beschreibung der ICMP-Meldung

Beispielhafte Einordnung im Netzwerk

Normale Datenübertragung mit TCP:

> Client → TCP-Verbindung → Server
> Beispiel: HTTPS-Webseite über TCP-Port 443

Normale Datenübertragung mit UDP:

```
Client → UDP-Datagramm → Server
Beispiel: DNS-Anfrage über UDP-Port 53
```

Kontrollmeldung mit ICMP:

```
Router oder Zielhost → ICMP-Meldung → Absender
Beispiel: Ziel nicht erreichbar oder Zeit überschritten
```

IHK-sichere Kurzformulierung

ICMP ist ein Kontrollprotokoll der Internetprotokollfamilie. Es dient nicht der normalen Datenübertragung zwischen Anwendungen, sondern wird für Fehler- und Statusmeldungen im IP-Netzwerk verwendet. Typische Beispiele sind das klassische ping mit ICMP Echo Request und ICMP Echo Reply sowie Fehlermeldungen wie Destination Unreachable oder Time Exceeded. Im Gegensatz zu TCP und UDP verwendet ICMP keine Ports, sondern Typen und Codes. Wichtig ist: Klassisches ping nutzt ICMP, aber ICMP wird nicht ausschließlich für ping verwendet. Außerdem wird der Begriff "Ping" umgangssprachlich manchmal auch für andere Latenz- oder Erreichbarkeitstests genutzt, zum Beispiel TCP-Ping, HTTP-Ping oder Game-Ping.

Merksätze

```
TCP transportiert zuverlässig.

UDP transportiert schnell und einfach.

ICMP meldet, prüft und diagnostiziert.

TCP und UDP verwenden Ports.

ICMP verwendet keine Ports.

TCP = Verbindung und Zuverlässigkeit

UDP = keine Verbindung und wenig Verwaltungsaufwand

ICMP = Kontroll- und Fehlermeldungen
```

Klassisches ping nutzt ICMP Echo Request und ICMP Echo Reply.

ICMP ist aber nicht nur für ping da.

Der Begriff "Ping" wird umgangssprachlich manchmal auch für andere Antwortzeit-Tests verwendet.

Traceroute nutzt unter anderem ICMP Time Exceeded.

Wenn ping nicht funktioniert,
heißt das nicht automatisch,
dass der Zielhost komplett offline ist.

ICMP sollte nicht pauschal komplett blockiert werden,
weil einige ICMP-Meldungen für Diagnose und Netzwerkfunktion wichtig sind.