6.4 ICMP, Ping und Traceroute

ICMP gehört zu den wichtigsten Protokollen im Umfeld von OSI-Schicht 3.

ICMP steht für:

```
Internet Control Message Protocol
```

Auf Deutsch sinngemäß:

```
Internet-Kontrollnachrichten-Protokoll
```

ICMP wird verwendet, um Kontroll- und Fehlermeldungen im IP-Netz zu übertragen.

Merksatz:

```
ICMP = Kontroll- und Fehlermeldungen für IP.
```

Warum gibt es ICMP?

IP selbst ist ein verbindungsloses Protokoll.

Das bedeutet:

```
IP sendet Pakete weiter,
baut aber keine Verbindung wie TCP auf.
```

Wenn im IP-Netz etwas nicht funktioniert, braucht man trotzdem Rückmeldungen.

Beispiele:

```
Ziel nicht erreichbar
Paket zu groß
TTL abgelaufen
Echo-Anfrage
Echo-Antwort
```

Diese Meldungen werden über ICMP übertragen.

Merksatz:

```
ICMP ergänzt IP um Kontroll- und Fehlermeldungen.
```

ICMP im OSI-Modell

ICMP gehört fachlich zum IP-Umfeld.

Es wird meistens bei Schicht 3 eingeordnet.

Warum?

```
ICMP arbeitet mit IP.
ICMP wird für IP-Kontrollmeldungen verwendet.
ICMP nutzt keine TCP- oder UDP-Ports.
```

Wichtig:

```
ICMP ist nicht TCP.
ICMP ist nicht UDP.
```

Merksatz:

```
ICMP gehört zum IP-Umfeld auf Schicht 3.
```

ICMP und Ports

ICMP nutzt keine TCP- oder UDP-Ports.

Das ist eine wichtige Prüfungsfalle.

TCP und UDP arbeiten mit Ports.

Beispiele:

```
TCP 80 = HTTP
TCP 443 = HTTPS
UDP 53 = DNS
```

ICMP arbeitet anders.

ICMP verwendet:

```
Typ
und
Code
```

Merksatz:

```
ICMP hat keine Ports,
sondern Typ und Code.
```

ICMP-Typ und ICMP-Code

ICMP-Nachrichten werden durch Typ und Code genauer beschrieben.

Der Typ sagt grob, welche Art von Nachricht es ist.

Der Code beschreibt die Nachricht genauer.

Beispiel:

ICMP-Nachricht	Bedeutung
Echo Request	Anfrage bei Ping
Echo Reply	Antwort bei Ping
Destination Unreachable	Ziel nicht erreichbar
Time Exceeded	Zeit / TTL abgelaufen

Für AP1/AP2 reicht meistens:

```
ICMP nutzt Typ und Code,
nicht TCP- oder UDP-Ports.
```

Merksatz:

```
Typ = Art der ICMP-Nachricht.
Code = genauere Ursache.
```

Ping

Ping ist ein Werkzeug zur Prüfung der IP-Erreichbarkeit.

Ping verwendet klassisch ICMP Echo Request und ICMP Echo Reply.

Vereinfacht:

```
Echo Request:
Bist du erreichbar?

Echo Reply:
Ja, ich bin erreichbar.
```

Wenn eine Antwort kommt, weiß man:

```
Das Ziel ist grundsätzlich per IP erreichbar.
Der Rückweg funktioniert ebenfalls.
ICMP wird nicht blockiert.
```

Merksatz:

```
Ping prüft grundlegende IP-Erreichbarkeit.
```

Ping-Ablauf

Beispiel:

```
PC pingt 192.168.10.1
```

Vereinfacht passiert:

```
1. PC erstellt ICMP Echo Request.
2. ICMP wird in ein IP-Paket verpackt.
3. IP-Paket wird lokal als Ethernet-Frame gesendet.
4. Zielgerät empfängt die Anfrage.
5. Zielgerät sendet ICMP Echo Reply zurück.
6. PC misst Antwortzeit und Paketverlust.
```

Merksatz:

```
Ping sendet ICMP-Anfrage und erwartet ICMP-Antwort.
```

Was Ping anzeigen kann

Ping kann zeigen:

```
- Ziel antwortet oder antwortet nicht
- ungefähre Antwortzeit
- Paketverlust
- Namensauflösung, wenn ein Name verwendet wird
- ob grundsätzlich IP-Kommunikation möglich ist
```

Beispiel:

```
ping 192.168.10.1
```

prüft direkt eine IP-Adresse.

Beispiel:

```
ping www.example.com
```

prüft zusätzlich, ob der Name aufgelöst werden kann.

Merksatz:

```
Ping auf IP prüft IP-Erreichbarkeit.
Ping auf Name prüft zusätzlich DNS-Auflösung.
```

Was Ping nicht sicher beweist

Ein erfolgreicher Ping bedeutet nicht automatisch:

```
Webseite funktioniert.
TCP-Port ist offen.
```

Anwendung läuft.
Benutzer kann sich anmelden.
Firewall erlaubt alle Dienste.
DNS ist vollständig korrekt.
Netzwerk ist fehlerfrei.

Ping prüft nur eine bestimmte Art von Erreichbarkeit.

Ein Gerät kann Ping beantworten, aber trotzdem keinen Webdienst bereitstellen.

Merksatz:

Ping erreichbar heißt nicht:
Anwendung funktioniert.

Wenn Ping nicht funktioniert

Wenn Ping nicht funktioniert, kann das viele Ursachen haben.

Mögliche Ursachen:

- Zielgerät ausgeschaltet
- falsche IP-Adresse
- falsche Subnetzmaske
- falsches Gateway
- fehlende Route
- Firewall blockiert ICMP
- ICMP am Ziel deaktiviert
- VLAN-Problem
- ARP-Problem
- Schicht-1-Problem
- Schicht-2-Problem

Wichtig:

Kein Ping bedeutet nicht automatisch,
dass das Ziel komplett unerreichbar ist.

Merksatz:

```
Ping-Fehler ist ein Hinweis,
aber noch keine eindeutige Ursache.
```

Ping und Firewall

Firewalls können ICMP blockieren.

Das bedeutet:

```
Ein Ziel kann erreichbar sein,
aber auf Ping nicht antworten.
```

Beispiel:

```
HTTPS funktioniert.
Ping funktioniert nicht.
```

Mögliche Erklärung:

```
TCP 443 ist erlaubt,
ICMP Echo ist blockiert.
```

Merksatz:

```
Geblockter Ping bedeutet nicht automatisch:
Ziel ist offline.
```

Ping und DNS unterscheiden

Wenn man einen Namen pingt, wird zuerst DNS benötigt.

Beispiel:

```
ping www.example.com
```

Vor dem eigentlichen Ping muss das System herausfinden:

```
Welche IP-Adresse gehört zu www.example.com?
```

Wenn DNS nicht funktioniert, kann der Ping auf den Namen scheitern.

Ein Ping auf die IP-Adresse kann trotzdem funktionieren.

Merksatz:

```
Ping auf Namen prüft auch DNS.
Ping auf IP prüft DNS nicht.
```

Beispiel: DNS oder Routing?

Fehlerbild:

```
ping 8.8.8.8 funktioniert.
ping www.example.com funktioniert nicht.
```

Wahrscheinliche Ursache:

```
DNS-Problem
```

Warum?

```
Die IP-Kommunikation ins Internet funktioniert grundsätzlich.
Aber der Name kann nicht aufgelöst werden.
```

Merksatz:

```
IP funktioniert,
Name nicht:
DNS prüfen.
```

Beispiel: Gateway prüfen

Ein sinnvoller erster Ping-Test im LAN ist oft das Standard-Gateway.

Beispiel:

```
Client:
192.168.10.20/24

Gateway:
192.168.10.1
```

Test:

```
ping 192.168.10.1
```

Wenn das Gateway nicht erreichbar ist, prüft man:

```
- IP-Adresse des Clients
- Subnetzmaske
- Gateway-Adresse
- VLAN
- ARP
- Switch-Port
- Link
```

Merksatz:

```
Gateway-Ping prüft die lokale Verbindung zum Router.
```

Beispiel: Internet-IP prüfen

Nach dem Gateway kann man eine externe IP-Adresse testen.

Beispiel:

```
ping 8.8.8.8
```

Wenn Gateway erreichbar ist, aber externe IP nicht, prüft man:

```
- Default Route
- Router
- Firewall
```

```
- NAT
- Provider-Verbindung
- Rückroute
- Internetanschluss
```

Merksatz:

```
Externe IP prüft Routing Richtung Internet,
aber nicht DNS.
```

Beispiel: Namen prüfen

Danach kann man einen Namen testen.

Beispiel:

```
ping www.example.com
```

Wenn externe IP erreichbar ist, aber Name nicht, prüft man:

```
- DNS-Server
- DNS-Konfiguration
- DNS-Erreichbarkeit
- Firewall-Regeln für DNS
- falsche Suchdomäne
- lokale Hosts-Datei
```

Merksatz:

```
Name funktioniert nicht:
DNS prüfen.
```

Ping-Reihenfolge bei Fehlersuche

Eine einfache Reihenfolge:

```
1. eigene IP-Konfiguration prüfen
2. eigenes Gateway pingen
3. anderes Gerät im gleichen Netz pingen
4. externe IP-Adresse pingen
5. DNS-Namen pingen
6. Dienst gezielt prüfen
```

Beispiel:

```
ping 192.168.10.1
ping 8.8.8.8
ping www.example.com
```

Merksatz:

```
Erst lokal,
dann extern,
dann Name.
```

Traceroute

Traceroute ist ein Werkzeug, um den Weg zu einem Ziel sichtbar zu machen.

Je nach Betriebssystem heißt der Befehl:

```
Windows:
tracert

Linux:
traceroute

Linux teilweise:
tracepath

macOS:
traceroute
```

Traceroute zeigt die Router auf dem Weg zum Ziel.

Merksatz:

```
Traceroute zeigt den Weg durch das IP-Netz.
```

Wofür nutzt man Traceroute?

Traceroute hilft bei Fragen wie:

```
Über welche Router läuft die Verbindung?
Wo stoppt die Verbindung?
Wie viele Hops gibt es?
Gibt es hohe Verzögerungen auf einem Abschnitt?
Gibt es Routing-Probleme?
Gibt es ungewöhnliche Wege?
```

Traceroute ist besonders hilfreich bei Problemen zwischen Netzen.

Merksatz:

```
Traceroute hilft bei der Routing-Fehlersuche.
```

Begriff: Hop

Ein Hop ist ein Schritt über einen Router.

Beispiel:

```
PC
→ Router 1
→ Router 2
→ Router 3
→ Ziel
```

Hier gibt es mehrere Hops.

Jeder Router auf dem Weg zählt als Hop.

Merksatz:

Hop = ein Router-Schritt auf dem Weg.

TTL

TTL steht für:

Time To Live

TTL ist ein Feld im IP-Paket.

Es begrenzt, wie lange ein Paket im Netz weitergeleitet werden darf.

Jeder Router verringert die TTL um 1.

Wenn TTL 0 erreicht, wird das Paket verworfen.

Merksatz:

TTL begrenzt die Lebensdauer eines IP-Pakets.

Warum ist TTL wichtig?

TTL verhindert, dass IP-Pakete endlos im Netz kreisen.

Das kann zum Beispiel bei einer Routing-Schleife passieren.

Ohne TTL könnten Pakete dauerhaft im Kreis laufen.

Mit TTL gilt:

Jeder Router verringert den Wert.
Bei 0 wird das Paket verworfen.

Merksatz:

TTL schützt vor endlosen Routing-Schleifen.

Traceroute und TTL

Traceroute nutzt das TTL-Verhalten aus.

Vereinfacht:

```
1. Erstes Paket wird mit TTL 1 gesendet.
2. Erster Router verringert TTL auf 0.
3. Erster Router verwirft das Paket.
4. Erster Router sendet eine ICMP-Time-Exceeded-Meldung zurück.
5. Traceroute kennt dadurch den ersten Router.
```

Dann:

```
Paket mit TTL 2
Paket mit TTL 3
Paket mit TTL 4
```

So wird Schritt für Schritt der Weg sichtbar.

Merksatz:

```
Traceroute findet Router,
indem TTL schrittweise erhöht wird.
```

ICMP Time Exceeded

Wenn TTL 0 erreicht, verwirft ein Router das Paket.

Oft sendet er dann eine ICMP-Meldung zurück.

Diese Meldung heißt:

```
Time Exceeded
```

Auf Deutsch sinngemäß:

```
Zeit überschritten
```

Traceroute nutzt diese Meldungen, um Router auf dem Weg zu erkennen.

Merksatz:

```
Time Exceeded zeigt:
TTL ist abgelaufen.
```

Traceroute-Ausgabe verstehen

Eine typische Traceroute-Ausgabe zeigt pro Zeile einen Hop.

Beispiel vereinfacht:

Hop	Gerät	Bedeutung
1	192.168.10.1	eigenes Gateway
2	Provider-Router	erster Router beim Provider
3	weiterer Router	Weg durchs Netz
4	Ziel	Ziel erreicht

Zusätzlich werden Antwortzeiten angezeigt.

Merksatz:

```
Jede Zeile bei Traceroute zeigt meist einen Router-Hop.
```

Sterne in Traceroute

In Traceroute-Ausgaben sieht man manchmal Sterne.

Beispiel:

```
* * *
```

Das bedeutet häufig:

```
keine Antwort auf diese Messung
```

Mögliche Ursachen:

```
- Router antwortet nicht auf ICMP
- Firewall blockiert
```

- Paket wurde verworfen
- Antwortweg funktioniert nicht
- Router priorisiert solche Antworten niedrig

Wichtig:

Sterne bedeuten nicht automatisch,
dass dort ein echter Ausfall ist.

Merksatz:

Sterne bei Traceroute können Blockierung oder fehlende Antwort bedeuten.

Hohe Zeiten in Traceroute

Hohe Antwortzeiten bei einem Hop können auf Verzögerung hinweisen.

Aber Vorsicht:

Router priorisieren Weiterleitung oft höher als Antworten an Traceroute.

Das bedeutet:

Ein Hop kann langsam antworten,
aber normalen Datenverkehr trotzdem schnell weiterleiten.

Wichtig ist besonders:

Steigen die Zeiten ab einem Hop dauerhaft?
Oder ist nur ein einzelner Hop auffällig?

Merksatz:

Traceroute-Zeiten immer vorsichtig interpretieren.

Traceroute und Firewall

Firewalls können Traceroute beeinflussen.

Mögliche Effekte:

```
- einzelne Hops antworten nicht
- Ziel antwortet nicht
- ICMP wird blockiert
- UDP-Traceroute wird blockiert
- Pfad wirkt unvollständig
```

Trotzdem kann die Anwendung funktionieren.

Merksatz:

```
Traceroute kann durch Firewalls unvollständig aussehen.
```

Traceroute ist nicht immer symmetrisch

Traceroute zeigt normalerweise den Hinweg aus Sicht des Absenders.

Der Rückweg kann anders verlaufen.

Das nennt man:

```
asymmetrisches Routing
```

Bei Internetverbindungen ist das nicht ungewöhnlich.

Merksatz:

```
Traceroute zeigt meist nur den Hinweg,
nicht sicher den Rückweg.
```

Pathping

Unter Windows gibt es zusätzlich:

```
pathping
```

Pathping kombiniert Eigenschaften von Ping und Traceroute.

Es zeigt den Weg und misst Paketverluste über längere Zeit.

Typischer Nutzen:

```
Paketverlust auf bestimmten Wegabschnitten erkennen
```

Merksatz:

```
Pathping kombiniert Weganzeige und Verlustmessung.
```

MTR

Unter Linux und macOS wird häufig MTR genutzt.

MTR kombiniert ebenfalls Ping und Traceroute.

Es zeigt laufend:

```
- Hops
- Antwortzeiten
- Paketverluste
- Schwankungen
```

MTR ist besonders hilfreich bei instabilen Netzwerkproblemen.

Merksatz:

```
MTR = laufende Traceroute- und Ping-Analyse.
```

ICMP Destination Unreachable

Destination Unreachable bedeutet:

```
Ziel nicht erreichbar
```

Das kann verschiedene Gründe haben.

Beispiele:

```
- Zielnetz nicht erreichbar
- Zielhost nicht erreichbar
- Protokoll nicht erreichbar
- Port nicht erreichbar
- Fragmentierung nötig, aber nicht möglich
```

Für AP1/AP2 reicht meist:

```
ICMP kann melden,
dass ein Ziel oder Weg nicht erreichbar ist.
```

Merksatz:

```
Destination Unreachable = Ziel oder Weg nicht erreichbar.
```

Paket zu groß und MTU

ICMP kann auch helfen, MTU-Probleme zu melden.

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

Das ist wichtig für:

```
Path MTU Discovery
```

Dabei wird herausgefunden, welche maximale Paketgröße auf dem Weg möglich ist.

Merksatz:

```
ICMP kann bei MTU-Problemen wichtige Hinweise liefern.
```

Path MTU Discovery

Path MTU Discovery versucht herauszufinden, wie groß Pakete auf dem gesamten Weg maximal sein dürfen.

Wenn ICMP-Meldungen blockiert werden, kann es zu schwer erkennbaren Problemen kommen.

Mögliche Symptome:

```
kleine Daten funktionieren
große Datenübertragungen hängen
Webseiten laden teilweise
VPN macht Probleme
```

Merksatz:

```
ICMP komplett zu blockieren kann MTU-Probleme verschleiern.
```

ICMPv4 und ICMPv6

IPv4 verwendet:

```
ICMPv4
```

IPv6 verwendet:

```
ICMPv6
```

ICMPv6 ist bei IPv6 besonders wichtig.

Warum?

```
IPv6 nutzt ICMPv6 unter anderem für Neighbor Discovery.
```

Wichtig:

```
ICMPv6 sollte nicht pauschal blockiert werden,
weil IPv6 sonst gestört werden kann.
```

Merksatz:

```
IPv6 braucht ICMPv6 für wichtige Grundfunktionen.
```

ICMP und Sicherheit

ICMP kann für Diagnose sehr nützlich sein.

Aber ICMP kann auch missbraucht werden.

Mögliche Risiken:

```
- Netzwerkerkundung
- Ping-Flood
- Informationsgewinn über erreichbare Systeme
- bestimmte Angriffsmuster
```

Deshalb blockieren oder begrenzen manche Firewalls ICMP.

Wichtig:

```
Nicht blind alles blockieren.
Sinnvoll filtern und begrenzen.
```

Merksatz:

```
ICMP ist nützlich,
sollte aber kontrolliert erlaubt werden.
```

Ping-Flood

Ein Ping-Flood ist ein Angriff oder Störungsszenario, bei dem sehr viele ICMP Echo Requests gesendet werden.

Ziel:

```
System oder Netzwerk überlasten
```

Schutzmaßnahmen:

```
- Rate Limiting
- Firewall-Regeln
- Monitoring
- DDoS-Schutz
- ICMP begrenzen
```

Merksatz:

```
Ping-Flood = viele ICMP-Anfragen zur Überlastung.
```

ICMP in der Fehlersuche

ICMP ist besonders hilfreich für:

```
- Erreichbarkeit prüfen
- Routing-Probleme erkennen
- TTL-Probleme verstehen
- Traceroute nutzen
- Paketverluste sehen
- Latenz messen
- MTU-Probleme erkennen
```

Aber:

```
ICMP-Ergebnisse müssen richtig interpretiert werden.
```

Merksatz:

```
ICMP ist Diagnosewerkzeug,
aber kein vollständiger Anwendungstest.
```

Systematische Prüfung mit Ping

Eine einfache Prüf-Reihenfolge:

```
1. eigene IP-Konfiguration prüfen
2. Loopback testen
3. eigene IP testen
4. Gateway testen
5. anderes Gerät im LAN testen
6. externe IP testen
7. DNS-Namen testen
8. Anwendung oder Dienst testen
```

Beispiele:

```
ping 127.0.0.1
ping eigene IP
ping Gateway
ping externe IP
ping DNS-Name
```

Merksatz:

```
Ping systematisch von nah nach fern einsetzen.
```

Loopback-Ping

Ein Ping auf die Loopback-Adresse prüft den lokalen IP-Stack.

IPv4-Loopback:

```
127.0.0.1
```

Beispiel:

```
ping 127.0.0.1
```

Wenn das funktioniert, arbeitet der lokale IP-Stack grundsätzlich.

Wenn es nicht funktioniert, liegt das Problem lokal am System.

Merksatz:

```
127.0.0.1 prüft das eigene System.
```

Eigene IP pingen

Nach dem Loopback kann man die eigene IP-Adresse testen.

Beispiel:

```
ping 192.168.10.20
```

Das prüft, ob die IP-Adresse am eigenen Adapter aktiv ist.

Wenn Loopback funktioniert, aber eigene IP nicht, prüft man:

```
- Netzwerkkarte
- IP-Konfiguration
- Adapterstatus
- Firewall
- Betriebssystem
```

Merksatz:

```
Eigene IP prüft lokale IP-Konfiguration am Adapter.
```

Gateway pingen

Danach prüft man das Standard-Gateway.

Beispiel:

```
ping 192.168.10.1
```

Wenn das Gateway nicht erreichbar ist, prüft man:

```
- Link
- VLAN
- ARP
- IP-Adresse
- Subnetzmaske
- Gateway-Adresse
- Switch-Port
- Router-Interface
```

Merksatz:

```
Gateway-Ping prüft lokale Netz- und Router-Erreichbarkeit.
```

Externe IP pingen

Wenn das Gateway erreichbar ist, kann man eine externe IP testen.

Beispiel:

```
ping 8.8.8.8
```

Wenn das nicht funktioniert, prüft man:

```
- Default Route
- NAT
- Firewall
- Provider
- Router
- Rückroute
- Internetverbindung
```

Merksatz:

```
Externe IP prüft Routing über das lokale Netz hinaus.
```

DNS-Namen pingen

Wenn externe IP funktioniert, aber ein Name nicht, liegt der Fehler häufig bei DNS.

Beispiel:

```
ping www.example.com
```

Mögliche Ursachen:

```
- falscher DNS-Server
- DNS-Server nicht erreichbar
- Firewall blockiert DNS
```

```
- falsche Suchdomäne
- lokale Namensauflösung fehlerhaft
```

Merksatz:

```
IP erreichbar,
Name nicht:
DNS prüfen.
```

Ping und Anwendungstest unterscheiden

Ping zeigt nicht, ob ein bestimmter Dienst funktioniert.

Beispiel:

```
ping server funktioniert
```

Aber:

```
Webseite lädt nicht.
```

Mögliche Ursachen:

```
- Webserver läuft nicht
- TCP-Port 80 oder 443 blockiert
- Zertifikatsproblem
- DNS zeigt auf falsche IP
- Reverse Proxy falsch
- Anwendung abgestürzt
```

Merksatz:

```
Ping prüft Erreichbarkeit,
nicht den Dienst.
```

Einordnung in das OSI-Modell

Thema	Schicht
Ethernet-Link	1
MAC-Adresse	2
VLAN	2
ARP	2 / 3-Bezug
IP-Adresse	3
Routing	3
ICMP	3
Ping	3
Traceroute	3
TTL	3
TCP-Port	4
DNS	7
HTTP / HTTPS	7

Merksatz:

> Ping und Traceroute prüfen vor allem Schicht 3.

Was ICMP nicht macht

ICMP macht nicht:

- TCP-Verbindung aufbauen
- UDP-Datenstrom verwalten
- Webseiten ausliefern
- DNS-Namen auflösen
- Benutzer authentifizieren
- Dateien übertragen
- Verschlüsselung bereitstellen

ICMP ist hauptsächlich für Kontroll- und Diagnosemeldungen im IP-Netz zuständig.

Merksatz:

ICMP ist Kontrolle und Diagnose,
nicht Anwendungstransport.

Typische IHK-Fragen

In AP1 und AP2 kann zum Beispiel gefragt werden:

- Was bedeutet ICMP?
- Wofür wird ICMP verwendet?
- Nutzt ICMP TCP- oder UDP-Ports?
- Was ist der Unterschied zwischen ICMP-Typ und Port?
- Was macht Ping?
- Was ist ein Echo Request?
- Was ist ein Echo Reply?
- Warum kann Ping blockiert sein?
- Was zeigt Traceroute?
- Was ist ein Hop?
- Was bedeutet TTL?
- Warum verhindert TTL endlose Routing-Schleifen?
- Wie nutzt Traceroute TTL?
- Was bedeutet Destination Unreachable?
- Warum ist ICMPv6 wichtig?

Typische Prüfungsfallen

ICMP ist nicht TCP.

ICMP ist nicht UDP.

ICMP nutzt keine TCP- oder UDP-Ports.

ICMP nutzt Typ und Code.

Ping nutzt typischerweise ICMP Echo Request und Echo Reply.

Ping-Erfolg bedeutet nicht,
dass eine Anwendung funktioniert.

Ping-Fehler bedeutet nicht automatisch,
dass ein Ziel offline ist.

Firewalls können ICMP blockieren.

Ping auf Namen prüft auch DNS.

Ping auf IP prüft DNS nicht.

Traceroute zeigt den Weg über Router.

TTL gehört zu IP auf Schicht 3.

TTL verhindert endloses Kreisen von IP-Paketen.

Sterne bei Traceroute bedeuten nicht automatisch Ausfall.

ICMPv6 ist für IPv6 besonders wichtig.

Wichtige Begriffe kurz erklärt

Begriff	Kurze Erklärung
ICMP	Internet Control Message Protocol
ICMPv4	ICMP für IPv4
ICMPv6	ICMP für IPv6
Echo Request	Ping-Anfrage
Echo Reply	Ping-Antwort
Destination Unreachable	Ziel oder Weg nicht erreichbar
Time Exceeded	TTL abgelaufen
Typ	Art der ICMP-Nachricht
Code	genauere Beschreibung der ICMP-Nachricht
Ping	Werkzeug zur Erreichbarkeitsprüfung
Traceroute	Werkzeug zur Wegverfolgung
tracert	Windows-Variante von Traceroute
Hop	Router-Schritt auf dem Weg

Begriff	Kurze Erklärung
TTL	Time To Live, Lebensdauerbegrenzung für IP-Pakete
Pathping	Windows-Werkzeug aus Ping und Traceroute
MTR	laufende Ping- und Traceroute-Analyse
Path MTU Discovery	Ermittlung der maximalen Paketgröße auf dem Weg
Ping-Flood	Überlastung durch viele ICMP-Anfragen

IHK-sichere Kurzformulierung

ICMP steht für Internet Control Message Protocol und gehört zum IP-Umfeld auf OSI-Schicht 3. Es wird für Kontroll- und Fehlermeldungen in IP-Netzen verwendet und nutzt keine TCP- oder UDP-Ports, sondern Typen und Codes. Ping verwendet typischerweise ICMP Echo Request und Echo Reply, um die grundlegende IP-Erreichbarkeit eines Ziels zu prüfen. Traceroute zeigt den Weg zu einem Ziel über mehrere Router und nutzt dabei das TTL-Verhalten von IP-Paketen. Ein erfolgreicher Ping beweist nicht, dass ein bestimmter Dienst funktioniert, und ein fehlgeschlagener Ping bedeutet nicht automatisch, dass das Ziel offline ist, da ICMP durch Firewalls blockiert werden kann.

Merksätze

ICMP = Internet Control Message Protocol.

ICMP gehört zum IP-Umfeld.

ICMP wird meist Schicht 3 zugeordnet.

ICMP ist nicht TCP.

ICMP ist nicht UDP.

ICMP nutzt keine Ports.

ICMP nutzt Typ und Code.

Ping nutzt Echo Request und Echo Reply.

Ping prüft IP-Erreichbarkeit.

Ping auf IP prüft kein DNS.

Ping auf Namen prüft auch DNS.

Ping-Erfolg heißt nicht:
Anwendung funktioniert.

Ping-Fehler heißt nicht automatisch:
Ziel offline.

Firewall kann ICMP blockieren.

Traceroute zeigt Router-Hops.

Hop = Router-Schritt.

TTL = Time To Live.

Jeder Router verringert TTL.

TTL 0 = Paket wird verworfen.

TTL verhindert Routing-Endlosschleifen.

Traceroute nutzt TTL.

Time Exceeded = TTL abgelaufen.

Sterne bei Traceroute vorsichtig interpretieren.

ICMPv6 ist für IPv6 wichtig.

ICMP ist Diagnose,
kein Anwendungstest.