19.6 TCP, UDP, ICMP und ARP Spickzettel

Dieser Spickzettel fasst vier wichtige Netzwerkprotokolle kompakt zusammen:

- TCP
- UDP
- ICMP
- ARP

Diese Protokolle tauchen häufig in Prüfungsaufgaben, Fehlersuche und Netzwerkanalyse auf.

Merksatz:

TCP und UDP transportieren Daten.
ICMP hilft bei Diagnose.
ARP findet MAC-Adressen im lokalen Netz.

Grundübersicht

Protokoll	Schicht	Hauptaufgabe
TCP	OSI-Schicht 4	zuverlässiger verbindungsorientierter Transport
UDP	OSI-Schicht 4	schneller verbindungsloser Transport
ICMP	OSI-Schicht 3	Kontroll- und Fehlermeldungen
ARP	zwischen Schicht 2 und 3	IPv4-Adresse zu MAC-Adresse auflösen

Merksatz:

TCP und UDP gehören zur Transportschicht.
ICMP gehört zur Netzwerkschicht.
ARP verbindet IPv4 und Ethernet im lokalen Netz.

TCP kurz erklärt

TCP steht für:

```
Transmission Control Protocol
```

Eigenschaften:

```
verbindungsorientiert
zuverlässig
bestätigt Daten
überträgt verlorene Daten erneut
stellt Reihenfolge sicher
nutzt Ports
hat mehr Overhead als UDP
```

Typische Anwendungen:

```
HTTPS
HTTP
SSH
SMTP
IMAP
POP3
SMB
RDP
```

Merksatz:

```
TCP = zuverlässig und verbindungsorientiert.
```

TCP-Verbindungsaufbau

TCP baut vor der Datenübertragung eine Verbindung auf.

Der Verbindungsaufbau heißt:

```
Three-Way Handshake
```

Ablauf:

```
1. SYN

2. SYN-ACK

3. ACK
```

Bedeutung:

```
Client möchte Verbindung aufbauen.
Server bestätigt und antwortet.
Client bestätigt endgültig.
```

Merksatz:

```
TCP startet mit SYN,
SYN-ACK,
ACK.
```

TCP-Zuverlässigkeit

TCP sorgt für zuverlässige Übertragung durch:

```
Sequenznummern
Bestätigungen
erneute Übertragung
Reihenfolgeprüfung
Fehlererkennung
Flusskontrolle
```

Merksatz:

```
TCP merkt,
ob Daten angekommen sind.
```

TCP-Ports

TCP nutzt Ports, um Daten einem Dienst oder Prozess zuzuordnen.

Beispiele:

Dienst	TCP-Port
SSH	22
HTTP	80
HTTPS	443
SMTP	25
IMAP	143
SMB	445
RDP	3389

Merksatz:

> TCP-Port zeigt den angesprochenen Dienst.

Typische TCP-Status

Status	Bedeutung
LISTEN	Dienst wartet auf eingehende Verbindungen
SYN_SENT	Client versucht Verbindung aufzubauen
SYN_RECEIVED	Server hat SYN erhalten und geantwortet
ESTABLISHED	Verbindung besteht
FIN_WAIT	Verbindung wird beendet
TIME_WAIT	Verbindung wurde beendet, Wartephase
CLOSE_WAIT	Gegenseite hat beendet, lokale Anwendung noch nicht

Merksatz:

> LISTEN heißt:
> Dienst wartet.
> ESTABLISHED heißt:
> Verbindung besteht.

TCP-Fehlerbilder

Fehlerbild	Mögliche Ursache

Verbindung kommt nicht zustande	Port blockiert, Dienst aus, Firewall
SYN_SENT bleibt stehen	Ziel antwortet nicht oder Firewall blockiert
Verbindung bricht ab	Timeout, Anwendung, Netzwerkproblem
Dienst lauscht nicht	Dienst nicht gestartet oder falsche Schnittstelle
viele Verbindungen offen	Last, Angriff oder Anwendung hängt

Merksatz:

```
TCP-Fehler betreffen oft Port,
Dienst,
Firewall
oder Verbindung.
```

UDP kurz erklärt

UDP steht für:

```
User Datagram Protocol
```

Eigenschaften:

```
verbindungslos
schnell
wenig Overhead
keine eingebaute Zustellgarantie
keine eingebaute Reihenfolgegarantie
keine erneute Übertragung durch UDP selbst
nutzt Ports
```

Typische Anwendungen:

```
DNS
DHCP
VoIP
Streaming
Gaming
NTP
```

SNMP

Merksatz:

UDP = schnell,
schlank
und verbindungslos.

Warum UDP verwendet wird

UDP wird verwendet, wenn geringe Verzögerung wichtiger ist als perfekte Zustellung.

Beispiele:

Sprache bei VoIP soll sofort ankommen.
Ein verlorenes Sprachpaket ist weniger schlimm als lange Verzögerung.

DNS-Anfragen sind klein und sollen schnell beantwortet werden.

Streaming kann einzelne Verluste oft besser verkraften als Verzögerung.

Merksatz:

UDP ist sinnvoll,
wenn Geschwindigkeit wichtiger ist als eingebaute Zuverlässigkeit.

UDP-Ports

Dienst	UDP-Port
DNS	53
DHCP Server	67
DHCP Client	68
NTP	123
SNMP	161
SNMP Trap	162

Merksatz:

UDP-Port zeigt ebenfalls den angesprochenen Dienst,
aber ohne TCP-Verbindungsaufbau.

UDP-Fehlerbilder

Fehlerbild	Mögliche Ursache
keine Antwort auf DNS	UDP 53 blockiert, DNS-Server falsch
DHCP funktioniert nicht	UDP 67/68, VLAN, DHCP-Relay
Zeit stimmt nicht	NTP UDP 123 blockiert oder Server falsch
SNMP liefert keine Werte	Community, Rechte, UDP 161, Firewall
VoIP abgehackt	Paketverlust, Jitter, Latenz

Merksatz:

UDP-Probleme erkennt man oft an fehlenden Antworten oder Qualitätseinbußen.

TCP und UDP vergleichen

Merkmal	TCP	UDP
Verbindung	verbindungsorientiert	verbindungslos
Aufbau	Three-Way Handshake	kein Verbindungsaufbau
Zuverlässigkeit	eingebaut	nicht eingebaut
Reihenfolge	wird gesichert	nicht garantiert
Overhead	höher	geringer
Geschwindigkeit	eher langsamer	eher schneller
Beispiele	HTTPS, SSH, SMTP	DNS, DHCP, VoIP

Merksatz:

TCP = zuverlässig.
UDP = wenig Overhead.

Wann TCP?

TCP eignet sich, wenn Daten vollständig und korrekt ankommen müssen.

Beispiele:

```
Webseite laden
Datei übertragen
E-Mail senden
Remotezugriff
Datenbankverbindung
Dateifreigabe
```

Merksatz:

```
TCP für vollständige und zuverlässige Übertragung.
```

Wann UDP?

UDP eignet sich, wenn Geschwindigkeit, geringe Verzögerung oder einfache Anfrage-Antwort-Kommunikation wichtig ist.

Beispiele:

```
DNS
DHCP
VoIP
Livestreaming
Online-Gaming
Zeitabgleich
```

Merksatz:

```
UDP für schnelle und zeitkritische Kommunikation.
```

ICMP kurz erklärt

ICMP steht für:

```
Internet Control Message Protocol
```

Aufgabe:

```
Kontroll-
Fehler-
und Diagnosemeldungen im IP-Netz
```

Typische Nutzung:

```
ping

traceroute

Fehlermeldungen bei nicht erreichbaren Zielen
```

Merksatz:

```
ICMP transportiert keine Anwendungsdaten,
sondern Kontrollinformationen.
```

ICMP und OSI-Schicht

ICMP gehört zur Netzwerkschicht.

OSI-Schicht:

```
Schicht 3
```

Grund:

```
ICMP arbeitet mit IP
und meldet Probleme bei IP-Kommunikation.
```

Merksatz:

```
ICMP gehört zu Schicht 3.
```

---

ping

ping nutzt ICMP Echo Request und Echo Reply.

Aufgabe:

```
Erreichbarkeit eines Ziels testen
```

Wichtig:

```
Ping prüft nicht,
ob ein bestimmter TCP- oder UDP-Dienst funktioniert.
```

Beispiel:

```
Ping funktioniert,
aber HTTPS auf TCP 443 ist blockiert.
```

Merksatz:

```
ping prüft ICMP-Erreichbarkeit,
nicht den Anwendungsdienst.
```

---

traceroute und tracert

traceroute oder tracert zeigen den Weg zum Ziel über Router.

Nutzung:

```
Pfad prüfen
Routingprobleme eingrenzen
Paketlaufzeit grob erkennen
Hops sichtbar machen
```

Wichtig:

```
Nicht jeder Router antwortet auf ICMP oder Traceroute.
Sternchen bedeuten nicht automatisch,
dass der gesamte Weg defekt ist.
```

Merksatz:

traceroute zeigt den Weg,

aber Ausgaben müssen interpretiert werden.

ICMP-Fehlerbilder

Fehlerbild	Mögliche Bedeutung
ping erfolgreich	Ziel antwortet auf ICMP
ping fehlgeschlagen	Ziel offline, ICMP blockiert, Routingproblem
hohe Antwortzeit	Latenz, Last oder lange Strecke
Paketverlust	Netzproblem, Überlastung oder Funkproblem
traceroute bricht ab	Firewall, Routing, ICMP-Filter
einzelne Hops antworten nicht	Router antwortet nicht auf ICMP, Weg kann trotzdem funktionieren

Merksatz:

Kein ping bedeutet nicht automatisch:

Ziel ist offline.

ICMP und Firewall

ICMP kann in Firewalls erlaubt oder blockiert werden.

Vorteil von ICMP erlauben:

bessere Diagnose

einfachere Fehlersuche

Grund für Einschränkung:

weniger Informationspreisgabe

Schutz gegen bestimmte Missbrauchsarten

Sicherheitsrichtlinie

Merksatz:

ICMP blockieren kann Fehlersuche erschweren.

ARP kurz erklärt

ARP steht für:

Address Resolution Protocol

Aufgabe:

IPv4-Adresse in MAC-Adresse auflösen

Einsatzbereich:

lokales Netzwerksegment

Beispiel:

Ein Client möchte das Gateway 192.168.1.1 erreichen.

Dafür braucht er die MAC-Adresse des Gateways.

Diese ermittelt er mit ARP.

Merksatz:

ARP findet die MAC-Adresse zu einer IPv4-Adresse im lokalen Netz.

Warum ARP nötig ist

IP-Adressen werden für logische Kommunikation genutzt.

Ethernet im lokalen Netz braucht aber MAC-Adressen.

Deshalb muss ein Host wissen:

Welche MAC-Adresse gehört zur Ziel-IP?

Für Ziele außerhalb des eigenen Netzes gilt:

```
Der Client ermittelt per ARP die MAC-Adresse des Gateways,
nicht die MAC-Adresse des entfernten Zielservers.
```

Merksatz:

```
Für entfernte Ziele wird lokal die MAC des Gateways benötigt.
```

ARP-Ablauf

Typischer Ablauf:

```
1. Host prüft:
   Liegt Ziel im eigenen Subnetz?

2. Wenn Ziel lokal ist:
   ARP fragt nach MAC-Adresse des Zielhosts.

3. Wenn Ziel extern ist:
   ARP fragt nach MAC-Adresse des Gateways.

4. Antwort wird in ARP-Tabelle gespeichert.
```

Merksatz:

```
ARP arbeitet nur im lokalen Netz.
```

ARP Request und ARP Reply

ARP Request:

```
Frage per Broadcast:

Wer hat diese IP-Adresse?
```

ARP Reply:

Antwort per Unicast:

Diese IP-Adresse gehört zu dieser MAC-Adresse.

Merksatz:

ARP Request ist Broadcast.
ARP Reply ist Antwort mit MAC-Adresse.

ARP-Tabelle

Die ARP-Tabelle speichert bekannte Zuordnungen.

Beispiel:

IPv4-Adresse

zu

MAC-Adresse

Vorteil:

nicht bei jedem Paket neu fragen

Problem:

falsche oder alte Einträge können Fehler verursachen.

Merksatz:

ARP-Tabelle ist der lokale Zwischenspeicher für IP-zu-MAC.

ARP und Gateway

Wenn ein Ziel nicht im eigenen Subnetz liegt, sendet der Client das Ethernet-Frame an die MAC-Adresse des Gateways.

Wichtig:

> IP-Ziel bleibt der entfernte Host.
>
> MAC-Ziel ist lokal das Gateway.

Merksatz:

> IP zeigt zum Endziel.
> MAC zeigt zum nächsten lokalen Hop.

ARP-Fehlerbilder

Fehlerbild	Mögliche Ursache
lokaler Host nicht erreichbar	ARP, VLAN, Switch, Firewall, Ziel aus
Gateway nicht erreichbar	falsches Gateway, ARP, VLAN, Router aus
doppelte IP-Adresse	ARP springt zwischen MAC-Adressen
falsche MAC-Zuordnung	ARP-Spoofing oder Cache-Problem
nur lokales Netz betroffen	Schicht 2 oder ARP prüfen

Merksatz:

> ARP-Probleme betreffen lokale IPv4-Kommunikation.

ARP-Spoofing

ARP-Spoofing ist ein Angriff, bei dem falsche ARP-Antworten gesendet werden.

Ziel:

> Datenverkehr umleiten
>
> Man-in-the-Middle ermöglichen
>
> Kommunikation stören

Schutzmaßnahmen:

Dynamic ARP Inspection
statische ARP-Einträge in Sonderfällen
Netzwerksegmentierung
Switch-Sicherheitsfunktionen
Verschlüsselung höherer Schichten
Monitoring

Merksatz:

ARP vertraut lokalen Antworten und kann missbraucht werden.

TCP, UDP, ICMP und ARP gemeinsam einordnen

Frage	Wahrscheinliches Thema
Ist der Dienst über Port erreichbar?	TCP oder UDP
Funktioniert Namensauflösung?	DNS über UDP/TCP 53
Funktioniert IP-Erreichbarkeit grob?	ICMP
Wie kommt IPv4 zur MAC-Adresse?	ARP
Warum geht ping, aber Webseite nicht?	ICMP geht, TCP 80/443 prüfen
Warum geht lokale Kommunikation nicht?	ARP, VLAN, Switch, IP
Warum geht Gateway nicht?	ARP, Gateway-IP, VLAN, Router

Merksatz:

Unterschiedliche Protokolle beantworten unterschiedliche Diagnosefragen.

Beispiel: Ping funktioniert, HTTPS nicht

Fehlerbild:

ping zum Server funktioniert.

Webseite über HTTPS funktioniert nicht.

Bedeutung:

```
ICMP-Erreichbarkeit ist vorhanden.
```

Mögliche Ursachen:

```
TCP 443 blockiert
Webserver läuft nicht
Zertifikatsproblem
Reverse Proxy fehlerhaft
Anwendung fehlerhaft
Firewall-Regel fehlt
```

Merksatz:

```
ping erfolgreich heißt nicht,
dass HTTPS funktioniert.
```

Beispiel: DNS funktioniert nicht

Fehlerbild:

```
Name wird nicht aufgelöst.
```

Mögliche Protokolle:

```
DNS über UDP 53

DNS über TCP 53
```

Mögliche Ursachen:

```
DNS-Server falsch
DNS-Server nicht erreichbar
Port 53 blockiert
falscher DNS-Eintrag
DNS-Cache
Split-DNS
```

Merksatz:

```
DNS-Probleme sind meist Schicht 7,
nutzen aber TCP oder UDP auf Schicht 4.
```

Beispiel: DHCP funktioniert nicht

Fehlerbild:

```
Client erhält 169.254.x.x.
```

Beteiligte Protokolle:

```
DHCP über UDP 67 und 68
```

Mögliche Ursachen:

```
DHCP-Server nicht erreichbar
falsches VLAN
DHCP-Relay fehlt
Scope erschöpft
Firewall blockiert
Netzwerkverbindung fehlerhaft
```

Merksatz:

```
DHCP-Fehler können durch Schicht 1,
2,
3
oder 7 verursacht werden.
```

Beispiel: lokales Ziel nicht erreichbar

Fehlerbild:

```
Client und Server sollen im gleichen Subnetz sein,
erreichen sich aber nicht.
```

Mögliche Prüfungen:

IP-Adresse
Subnetzmaske
VLAN
Switchport
ARP-Tabelle
lokale Firewall
doppelte IP-Adresse

Merksatz:

Im gleichen Subnetz sind ARP,
VLAN
und lokale Firewall besonders wichtig.

Beispiel: externes Ziel nicht erreichbar

Fehlerbild:

Ziel liegt außerhalb des eigenen Subnetzes.

Beteiligte Schritte:

Client prüft Zielnetz.
Client sendet an Gateway.
ARP ermittelt MAC-Adresse des Gateways.
Router leitet IP-Paket weiter.
NAT oder Firewall können beteiligt sein.

Merksatz:

Externe Kommunikation braucht Gateway und Routing.

Typische Werkzeuge

Werkzeug	Hilft bei

ping	ICMP-Erreichbarkeit
traceroute / tracert	Weg über Router
arp	ARP-Tabelle anzeigen
ip neigh	Nachbartabelle unter Linux
ipconfig /all	IP-Konfiguration Windows
ip addr	IP-Konfiguration Linux
netstat	Verbindungen und Ports
ss	Sockets und Ports unter Linux
nslookup	DNS prüfen
dig	DNS detailliert prüfen
tcpdump	Pakete mitschneiden
Wireshark	Pakete grafisch analysieren

Merksatz:

> Werkzeug passend zur vermuteten Schicht wählen.

Prüfungsfalle: ping falsch interpretieren

Ping kann fehlschlagen, obwohl der Dienst erreichbar ist.

Mögliche Gründe:

> ICMP blockiert
> Ziel antwortet nicht auf ping
> Firewall filtert ICMP

Ping kann funktionieren, obwohl der Dienst nicht erreichbar ist.

Mögliche Gründe:

> TCP-Port blockiert
> Anwendung läuft nicht
> TLS-Problem
> Rechteproblem

Merksatz:

ping ist Diagnose,
aber kein vollständiger Funktionstest.

Prüfungsfalle: ARP nur im lokalen Netz

ARP funktioniert nicht über Router hinweg.

Für entfernte Ziele wird nicht die MAC-Adresse des Zielservers gesucht, sondern die MAC-Adresse des Gateways.

Merksatz:

ARP kennt nur lokale Nachbarn.

Prüfungsfalle: TCP und UDP nicht vermischen

TCP 53 und UDP 53 sind unterschiedliche Regeln.

TCP 443 und UDP 443 sind nicht automatisch dasselbe.

Eine Firewall-Regel muss das richtige Transportprotokoll erlauben.

Merksatz:

Portnummer ohne TCP oder UDP ist unvollständig.

Prüfungsfalle: UDP ist nicht automatisch unsicher

UDP hat keine eingebaute Zustellgarantie.

Das bedeutet aber nicht automatisch, dass UDP „schlecht“ oder „unsicher“ ist.

Es ist für bestimmte Anwendungen sinnvoll, zum Beispiel DNS, DHCP, VoIP oder NTP.

Merksatz:

UDP ist nicht schlechter,
sondern für andere Anforderungen gebaut.

Typische IHK-Fragen

In AP1 und AP2 kann zum Beispiel gefragt werden:

- Was ist TCP?
- Was ist UDP?
- Vergleichen Sie TCP und UDP.
- Was ist der TCP Three-Way Handshake?
- Warum nutzt DNS häufig UDP?
- Warum eignet sich UDP für VoIP?
- Was macht ICMP?
- Wofür wird ping verwendet?
- Warum ersetzt ping keinen Diensttest?
- Was zeigt traceroute?
- Was macht ARP?
- Warum wird bei externen Zielen die MAC-Adresse des Gateways benötigt?
- Was ist ARP-Spoofing?
- Warum muss man bei Firewall-Regeln TCP und UDP unterscheiden?

IHK-sichere Kurzformulierung

TCP und UDP sind Transportprotokolle der OSI-Schicht 4. TCP ist verbindungsorientiert und zuverlässig. Es nutzt einen Verbindungsaufbau, Bestätigungen und erneute Übertragung verlorener Daten. UDP ist verbindungslos, schlank und hat keine eingebaute Zustellgarantie. Es eignet sich für schnelle oder zeitkritische Kommunikation wie DNS, DHCP, VoIP oder NTP. ICMP arbeitet auf Schicht 3 und dient Kontroll- und Diagnosemeldungen, zum Beispiel bei ping oder traceroute. ARP löst im lokalen IPv4-Netz eine IP-Adresse in eine MAC-Adresse auf. Für Ziele außerhalb des eigenen Subnetzes wird per ARP die MAC-Adresse des Gateways ermittelt.

Merksätze

TCP ist zuverlässig.

TCP ist verbindungsorientiert.

TCP nutzt Ports.

TCP startet mit SYN,
SYN-ACK,
ACK.

UDP ist verbindungslos.

UDP ist schnell und schlank.

UDP hat keine eingebaute Zustellgarantie.

UDP nutzt ebenfalls Ports.

TCP und UDP gehören zu Schicht 4.

ICMP gehört zu Schicht 3.

ICMP dient Diagnose und Fehlermeldungen.

ping nutzt ICMP.

ping ist kein vollständiger Diensttest.

traceroute zeigt den Weg über Router.

Nicht jeder Hop muss antworten.

ARP löst IPv4 zu MAC auf.

ARP arbeitet lokal.

ARP Request ist Broadcast.

ARP Reply liefert die MAC-Adresse.

ARP-Tabelle speichert Zuordnungen.

Für externe Ziele wird die MAC des Gateways genutzt.

IP zeigt zum Endziel.

MAC zeigt zum nächsten lokalen Hop.

ARP-Spoofing kann Verkehr umleiten.

TCP 53 und UDP 53 getrennt beachten.

Portnummer immer mit TCP oder UDP nennen.

Host erreichbar heißt nicht Dienst erreichbar.

ICMP blockiert heißt nicht automatisch Ziel offline.

UDP ist nicht schlechter,
sondern für andere Anforderungen gebaut.