zurück

Ports & Protokolle – Grundlagen

Ports und Protokolle gehören zu den wichtigsten Grundlagen der Netzwerktechnik. Jeder Netzwerkdienst – egal ob Webserver, Mailserver oder DNS – nutzt bestimmte Ports und Protokolle, um Daten zu senden oder zu empfangen.

Was ist ein Port?

Ein Port ist eine **logische Tür** in einem System, über die eine Anwendung Daten empfängt oder versendet.
Vergleich:

- IP-Adresse = Straßenadresse
- Port = Wohnungstür

Arten von Ports

Es gibt drei Portbereiche:

- **0–1023**: Well-Known Ports (standardisierte Dienste)
- **1024–49151**: Registered Ports (für spezifische Anwendungen)
- **49152–65535**: Dynamische/ephemere Ports (z. B. Client-Verbindungen)

TCP und UDP

Ports können mit zwei Transportprotokollen verwendet werden:

- **TCP** – verbindungsorientiert
  - zuverlässige Übertragung
  - Fehlerkorrektur
  - geordnete Pakete
  - Beispiel: Web, Mail, SSH

- **UDP** – verbindungslos
  - schnell
  - keine Bestätigung
  - Beispiel: DNS, VoIP, Streaming

Wichtige Standardports

Web & Sicherheit

- **80/TCP** – HTTP
- **443/TCP** – HTTPS
- **8080/TCP** – HTTP Proxy
- **8443/TCP** – Alternativer HTTPS-Port

DNS

- **53/UDP** – Standardanfragen
- **53/TCP** – Zonentransfers

Mail

- **25/TCP** – SMTP
- **465/TCP** – SMTPs (alt)
- **587/TCP** – Submission (empfohlen)
- **110/TCP** – POP3
- **995/TCP** – POP3s
- **143/TCP** – IMAP
- **993/TCP** – IMAPs

Fernzugriff

- **22/TCP** – SSH
- **23/TCP** – Telnet (unsicher)
- **3389/TCP** – RDP

Dateiübertragung

- **20/21 TCP** – FTP
- **22/TCP** – SFTP (über SSH)
- **445/TCP** – SMB/CIFS
- **2049/TCP/UDP** – NFS

Netzwerkdienste

- **67/UDP** – DHCP Server
- **68/UDP** – DHCP Client
- **161/UDP** – SNMP
- **162/UDP** – SNMP Trap
- **69/UDP** – TFTP

VPN

- **500/UDP** – IKE
- **4500/UDP** – IPsec NAT-T
- **1194/UDP** – OpenVPN
- **51820/UDP** – WireGuard

Ports im Client-Verkehr

Ein Client nutzt für ausgehende Verbindungen dynamische Ports:

Beispiel:

- Browser → Port 443/TCP (Server)
- Client → zufälliger Port (z. B. 53425)

Darstellung:

```
Client: 192.168.1.20:53425  →  Server: 172.16.10.5:443
```

ASCII-Diagramm: Ports & Verbindungen

```
+---------------------+        +-------------------------+
|    Client           | 443    |         Server          |
|  192.168.1.20       |------->|    172.16.10.5          |
|  Port 53425         |        |    Port 443 (HTTPS)     |
+---------------------+        +-------------------------+
```

Protokolle und ihre Aufgaben

Layer 4 – Transport

- TCP – Zuverlässige Übertragung
  * UDP – Schnelle Übertragung

Layer 7 – Anwendung

- HTTP/HTTPS – Webseiten
  * DNS – Namensauflösung
  * SMTP/IMAP/POP3 – E-Mail
  * DHCP – automatische IP-Vergabe
  * SSH – sichere Verbindung
  * SMB – Windows-Freigaben

Wie Ports in Firewalls verwendet werden

Beispiel: Port 22 blockiert?
→ Kein SSH-Zugriff

Beispiel: Port 53 blockiert?
→ Keine DNS-Auflösung → kein Internet

Häufige Prüfungs- und Praxisfragen

- Warum nutzt DNS Port 53 UDP **und** TCP?
    - Welche Ports müssen offen sein für einen Mailserver?
      * Was passiert, wenn Port 80 zu ist?
      * Warum nutzt HTTPS Port 443?
      * Welcher Port für DHCP?

Zusammenfassung

- Ports sind logische Türen für Anwendungen
    - TCP und UDP bestimmen, wie Daten übertragen werden
      * Standardports sind festgelegt (0–1023)
      * Ports sind essentiell für Firewalls, Routing und Troubleshooting
      * Jede Anwendung nutzt bestimmte Ports → daher wichtig für IHK & Praxis