

OSI-Modell (Open Systems Interconnection)

Das OSI-Referenzmodell beschreibt die standardisierte Kommunikation in Netzwerken in 7 Schichten. Jede Schicht hat klar abgegrenzte Aufgaben und dient der Kapselung von Funktionen.

Kurzüberblick

| Ebene | Name (de/en) | Kernaufgaben | Typische Protokolle/Beispiele |
|-------|----------------------------|---|---|
| 7 | Anwendung / Application | Netzwerkdienste für Apps, Benutzeroberfläche | HTTP(S), SMTP/IMAP/POP3, FTP, DNS, DHCP-Client, SNMP-Manager, NTP |
| 6 | Darstellung / Presentation | Syntax/Format der Daten, Verschlüsselung/Kompression | TLS/SSL, ASCII/UTF-8, JPEG/PNG, MPEG |
| 5 | Sitzung / Session | Dialogsteuerung, Sitzungsauf-/abbau, Checkpoints | NetBIOS, RPC, (Sitzungs-Logik vieler Frameworks) |
| 4 | Transport / Transport | Ende-zu-Ende-Transport, Segmentierung, Fluss- & Fehlerkontrolle | TCP, UDP, SCTP, QUIC* |
| 3 | Vermittlung / Network | Logische Adressierung, Routing, Fragmentierung | IP (v4/v6), ICMP/ICMPv6, OSPF, BGP, IPsec (Tunnel/Transport) |
| 2 | Sicherung / Data Link | Frames, MAC-Adressen, Fehlererkennung, Medienzugriff | Ethernet (802.3), WLAN (802.11), ARP*, VLAN (802.1Q), PPP |
| 1 | Bitübertragung / Physical | Bits, elektrische/optische Signale, Stecker, Frequenzen | Kabel (Twisted Pair, LWL), Steckertypen, Modulation, Repeater |

Hinweise:

ARP arbeitet funktional zwischen L2/L3 (oft "Layer 2.5") und wird in der Praxis L2 zugeordnet (MAC-Auflösung zu IP).

QUIC läuft über UDP (L4) und implementiert transportähnliche Funktionen in der Anwendungsschicht (TCP/IP-Sicht). In OSI-Zuordnungen variiert die Darstellung.

Eselsbrücken

Von oben nach unten:

Alle Priester Sehen Tote Nackte Dicke Pferde

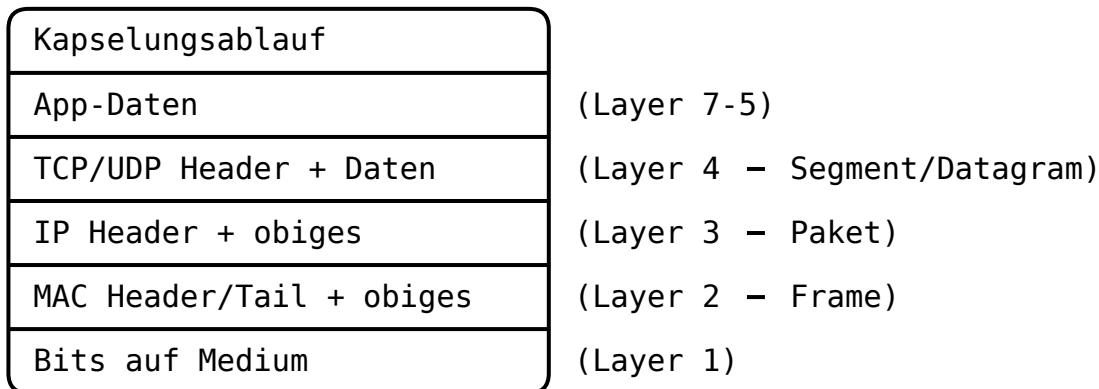
(Anwendung – Darstellung – Sitzung – Transport – Netzwerk – Sicherung – Physik)

Von unten nach oben:

Please Do Not Throw Sausage Pizza Away

PDU-Namen & Kapselung

| OSI-Schicht | PDU-Name |
|-------------|--------------------------------|
| 7-5 | Daten/Nutzdaten |
| 4 | Segment (TCP) / Datagram (UDP) |
| 3 | Paket (IP-Packet) |
| 2 | Frame |
| 1 | Bitstrom |



Geräte & typische Aufgaben je Schicht

| Schicht | Typische Geräte | Kernaufgaben im Betrieb |
|---------|----------------------------------|---|
| 1 | Repeater, Medienkonverter | Signalverstärkung/-anpassung |
| 2 | Switch, Bridge, WLAN-AP | MAC-Lernen/Forwarding, VLAN-Tagging (802.1Q), STP |
| 3 | Router, L3-Switch | Routing, Subnetting, NAT, QoS-Markierung (DSCP) |
| 4 | L4-Load-Balancer, Firewalls | Port-basiertes Filtern, Session-Tracking |
| 5-7 | Proxy, L7-Firewall/WAF, Gateways | DPI, TLS-Term., Caching, AuthN/AuthZ, App-Protokoll-Logik |

OSI vs. TCP/IP-Modell

| TCP/IP-Ebene | Entspricht OSI | Beispiele |
|--------------|----------------|--------------------------|
| Anwendung | 5-7 | HTTP(S), DNS, SMTP, TLS |
| Transport | 4 | TCP, UDP, QUIC(über UDP) |
| Internet | 3 | IP, ICMP, OSPF/BGP |
| Netz-Zugang | 1-2 | Ethernet, WLAN, ARP, PPP |

Praxis-Mapping (häufige Protokolle)

| Protokoll | OSI | Bemerkung |
|------------|--|--|
| HTTP/HTTPS | 7 (mit TLS=6) | Web, APIs; Ports 80/443 |
| DNS | 7 (Transp. via UDP/TCP-4) | Namensauflösung; 53 / UDP / TCP |
| DHCPv4/v6 | 7 (Nachrichten), 2/3 für Transport/Relay | Zuweisung IP/Optionen; Broadcast/Multicast |
| TLS/SSL | 6 | Verschlüsselung, Zertifikate |

| Protokoll | OSI | Bemerkung |
|-------------|--------------------------|--|
| SSH | 7/6/4 | Remote-Shell (22/TCP), verschlüsselt |
| ICMP/ICMPv6 | 3 | Ping/Traceroute, Fehlermeldungen |
| OSPF/BGP | 3 | Routingprotokolle |
| ARP/NDP | 2.5 / 3 | Auflösung IP→MAC (ARP), Nachbarschaft (NDP/ICMPv6) |
| IPsec | 3 (mit Kryptofunktionen) | AH/ESP, Tunnel/Transport |

VLAN, Subnetze & Tagging (L2/L3)

VLAN (802.1Q): L2-Segmentierung per Tag (VLAN-ID). Switch weist Ports VLANs zu (Access/Trunk).

Subnetz: L3-Segmentierung per IP-Netz (Maske/Prefix). Router verbindet Subnetze.

Inter-VLAN-Routing: L3-Switch/Router routet zwischen VLAN-Interfaces (SVIs).

QoS-Markierung: L2 (PCP-Bits), L3 (DSCP) – je nach Technik.

Trunk (802.1Q) ————— Access | SW1 |—————| SW2 | Access VLAN 10 | fa1/1 |—[VLAN10] [VLAN10]—| fa1/2 |—[VLAN20] [VLAN20]—| fa3/6 (SVI L3-Routing optional auf SW/Router)

Häufige Prüfungsfallen

ARP ist kein L3-Routingprotokoll → ARP wird praktisch L2 zugeordnet (MAC-Auflösung).

Ports ≠ Layer 3! → Ports sind L4 (TCP/UDP).

Switch ≠ Router → Switch = L2 (MAC/Frames), Router = L3 (IP/Packets).

TLS ist Schicht 6, nicht 7 (rein OSI-Lehre; in TCP/IP sitzt es "in" der Anwendung).

Ping (ICMP) ist L3 – Firewalls können ICMP separat filtern.

VLAN ≠ Subnetz – oft zusammen geplant, technisch jedoch L2 vs. L3.

Troubleshooting nach Schichten (Werkzeuge)

| Ebene | Typische Checks | Tools/Kommandos |
|-------|----------------------------------|--|
| 1 | Link/Signal, Kabel, Stecker | Link-LED, ethtool, Loopback-Plug |
| 2 | MAC-Tabellen, VLAN, Duplex | show mac address-table, ip link, iw, tcpdump -e |
| 3 | IP/Route, Gateway, MTU | ip addr/route, ping, traceroute, mtr |
| 4 | Ports/Sessions, Retransmits | ss -Intup, netstat, tcpdump port 443 |
| 5-7 | TLS-Handshake, HTTP-Status, Auth | openssl s_client, curl -v, Browser-DevTools, wireshark |

MTU, Fragmentierung & Path MTU Discovery (PMTUD)

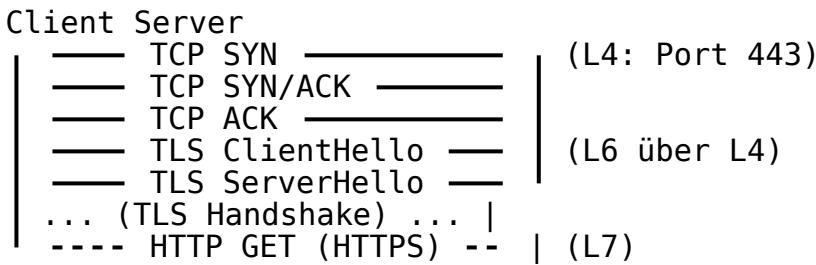
MTU (z. B. Ethernet 1500) begrenzt L2-Frame-Nutzlast → große L3-Pakete werden fragmentiert (IPv4) oder verworfen (IPv6 + "Packet Too Big").

PMTUD bestimmt maximal übertragbare Größe auf dem Pfad.

Symptome bei MTU-Problemen: Hänger bei TLS-Handshake, VPN-Tunnels, nur kleine Pings funktionieren.

[Host A] — (1500) — [Router] — (1400) — [VPN] — (1280) — [Host B] PMTUD meldet "Too Big" — MSS-Reduktion/Fragmentierung

OSI in der Praxis: Handshake-Beispiel (TLS über TCP)



Prüfungs-Quick-Check (Fragen & Kurzantworten)

- **Auf welcher Schicht arbeitet ein Switch?**
 - → L2 (MAC/Frames), L3-Switch zusätzlich L3.
- **Wofür ist ARP zuständig?**
 - → Zuordnung IP → MAC im lokalen Netz (Broadcast ARP-Request).
- **Wo liegen Ports?**
 - → L4 (TCP/UDP).
- **Was kapselt was?**
 - → Daten → Segment/Datagram → Paket → Frame → Bits.
- **Unterschied VLAN/Subnetz?**
 - → L2-Tagging vs. L3-Adressraum/Routing.
- **Welche Schicht prüft Routingtabellen?**
 - → L3.
- **Welche Schicht verschlüsselt (OSI-Lehre)?**
 - → L6 (z. B. TLS).

Protokoll-Cheat-Sheet (Ports)

| Dienst | Port/Proto | OSI-Sicht |
|-----------------|---------------------------|------------------------------------|
| HTTP/HTTPS | 80/443 TCP | 7 (TLS=6) über 4 |
| DNS | 53 UDP/TCP | 7 über 4 |
| SMTP/Submission | 25/587 TCP | 7 über 4 |
| IMAP(S) | 143/993 TCP | 7 (TLS=6) über 4 |
| SSH | 22 TCP | 7/6/4 |
| NTP | 123 UDP | 7 über 4 |
| DHCPv4 | 67/68 UDP (Server/Client) | 7 Nachrichten, Broadcast auf L2/L3 |

| Dienst | Port/Proto | OSI-Sicht |
|--------|------------------------|-----------|
| SNMP | 161/162 UDP (Get/Trap) | 7 über 4 |

Zusammenfassung als Schichten-Stack (A2S)



Merksätze zum Mitnehmen

“MAC lokal, IP global, Port spricht die App”

“VLAN trennt L2, Subnetz trennt L3”

“TLS schützt Inhalte, nicht die IP-Header”

From:
<http://wiki.nctl.de/dokuwiki/> - □ **Veni. Vidi. sudo rm -rf / vici.**

Permanent link:
<http://wiki.nctl.de/dokuwiki/doku.php?id=it-themen:allgemein:osi-referenzmodell&rev=1759910154>

Last update: **08.10.2025 09:55**

