

Netzwerkgrundlagen Layer 1 und Layer 2

Ausgangslage

In diesem Modul erarbeitet ihr euch die wichtigsten Grundlagen der Netzwerktechnik auf OSI Layer 1 und OSI Layer 2. Zuerst untersucht ihr, wie Daten physikalisch übertragen werden. Danach betrachtet ihr, wie Switches Ethernet-Frames weiterleiten, wie VLANs Netze trennen und wie einfache Netzwerkfehler eingegrenzt werden.

Das Modul verbindet Theorie, Praxis, Dokumentation und kurze Präsentationen. Ziel ist nicht, möglichst viele Begriffe auswendig zu lernen. Ziel ist, dass ihr Netzwerke beobachten, erklären, aufbauen und bei einfachen Fehlern sinnvoll prüfen könnt.

Layer 1

Layer 1 ist die physikalische Schicht des OSI-Modells. Sie beschreibt, wie Bits als elektrische, optische oder drahtlose Signale übertragen werden.

Typische Themen auf Layer 1 sind:

- Kabel und Stecker
- Signalübertragung
- Dämpfung und Störungen
- Kupferverkabelung mit Twisted Pair und RJ45
- Glasfaser mit Singlemode und Multimode
- einfache Messungen mit Kabeltester oder Messgerät

Layer 1 entscheidet, ob überhaupt eine brauchbare Verbindung besteht. Wenn ein Kabel defekt ist, ein Stecker falsch aufgelegt wurde oder ein Signal zu stark gedämpft wird, können höhere Schichten nicht zuverlässig arbeiten.

Kupferverkabelung

In lokalen Netzwerken werden häufig Twisted-Pair-Kabel eingesetzt. Die Adern sind paarweise verdreht, damit elektromagnetische Störungen reduziert werden. Typische Kategorien sind Cat5e, Cat6 und Cat6a.

Wichtige Begriffe:

- RJ45: üblicher Netzwerkstecker für Ethernet über Kupfer
- UTP: ungeschirmtes Twisted-Pair-Kabel
- STP oder S/FTP: geschirmte Varianten
- PoE: Stromversorgung über Netzkabel
- Dämpfung: Abschwächung des Signals über die Leitung
- NEXT: Übersprechen zwischen Adernpaaren am nahen Ende

Kupfer eignet sich besonders für kurze Strecken im Gebäude, zum Beispiel vom Arbeitsplatz zum Switch. Ethernet über Twisted Pair ist in der Regel auf 100 Meter pro Strecke begrenzt.

Glasfaser

Glasfaser überträgt Daten mit Licht. Dadurch ist sie unempfindlich gegen elektromagnetische Störungen und eignet sich für hohe Datenraten sowie längere Distanzen.

Wichtige Begriffe:

- Singlemode: kleine Kernstärke, sehr lange Distanzen

- Multimode: grössere Kernstärke, häufig für kürzere Gebäudestrecken
- LC, SC, ST: typische Steckerarten
- SFP: Transceiver-Modul für Switches
- OTDR: Messgerät zur Analyse von Glasfaserstrecken
- Spleissen: dauerhaftes Verbinden von Glasfasern

Glasfaser wird häufig für Backbones, Etagen-Uplinks, Verbindungen zwischen Gebäuden und Rechenzentren eingesetzt.

Layer 2

Layer 2 ist die Sicherungsschicht. In Ethernet-Netzen arbeitet hier der Switch. Er leitet Frames anhand von MAC-Adressen weiter.

Wichtige Begriffe:

- MAC-Adresse: eindeutige Hardwareadresse einer Netzwerkschnittstelle
- MAC-Adress-Tabelle: Tabelle des Switches mit MAC-Adresse, Port und VLAN
- Learning: der Switch lernt die Quell-MAC-Adresse eines Frames
- Forwarding: gezieltes Weiterleiten an den bekannten Zielport
- Flooding: Weiterleiten an mehrere Ports, wenn das Ziel unbekannt ist
- Broadcast: Nachricht an alle Geräte in einer Broadcast-Domäne

Ein Switch lernt aus eingehenden Frames, welche MAC-Adresse an welchem Port erreichbar ist. Dadurch kann er Frames gezielt weiterleiten.

VLANs und Trunks

VLANs teilen ein physisches Switch-Netz in getrennte logische Netze auf. Dadurch entstehen getrennte Broadcast-Domänen.

Wichtige Begriffe:

- VLAN: virtuelles LAN
- Access Port: Port für ein Endgerät in genau einem VLAN
- Trunk Port: Verbindung, die mehrere VLANs transportieren kann
- 802.1Q: Standard für VLAN-Tagging
- allowed VLANs: VLANs, die über einen Trunk erlaubt sind
- Native VLAN: VLAN ohne Tag auf einem 802.1Q-Trunk

Access Ports werden typischerweise für Clients, Drucker oder Telefone verwendet. Trunk Ports werden häufig zwischen Switches oder zu virtualisierten Plattformen eingesetzt.

ARP und Fehlersuche

ARP verbindet IP-Adressen mit MAC-Adressen. Ein Gerät, das eine IP-Adresse im gleichen lokalen Netz erreichen will, muss die passende MAC-Adresse kennen. Dafür sendet es eine ARP-Anfrage.

Bei einfacher Fehlersuche helfen strukturierte Prüfschritte:

1. Ist die physikalische Verbindung vorhanden?
2. Ist der Port aktiv?
3. Ist das richtige VLAN zugewiesen?
4. Lernt der Switch die MAC-Adresse?
5. Funktioniert ping?
6. Gibt es passende ARP-Einträge?

7. Stimmen Trunk und erlaubte VLANs?

Die wichtigsten Diagnosebefehle in diesem Modul sind:

```
show mac address-table
show vlan
show interfaces trunk
show arp
ping
arp -a
ipconfig /all
ip addr
```

Abgaben

Am Ende des Moduls gebt ihr eine Lerndokumentation ab. Sie enthält:

- Einführungsnotizen zu OSI Layer 1 und Layer 2
- Kabelübersicht
- Vergleich Kupfer und Glasfaser
- Mess- oder Beobachtungsprotokoll
- Unterlagen zur Layer-1-Präsentation
- Dokumentation zu Switching und MAC-Adressen
- VLAN- und Trunk-Dokumentation
- ARP- und Troubleshooting-Beispiel
- Schlussreflexion

Die Dokumentation soll in eigenen Worten geschrieben sein. Screenshots, Skizzen, Topologien und Tabellen sind erwünscht, wenn sie den Inhalt verständlicher machen.