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 logisch trennen und wie einfache Netzwerkfehler systematisch eingegrenzt werden können.

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. Dazu gehört auch, technische Inhalte in eigenen Worten festzuhalten und verständlich darzustellen.

Lernziele des Moduls

Nach Abschluss des Moduls könnt ihr:

- die Aufgaben von OSI Layer 1 und Layer 2 in einfachen Worten erklären
- wichtige Übertragungsmedien unterscheiden und ihren Einsatz begründen
- grundlegende Begriffe zu Kupferverkabelung und Glasfaser korrekt verwenden
- erklären, wie ein Switch Frames anhand von MAC-Adressen weiterleitet
- VLANs, Access Ports und Trunk Ports grundlegend einordnen
- den ARP-Prozess einfach und fachlich korrekt beschreiben
- einfache Netzwerkfehler schrittweise untersuchen
- Beobachtungen, Skizzen und Ergebnisse sauber dokumentieren
- technische Inhalte in einer kurzen Präsentation verständlich aufbereiten

Arbeitsweise im Modul

Im Modul arbeitet ihr mit verschiedenen Formen:

- Fachtext lesen und zusammenfassen
- Begriffe ordnen und vergleichen
- Tabellen ausfüllen
- Skizzen und einfache Topologien erstellen
- Beobachtungen im Lab oder in einer Simulation festhalten
- Ergebnisse in eigenen Worten dokumentieren
- kurze Präsentationen vorbereiten und durchführen

Die Kombination aus Theorie und Praxis ist wichtig. Viele Netzwerkprobleme werden erst wirklich verständlich, wenn man Geräte, Kabel, Ports oder Konsolenausgaben selbst gesehen hat.

Layer 1

Layer 1 ist die physikalische Schicht des OSI-Modells. Sie beschreibt, wie Bits als elektrische, optische oder drahtlose Signale übertragen werden. Auf dieser Schicht geht es nicht um IP-Adressen oder MAC-Adressen, sondern um die grundlegende Übertragung von Signalen.

Typische Themen auf Layer 1 sind:

- Kabel und Stecker
- Signalübertragung
- Dämpfung und Störungen

- Kupferverkabelung mit Twisted Pair und RJ45
- Glasfaser mit Singlemode und Multimode
- Link, Portstatus und physikalische Verbindung
- 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. Darum beginnt Fehlersuche in der Praxis oft zuerst bei den einfachsten Punkten auf Layer 1.

Typische Fragen zu Layer 1

- Ist das Kabel richtig eingesteckt?
- Ist der Port aktiv?
- Leuchtet die Link-LED?
- Ist ein Kabel beschädigt oder geknickt?
- Passt das verwendete Medium zur Verbindung?
- Ist die Strecke zu lang oder zu störungsanfällig?

Kupferverkabelung

In lokalen Netzwerken werden häufig Twisted-Pair-Kabel eingesetzt. Die Adern sind paarweise verdrillt, 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
- `FTP`, `STP`, `S/FTP`: geschirmte Varianten
- `PoE`: Stromversorgung über das Netzwerkkabel
- `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.

Wichtige Hinweise zu Kupfer

- Verdrillte Adernpaare helfen, Störungen zu reduzieren.
- Geschirmte Kabel können in störungsreichen Umgebungen sinnvoll sein.
- Schlechte Stecker, zu enge Biegeradien oder beschädigte Kabel können Probleme verursachen.
- PoE ist praktisch, weil Endgeräte wie Access Points oder IP-Telefone über das Netzwerkkabel mit Strom versorgt werden können.

Typische Einsatzorte von Kupfer

- Arbeitsplatzanschlüsse
- Drucker und VoIP-Telefone
- Access Points
- Verbindungen innerhalb eines Raums oder Büros
- Patchfelder und Netzwerkdosen im Gebäude

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, geeignet für sehr lange Distanzen
- `Multimode`: grössere Kernstärke, häufig für kürzere Strecken im Gebäude oder Rechenzentrum
- `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 im Rechenzentrum eingesetzt.

Wichtige Hinweise zu Glasfaser

- Glasfaser ist empfindlicher gegenüber Schmutz an Steckern und unsachgemässer Behandlung.
- Die Reinigung von Steckverbindern ist in der Praxis wichtig.
- Glasfaser eignet sich besonders dort, wo lange Distanzen, hohe Bandbreiten oder geringe Störanfälligkeit gefordert sind.
- Die Installation und Messung ist meist anspruchsvoller als bei Kupfer.

Typische Einsatzorte von Glasfaser

- Uplinks zwischen Switches
- Backbone-Verbindungen
- Gebäudeverbindungen
- Rechenzentren
- Verbindungen mit hohen Bandbreitenanforderungen

Layer 2

Layer 2 ist die Sicherungsschicht. In Ethernet-Netzen arbeitet hier der Switch. Er leitet Frames anhand von MAC-Adressen weiter. Auf dieser Schicht geht es darum, wie Geräte innerhalb eines lokalen Netzes miteinander kommunizieren.

Wichtige Begriffe:

- `MAC-Adresse`: eindeutige Hardwareadresse einer Netzwerkschnittstelle
- `Frame`: Dateneinheit auf Layer 2
- `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. Wenn die Zieladresse noch nicht bekannt ist, wird ein Frame innerhalb des betreffenden VLANs an mehrere Ports weitergeleitet.

Kommunikationsarten

- `Unicast`: Kommunikation an genau ein Zielgerät
- `Broadcast`: Kommunikation an alle Geräte im gleichen Broadcast-Bereich
- `Multicast`: Kommunikation an eine bestimmte Gruppe von Empfängern
- `Anycast`: Kommunikation an den nächstgeeigneten Empfänger, meist eher ein Thema auf höheren Schichten

Warum Layer 2 wichtig ist

Layer 2 ist die Grundlage für die Kommunikation im lokalen Netzwerk. Ohne funktionierende Weiterleitung durch Switches, korrekte MAC-Zuordnung und passende VLAN-Zuweisung können Geräte trotz intakter Kabel nicht sinnvoll miteinander kommunizieren.

VLANs und Trunks

VLANs teilen ein physisches Switch-Netz in getrennte logische Netze auf. Dadurch entstehen getrennte Broadcast-Domänen. Geräte in unterschiedlichen VLANs sind logisch voneinander getrennt, auch wenn sie am gleichen physischen Switch angeschlossen sind.

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, dessen Frames auf dem Trunk standardmässig ungetaggt übertragen werden

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

Warum VLANs eingesetzt werden

VLANs helfen dabei,

- Netzwerke logisch zu strukturieren
- Broadcast-Verkehr zu begrenzen
- unterschiedliche Benutzergruppen oder Dienste zu trennen
- Sicherheit und Übersicht zu verbessern
- grosse Netze besser zu organisieren

Einfache Beispiele

- VLAN 10: Verwaltung
- VLAN 20: Lernende
- VLAN 30: Server oder Drucker

Auch wenn alle Geräte an demselben Switch hängen, gehören sie logisch zu getrennten Netzen, solange Routing zwischen den VLANs nicht ausdrücklich eingerichtet wird.

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 als Broadcast. Das Gerät mit der gesuchten IP-Adresse antwortet mit seiner MAC-Adresse.

ARP ist wichtig, weil Geräte auf Layer 3 mit IP-Adressen arbeiten, die tatsächliche Übertragung im lokalen Ethernet aber über MAC-Adressen erfolgt.

Grundidee des ARP-Ablaufs

1. Ein Gerät möchte ein Ziel im gleichen lokalen Netz erreichen.
2. Es kennt die Ziel-IP-Adresse, aber noch nicht die passende MAC-Adresse.
3. Es sendet eine ARP-Anfrage als Broadcast.
4. Das Zielgerät antwortet mit seiner MAC-Adresse.
5. Die Zuordnung wird vorübergehend in der ARP-Tabelle gespeichert.
6. Danach kann das Gerät den Ethernet-Frame an die passende MAC-Adresse senden.

Strukturierte Fehlersuche

Bei einfacher Fehlersuche helfen feste Prüfschritte. Arbeite nach Möglichkeit immer vom Einfachen zum Komplexeren:

1. Ist die physikalische Verbindung vorhanden?
2. Ist der Port aktiv?
3. Ist das richtige Kabel oder Medium verwendet?
4. Ist das richtige VLAN zugewiesen?
5. Lernt der Switch die MAC-Adresse?
6. Funktioniert `ping`?
7. Gibt es passende ARP-Einträge?
8. Stimmen Trunk und erlaubte VLANs?
9. Passt die IP-Konfiguration zum Netz?

Typische Fehlerbilder in diesem Modul

- Kabel nicht eingesteckt oder beschädigt
- Port ohne Link
- falsches VLAN am Access Port
- benötigtes VLAN auf dem Trunk nicht erlaubt
- Ziel-MAC-Adresse noch nicht gelernt
- falsche oder unvollständige IP-Konfiguration
- fehlender ARP-Eintrag oder keine Antwort auf ARP

Wichtige Befehle in diesem Modul

Die wichtigsten Diagnosebefehle in diesem Modul sind:

```
show mac address-table
show vlan
show interfaces trunk
show arp
show interfaces status
```

```
ping
arp -a
ipconfig /all
ip addr
```

Hinweise zur Dokumentation

Eine gute Lerndokumentation ist nicht einfach eine Sammlung von Screenshots. Sie zeigt, dass ihr verstanden habt, was ihr beobachtet habt.

Achtet deshalb auf folgende Punkte:

- schreibt in eigenen Worten
- verwendet Fachbegriffe korrekt
- ergänzt Skizzen, Tabellen oder einfache Topologien
- trennt Beobachtung und Vermutung
- dokumentiert Befehle und deren Bedeutung
- haltet fest, was funktioniert hat und was nicht
- erklärt kurz, was ihr aus der Aufgabe gelernt habt

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-Be