

20.3 Trainer – Schicht 2 / Ethernet, MAC-Adressen, Switching, VLAN und ARP

Diese Trainer-Seite wiederholt die OSI-Schicht 2, Ethernet, MAC-Adressen, Switching, VLANs und ARP.

Ziel ist, typische Prüfungsfragen zur lokalen Netzwerkkommunikation sicher zu lösen.

Merksatz:

Schicht 2 fragt:
Funktioniert die lokale Zustellung im gleichen Netzwerksegment?

Lernziele

Nach dieser Seite solltest du sicher können:

- OSI-Schicht 2 einordnen
- MAC-Adressen erklären
- Ethernet-Frames verstehen
- Switching erklären
- MAC-Adresstabellen nutzen
- Flooding und Broadcast unterscheiden
- VLANs einordnen
- Access-Port und Trunk-Port unterscheiden
- ARP erklären
- typische Schicht-2-Fehler erkennen

Kurzüberblick: OSI-Schicht 2

OSI-Schicht 2 heißt:

Sicherungsschicht

Aufgabe:

Datenübertragung im lokalen Netzwerksegment organisieren.

Typische Begriffe:

Ethernet
Frame
MAC-Adresse
Switch
VLAN
ARP
Broadcast
MAC-Adresstabelle
STP
Loop
Broadcast-Sturm

Merksatz:

Schicht 2 arbeitet lokal mit Frames und MAC-Adressen.

Kurzüberblick: Schicht 2 und Schicht 3

Thema	Schicht	Zweck
MAC-Adresse	2	lokale Zustellung
Ethernet-Frame	2	lokale Dateneinheit
Switch	2	Weiterleitung im LAN
VLAN	2	logische Trennung
IP-Adresse	3	logische Adressierung
Routing	3	Verbindung zwischen Netzen

Merksatz:

MAC lokal.
IP logisch.
Switch lokal.
Router zwischen Netzen.

Aufgabe 1

Wie heißt OSI-Schicht 2?

Antwort anzeigen

OSI-Schicht 2 heißt:

Sicherungsschicht

Englisch:

Data Link Layer

Aufgabe:

lokale Übertragung von Frames über MAC-Adressen.

Merksatz:

Schicht 2 = Sicherungsschicht.

Aufgabe 2

Welche Adresse gehört zu OSI-Schicht 2?

A: IP-Adresse

B: MAC-Adresse

C: Portnummer

D: URL

Antwort anzeigen

Richtig ist:

B: MAC-Adresse

Begründung:

MAC-Adressen werden auf OSI-Schicht 2 zur lokalen Zustellung im LAN verwendet.

Merksatz:

MAC-Adresse = Schicht 2.

Aufgabe 3

Was ist eine MAC-Adresse?

Antwort anzeigen

Eine MAC-Adresse ist eine Hardware-Adresse einer Netzwerkschnittstelle.

Sie dient zur lokalen Kommunikation im Netzwerksegment.

Beispiel:

AA:BB:CC:11:22:33

Typisch:

48 Bit lang

hexadezimale Schreibweise

Merksatz:

MAC-Adresse identifiziert eine Netzwerkschnittstelle im lokalen Netz.

Aufgabe 4

Was ist ein Ethernet-Frame?

Antwort anzeigen

Ein Ethernet-Frame ist die Dateneinheit auf OSI-Schicht 2.

Er enthält unter anderem:

Ziel-MAC-Adresse

Quell-MAC-Adresse

Nutzdaten

Prüfinformationen

Merksatz:

Ethernet überträgt Frames.

Aufgabe 5

Welche Informationen sind typisch in einem Ethernet-Frame enthalten?

Bestandteil	Enthalten?
Ziel-MAC-Adresse	?
Quell-MAC-Adresse	?
Ziel-Port TCP 443	?
IP-Nutzdaten	?

Antwort anzeigen

Bestandteil	Enthalten?
Ziel-MAC-Adresse	ja
Quell-MAC-Adresse	ja

Bestandteil	Enthalten?
Ziel-Port TCP 443	nicht direkt Schicht 2, sondern Teil der höheren Schichten
IP-Nutzdaten	ja, als Nutzdaten im Frame

Merksatz:

Der Frame transportiert höhere Schichten als Nutzdaten.

Aufgabe 6

Was macht ein Switch?

Antwort anzeigen

Ein Switch verbindet Geräte im lokalen Netzwerk.

Er arbeitet hauptsächlich auf OSI-Schicht 2 und leitet Ethernet-Frames anhand von MAC-Adressen weiter.

Merksatz:

Switch = lokale Weiterleitung anhand MAC-Adressen.

Aufgabe 7

Wie lernt ein Switch seine MAC-Adresstabelle?

Antwort anzeigen

Ein Switch lernt aus der Quell-MAC-Adresse eingehender Frames.

Wenn ein Frame an Port 3 ankommt, merkt sich der Switch:

Diese Quell-MAC-Adresse ist über Port 3 erreichbar.

Merksatz:

Switch lernt aus Quell-MAC-Adressen.

Aufgabe 8

Ein Switch kennt die Ziel-MAC-Adresse.

Was passiert?

Antwort anzeigen

Der Switch leitet den Frame gezielt an den Port weiter, an dem die Ziel-MAC-Adresse bekannt ist.

Merksatz:

bekannte Ziel-MAC:
gezielte Weiterleitung.

Aufgabe 9

Ein Switch kennt die Ziel-MAC-Adresse nicht.

Was passiert?

Antwort anzeigen

Der Switch flutet den Frame.

Das bedeutet:

Er sendet den Frame an alle Ports im gleichen VLAN,
außer an den Eingangsport.

Merksatz:

unbekannte Ziel-MAC:
Flooding.

Aufgabe 10

Was bedeutet Flooding?

Antwort anzeigen

Flooding bedeutet:

Ein Switch sendet einen Frame an alle Ports im gleichen VLAN,
außer an den Port,
über den der Frame gekommen ist.

Flooding passiert bei:

unbekannter Ziel-MAC-Adresse

Broadcast

bestimmten Multicast-Fällen

Merksatz:

Flooding ist nicht immer ein Fehler.

Aufgabe 11

Was ist ein Broadcast?

Antwort anzeigen

Ein Broadcast ist eine Nachricht an alle Geräte im gleichen Broadcast-Bereich.

Beispiel:

ARP Request

Broadcasts bleiben normalerweise im gleichen VLAN.

Merksatz:

Broadcast erreicht alle Geräte im gleichen VLAN.

Aufgabe 12

Was ist eine Broadcast-Domäne?

Antwort anzeigen

Eine Broadcast-Domäne ist der Bereich, in dem Broadcasts verteilt werden.

Ohne VLAN:

oft gesamtes Switch-Netz

Mit VLAN:

jedes VLAN ist eine eigene Broadcast-Domäne

Merksatz:

VLANs trennen Broadcast-Domänen.

Aufgabe 13

Was ist ein VLAN?

Antwort anzeigen

VLAN steht für:

Virtual Local Area Network

Ein VLAN trennt ein physisches Netzwerk logisch in mehrere getrennte Layer-2-Bereiche.

Beispiele:

VLAN 10 Verwaltung

VLAN 20 Clients

VLAN 30 Server

VLAN 40 Gäste

Merksatz:

VLAN = logische Trennung auf Schicht 2.

Aufgabe 14

Nenne zwei Gründe für den Einsatz von VLANs.

Antwort anzeigen

Mögliche Gründe:

logische Netztrennung

kleinere Broadcast-Domänen

bessere Struktur

Trennung von Abteilungen

Trennung von Gästen und internem Netz

Trennung von Servern und Clients

separate Managementnetze

IHK-sichere Antwort:

VLANs werden eingesetzt,
um Netzbereiche logisch zu trennen
und Broadcast-Domänen zu verkleinern.

Aufgabe 15

Ist ein VLAN dasselbe wie ein IP-Subnetz?

Antwort anzeigen

Nein.

VLAN:

logische Trennung auf OSI-Schicht 2

IP-Subnetz:

logische IP-Aufteilung auf OSI-Schicht 3

Wichtig:

In der Praxis bekommt ein VLAN häufig ein eigenes IP-Subnetz.
Fachlich sind VLAN und Subnetz aber nicht dasselbe.

Merksatz:

VLAN = Layer 2.
Subnetz = Layer 3.

Aufgabe 16

Was ist ein Access-Port?

Antwort anzeigen

Ein Access-Port gehört normalerweise zu genau einem VLAN.

Typische Nutzung:

PC

Drucker

Telefon

normales Endgerät

Das Endgerät muss das VLAN meist nicht selbst kennen.

Merksatz:

Access-Port = ein VLAN für Endgeräte.

Aufgabe 17

Was ist ein Trunk-Port?

Antwort anzeigen

Ein Trunk-Port transportiert mehrere VLANs über eine Verbindung.

Typische Nutzung:

Verbindung zwischen Switches

Verbindung zu Router

Verbindung zu Firewall

Verbindung zu Hypervisor

Verbindung zu VLAN-fähigem Access Point

Merksatz:

Trunk-Port = mehrere VLANs über eine Verbindung.

Aufgabe 18

Ordne zu.

Porttyp	Bedeutung
Access-Port	?
Trunk-Port	?

Antwort anzeigen

Porttyp	Bedeutung
Access-Port	ein VLAN, typisch für Endgeräte
Trunk-Port	mehrere VLANs, typisch zwischen Netzwerkgeräten

Merksatz:

Access = ein VLAN.

Trunk = mehrere VLANs.

Aufgabe 19

Was bedeutet VLAN-Tagging?

Antwort anzeigen

VLAN-Tagging bedeutet:

Ein Ethernet-Frame enthält eine VLAN-Information.

Häufiger Standard:

IEEE 802.1Q

Typisch bei:

Trunk-Verbindungen

Merksatz:

802.1Q markiert Frames mit VLAN-Information.

Aufgabe 20

Was ist der Unterschied zwischen untagged und tagged?

Antwort anzeigen

Untagged:

Frame enthält keinen VLAN-Tag für das Endgerät.

Typisch:

Access-Port

Tagged:

Frame enthält VLAN-Information.

Typisch:

Trunk-Port

Merksatz:

Access meist untagged.

Trunk meist tagged.

Aufgabe 21

Was ist ARP?

Antwort anzeigen

ARP steht für:

Address Resolution Protocol

Aufgabe:

ARP löst im lokalen IPv4-Netz eine IP-Adresse in eine MAC-Adresse auf.

Beispiel:

Der Client kennt die IP-Adresse des Gateways,
braucht aber für Ethernet die MAC-Adresse des Gateways.

Merksatz:

ARP findet die MAC-Adresse zu einer IPv4-Adresse.

Aufgabe 22

Warum braucht man ARP?

Antwort anzeigen

IPv4 arbeitet mit IP-Adressen.

Ethernet im lokalen Netz benötigt aber MAC-Adressen.

ARP verbindet diese beiden Ebenen, indem eine IPv4-Adresse einer MAC-Adresse zugeordnet wird.

Merksatz:

IP sagt,
welches Ziel gemeint ist.

MAC sagt,
wohin lokal gesendet wird.

Aufgabe 23

Ein Client möchte einen Server im gleichen Subnetz erreichen.

Welche MAC-Adresse wird verwendet?

Antwort anzeigen

Verwendet wird:

die MAC-Adresse des Zielserver

Begründung:

Das Ziel liegt im gleichen lokalen Subnetz.
Der Client kann daher direkt lokal per Ethernet an die MAC-Adresse des Zielserver senden.

Merksatz:

gleiches Subnetz:
MAC des Zielhosts.

Aufgabe 24

Ein Client möchte einen Server in einem anderen Subnetz erreichen.

Welche MAC-Adresse wird verwendet?

Antwort anzeigen

Verwendet wird:

die MAC-Adresse des Standardgateways

Begründung:

Das Ziel liegt außerhalb des lokalen Subnetzes.
Der Client sendet das Ethernet-Frame lokal an das Gateway.
Das IP-Ziel bleibt aber der entfernte Server.

Merksatz:

anderes Subnetz:
MAC des Gateways.

Aufgabe 25

Was ist ein ARP Request?

Antwort anzeigen

Ein ARP Request ist eine Anfrage per Broadcast.

Vereinfacht:

Wer hat diese IPv4-Adresse?

Beispiel:

Wer hat 192.168.1.1?

Merksatz:

ARP Request = Broadcast-Frage.

Aufgabe 26

Was ist ein ARP Reply?

Antwort anzeigen

Ein ARP Reply ist die Antwort auf einen ARP Request.

Vereinfacht:

Diese IPv4-Adresse gehört zu dieser MAC-Adresse.

Merksatz:

ARP Reply liefert die MAC-Adresse.

Aufgabe 27

Was ist eine ARP-Tabelle?

Antwort anzeigen

Die ARP-Tabelle speichert bekannte Zuordnungen:

IPv4-Adresse

zu

MAC-Adresse

Vorteil:

Der Host muss nicht für jedes Paket erneut per ARP fragen.

Merksatz:

ARP-Tabelle = Zwischenspeicher für IP-zu-MAC.

Aufgabe 28

Was ist ARP-Spoofing?

Antwort anzeigen

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

Netzwerksegmentierung

Switch-Sicherheitsfunktionen

Monitoring

Verschlüsselung höherer Schichten

Merksatz:

ARP-Spoofing manipuliert lokale IP-zu-MAC-Zuordnungen.

Aufgabe 29

Was ist STP?

Antwort anzeigen

STP steht für:

Spanning Tree Protocol

Aufgabe:

Layer-2-Schleifen verhindern

Warum wichtig?

Schleifen können Broadcast-Stürme verursachen
und das Netzwerk stark belasten oder lahmlegen.

Merksatz:

STP verhindert Switch-Schleifen.

Aufgabe 30

Was ist ein Broadcast-Sturm?

Antwort anzeigen

Ein Broadcast-Sturm entsteht, wenn Broadcasts durch Schleifen immer wieder weitergeleitet werden.

Folgen:

Netz wird langsam

Switches werden überlastet

Clients verlieren Verbindung

Dienste brechen ab

Merksatz:

Layer-2-Schleifen können das Netzwerk lahmlegen.

Aufgabe 31

Ein Client bekommt eine IP-Adresse aus dem falschen Netz.

Welches Schicht-2-Thema ist naheliegend?

Antwort anzeigen

Naheliegend ist:

falsches VLAN

Begründung:

Wenn ein Client am falschen VLAN hängt,
kann er vom falschen DHCP-Scope eine Adresse erhalten.

Merksatz:

falsches VLAN:
häufig falsche IP-Konfiguration.

Aufgabe 32

Ein Client bekommt keine DHCP-Adresse. Nur dieser eine Switchport ist betroffen.

Welche Ursachen sind wahrscheinlich?

Antwort anzeigen

Mögliche Ursachen:

Switchport deaktiviert

falsches Access-VLAN

Kabel oder Dose defekt

Port Security blockiert

VLAN nicht korrekt zugewiesen

Endgerät defekt

Merksatz:

Nur ein Port betroffen:
Port,
VLAN,
Kabel
und Endgerät prüfen.

Aufgabe 33

Mehrere VLANs funktionieren zwischen zwei Switches nicht richtig.

Was sollte geprüft werden?

Antwort anzeigen

Prüfen:

Trunk-Port aktiv?

VLANs auf Trunk erlaubt?

VLANs auf beiden Switches vorhanden?

Tagging korrekt?

Native VLAN passend?

Gegenstelle korrekt konfiguriert?

Merksatz:

Mehrere VLANs betroffen:

Trunk prüfen.

Aufgabe 34

Ein Gerät ist im richtigen IP-Subnetz, aber lokale Kommunikation funktioniert trotzdem nicht.

Welche Schicht-2-Themen können Ursache sein?

Antwort anzeigen

Mögliche Ursachen:

falsches VLAN

ARP-Problem

lokale Firewall

Switchport blockiert

Port Security

MAC-Adresstabelle fehlerhaft oder veraltet

Duplex- oder Linkproblem

Merksatz:

Gleiches Subnetz heißt nicht automatisch,
dass Layer 2 sauber funktioniert.

Aufgabe 35

Was ist Port Security?

Antwort anzeigen

Port Security begrenzt, welche oder wie viele MAC-Adressen an einem Switchport erlaubt sind.

Ziel:

unautorisierte Geräte erschweren

einfache Angriffe reduzieren

Portmissbrauch begrenzen

Merksatz:

Port Security kontrolliert MAC-Adressen am Switchport.

Aufgabe 36

Was ist 802.1X?

Antwort anzeigen

802.1X ist portbasierte Netzwerkzugangskontrolle.

Prinzip:

Ein Gerät oder Benutzer muss sich authentifizieren,
bevor Netzwerkzugriff erlaubt wird.

Typisch mit:

RADIUS

Zertifikaten

Benutzerkonto

Merksatz:

802.1X prüft Zugriff vor Netzzugang.

Aufgabe 37

Welche Aussage ist richtig?

A: VLANs ersetzen immer eine Firewall.

B: VLANs trennen Broadcast-Domänen.

C: VLANs gehören ausschließlich zu OSI-Schicht 7.

D: Ein Access-Port transportiert immer mehrere VLANs.

Antwort anzeigen

Richtig ist:

B: VLANs trennen Broadcast-Domänen.

Begründung:

VLANs trennen Layer-2-Bereiche logisch.
Sie ersetzen aber keine Firewall,
wenn Verkehr zwischen VLANs kontrolliert werden soll.

Merksatz:

VLAN trennt.
Firewall kontrolliert.

Aufgabe 38

Welche Antwort ist besser?

Aufgabe:

Warum braucht man für Kommunikation zwischen VLANs Routing?

Antwort A:

Weil VLANs sonst nicht modern genug sind.

Antwort B:

VLANs sind getrennte Layer-2-Bereiche.
Damit Geräte aus verschiedenen VLANs miteinander kommunizieren können,
müssen die jeweiligen IP-Netze über einen Router,
Layer-3-Switch
oder eine Firewall geroutet werden.

Antwort anzeigen

B ist besser.

Begründung:

Die Antwort erklärt die technische Trennung auf Schicht 2 und den Bedarf für Routing auf Schicht 3.

Merksatz:

VLANs trennen.
Routing verbindet.

Aufgabe 39

Welche Antwort ist besser?

Aufgabe:

Ein Switch sendet einen Frame an alle Ports im VLAN.
Ist das automatisch ein Fehler?

Antwort A:

Ja,
immer.

Antwort B:

Nein.
Bei unbekannter Ziel-MAC-Adresse oder Broadcast ist Flooding normales Verhalten.
Es wird erst problematisch,
wenn durch Schleifen oder Fehlkonfigurationen dauerhaft sehr viel Broadcast- oder Flooding-Verkehr entsteht.

Antwort anzeigen

B ist besser.

Begründung:

Flooding ist ein normales Switching-Verhalten,
wenn die Ziel-MAC-Adresse unbekannt ist.
Es ist nicht automatisch ein Fehler.

Merksatz:

Flooding normal,
Broadcast-Sturm kritisch.

Aufgabe 40

Was ist die wichtigste Unterscheidung zwischen MAC-Adresse, IP-Adresse und Port?

Antwort anzeigen

MAC-Adresse:

lokale Zustellung auf Schicht 2

IP-Adresse:

logische Adressierung auf Schicht 3

Port:

Zuordnung zu Dienst oder Prozess auf Schicht 4

Merksatz:

MAC lokal.
IP logisch.
Port Dienst.

Mini-Prüfung: schnelle Zuordnung

Frage	Antwort
Welche OSI-Schicht ist Ethernet?	Schicht 2
Welche OSI-Schicht ist MAC?	Schicht 2
Welche OSI-Schicht ist VLAN?	Schicht 2
Welche OSI-Schicht ist IP?	Schicht 3
Welche OSI-Schicht ist TCP?	Schicht 4
Was leitet ein Switch weiter?	Frames
Woran orientiert sich ein Switch?	MAC-Adressen
Was lernt ein Switch aus eingehenden Frames?	Quell-MAC-Adresse
Was passiert bei unbekannter Ziel-MAC?	Flooding
Was trennt VLAN?	Broadcast-Domänen
Was macht ARP?	IPv4 zu MAC auflösen
Was verhindert STP?	Layer-2-Schleifen

Mini-Prüfung: Fehlerbild erkennen

Fehlerbild	Wahrscheinliches Thema
Client im falschen Netz	falsches VLAN
nur ein Switchport betroffen	Access-Port, Kabel, Port Security
mehrere VLANs über Switchverbindung betroffen	Trunk
Broadcasts legen Netz lahm	Loop, STP, Broadcast-Sturm
lokale IP erreichbar, aber MAC ändert sich ständig	doppelte IP oder ARP-Spoofing
gleiches Subnetz, aber keine lokale Kommunikation	VLAN, ARP, Firewall, Switchport
DHCP nur in einem VLAN defekt	VLAN, DHCP-Relay, DHCP-Scope
Gerät bekommt falschen DHCP-Bereich	falsches VLAN

IHK-sichere Kurzformulierung

Die OSI-Schicht 2 ist die Sicherungsschicht. Sie organisiert die lokale Kommunikation im Netzwerksegment. Ethernet nutzt Frames, die unter anderem Quell- und Ziel-MAC-Adressen enthalten. Ein Switch arbeitet hauptsächlich auf Schicht 2 und leitet Frames anhand seiner MAC-Adresstabelle weiter. Diese Tabelle lernt er aus den Quell-MAC-Adressen eingehender Frames. Ist die Ziel-MAC unbekannt, wird der Frame im VLAN geflutet. VLANs trennen ein physisches Netzwerk

logisch in mehrere Broadcast-Domänen. Access-Ports gehören meist zu einem VLAN, Trunk-Ports transportieren mehrere VLANs mit VLAN-Tagging nach IEEE 802.1Q. ARP löst im lokalen IPv4-Netz IP-Adressen in MAC-Adressen auf.

Merksätze

Schicht 2 ist die Sicherungsschicht.

Schicht 2 arbeitet mit Frames.

Ethernet nutzt Frames.

MAC-Adresse gehört zu Schicht 2.

Switches arbeiten hauptsächlich auf Schicht 2.

Switches leiten anhand von MAC-Adressen weiter.

Switch lernt aus Quell-MAC-Adressen.

Bekannte Ziel-MAC:
gezielte Weiterleitung.

Unbekannte Ziel-MAC:
Flooding.

Broadcast erreicht alle Geräte im gleichen VLAN.

VLANs trennen Broadcast-Domänen.

VLAN ist Layer 2.

Subnetz ist Layer 3.

VLAN und Subnetz sind nicht dasselbe.

Access-Port = ein VLAN.

Trunk-Port = mehrere VLANs.

802.1Q markiert VLAN-Frames.

Access meist untagged.

Trunk meist tagged.

VLAN trennt.

Firewall kontrolliert.

Inter-VLAN-Kommunikation braucht Routing.

ARP löst IPv4 zu MAC auf.

ARP arbeitet lokal.

ARP Request ist Broadcast.

ARP Reply liefert die MAC-Adresse.

Gleiches Subnetz:

MAC des Zielhosts.

Anderes Subnetz:

MAC des Gateways.

IP zeigt zum Endziel.

MAC zeigt zum nächsten lokalen Hop.

STP verhindert Layer-2-Schleifen.

Broadcast-Sturm kann ein Netz lahmlegen.

Port Security kontrolliert MAC-Adressen.

802.1X prüft Netzzugang.

Falsches VLAN führt oft zu falscher IP-Konfiguration.

Mehrere VLANs betroffen:

Trunk prüfen.

Nur ein Port betroffen:

Port,

VLAN,

Kabel

und Endgerät prüfen.
