5.5 ARP – IP-Adresse zur MAC-Adresse auflösen

ARP gehört zu den wichtigsten Grundlagen im lokalen Netzwerk.

ARP steht für:

```
Address Resolution Protocol
```

Auf Deutsch sinngemäß:

```
Adressauflösungsprotokoll
```

ARP wird benötigt, damit ein Gerät zu einer bekannten IP-Adresse die passende MAC-Adresse im lokalen Netzwerk herausfinden kann.

Merksatz:

```
ARP findet die MAC-Adresse zu einer IP-Adresse im lokalen Netz.
```

Warum braucht man ARP?

IP-Adressen gehören zu OSI-Schicht 3.

MAC-Adressen gehören zu OSI-Schicht 2.

Ein Ethernet-Frame braucht für die lokale Zustellung eine Ziel-MAC-Adresse.

Wenn ein PC nur die Ziel-IP-Adresse kennt, muss er herausfinden:

```
Welche MAC-Adresse gehört zu dieser IP-Adresse?
```

Genau dafür wird ARP verwendet.

Merksatz:

```
IP allein reicht im Ethernet-LAN nicht aus,
der Frame braucht eine Ziel-MAC-Adresse.
```

Schicht 2 und Schicht 3 zusammengedacht

Ein Gerät arbeitet beim Senden im LAN mit mehreren Schichten gleichzeitig.

Beispiel:

```
Ziel-IP-Adresse:
192.168.10.20
```

Damit der Frame im lokalen Ethernet gesendet werden kann, braucht der PC zusätzlich:

```
Ziel-MAC-Adresse:
zum Beispiel AA:BB:CC:11:22:33
```

ARP verbindet diese beiden Ebenen.

Adresse	Schicht	Aufgabe
MAC-Adresse	2	lokale Zustellung im LAN
IP-Adresse	3	logische Adressierung im IP-Netz

Merksatz:

```
ARP verbindet IP-Adresse und MAC-Adresse im lokalen Netz.
```

Grundprinzip von ARP

ARP arbeitet nach dem Prinzip:

```
Wer hat diese IP-Adresse?
Bitte melde deine MAC-Adresse.
```

Ein Gerät sendet also eine Anfrage ins lokale Netzwerk.

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

Merksatz:

```
ARP fragt:
Wer hat diese IP?
```

ARP-Anfrage

Eine ARP-Anfrage wird verwendet, wenn ein Gerät die MAC-Adresse zu einer IP-Adresse noch nicht kennt.

Beispiel:

```
PC A möchte PC B erreichen.
PC A kennt die IP-Adresse von PC B.
PC A kennt aber noch nicht die MAC-Adresse von PC B.
```

Dann sendet PC A eine ARP-Anfrage.

Sinngemäß:

```
Wer hat 192.168.10.20?
Bitte 192.168.10.10 antworten.
```

Merksatz:

```
ARP-Anfrage = Suche nach der MAC-Adresse zu einer IP-Adresse.
```

ARP-Anfrage als Broadcast

Eine ARP-Anfrage wird als Broadcast gesendet.

Warum?

```
Der Absender kennt die Ziel-MAC-Adresse noch nicht.
```

Deshalb wird die Anfrage an alle Geräte im lokalen Netz geschickt.

Die Broadcast-MAC-Adresse lautet:

```
FF:FF:FF:FF:FF:FF
```

Alle Geräte im lokalen Netz empfangen die ARP-Anfrage.

Aber nur das Gerät mit der gesuchten IP-Adresse antwortet.

Merksatz:

```
ARP-Anfrage = Broadcast.
```

ARP-Antwort

Die ARP-Antwort kommt von dem Gerät, das die gesuchte IP-Adresse besitzt.

Die Antwort enthält die passende MAC-Adresse.

Beispiel:

```
PC B antwortet:
192.168.10.20 gehört zu AA:BB:CC:11:22:33
```

Danach kann PC A Ethernet-Frames gezielt an die MAC-Adresse von PC B senden.

Merksatz:

```
ARP-Antwort liefert die gesuchte MAC-Adresse.
```

ARP-Antwort als Unicast

Eine ARP-Antwort wird normalerweise als Unicast gesendet.

Das bedeutet:

```
Die Antwort geht gezielt an den Absender der ARP-Anfrage.
```

Beispiel:

```
PC B antwortet direkt an PC A.
```

Warum?

```
PC B kennt aus der ARP-Anfrage bereits die MAC-Adresse von PC A.
```

Merksatz:

```
ARP-Antwort = meistens Unicast.
```

ARP im gleichen IP-Netz

ARP funktioniert für Ziele im gleichen lokalen IP-Netz.

Beispiel:

Gerät	IP-Adresse
PC A	192.168.10.10/24
PC B	192.168.10.20/24

Beide Geräte befinden sich im gleichen Subnetz:

```
192.168.10.0/24
```

Wenn PC A PC B erreichen möchte, sucht PC A per ARP die MAC-Adresse von PC B.

Merksatz:

```
Gleiches Subnetz:
ARP sucht die MAC-Adresse des Zielgeräts.
```

ARP bei Ziel in anderem Netz

Wenn das Ziel in einem anderen IP-Netz liegt, sucht der PC nicht die MAC-Adresse des entfernten Zielservers.

Stattdessen sucht er die MAC-Adresse seines Standard-Gateways.

Beispiel:

```
PC:
192.168.10.10/24

Ziel:
8.8.8.8
```

Das Ziel liegt nicht im lokalen Netz.

Der PC sendet deshalb den Ethernet-Frame an die MAC-Adresse des Routers.

Im IP-Paket bleibt als Ziel-IP aber weiterhin:

```
8.8.8.8
```

Merksatz:

```
Anderes Netz:
ARP sucht die MAC-Adresse des Gateways.
```

Standard-Gateway und ARP

Das Standard-Gateway ist der Router, über den ein Gerät andere Netzwerke erreicht.

Wenn ein Ziel nicht im eigenen Subnetz liegt, sendet der PC an das Standard-Gateway.

Dafür braucht der PC die MAC-Adresse des Gateways.

Diese wird per ARP ermittelt.

Beispiel:

```
Gateway-IP:
192.168.10.1

ARP fragt:
Wer hat 192.168.10.1?
```

Merksatz:

```
Für entfernte Ziele braucht der PC die MAC-Adresse des Gateways.
```

MAC-Adresse ändert sich pro Netzwerkabschnitt

Wenn Daten über Router übertragen werden, ändern sich die MAC-Adressen auf jedem lokalen Abschnitt.

Beispiel:

```
PC
→ Router
→ weiterer Router
→ Server
```

Auf jedem Abschnitt gibt es neue Ethernet-Frames mit neuen Quell- und Ziel-MAC-Adressen.

Die IP-Adressen bleiben grundsätzlich erhalten, außer bei NAT oder PAT.

Merksatz:

```
MAC-Adressen gelten nur lokal bis zum nächsten Router.
```

IP-Adresse bleibt grundsätzlich erhalten

Während sich die MAC-Adressen von Abschnitt zu Abschnitt ändern, bleibt die Ziel-IP-Adresse normalerweise gleich.

Beispiel:

```
PC möchte 8.8.8.8 erreichen.
```

Auf dem ersten Ethernet-Abschnitt gilt:

```
Ziel-MAC = Router
Ziel-IP = 8.8.8.8
```

Der Router entfernt den alten Ethernet-Frame und erstellt für den nächsten Abschnitt einen neuen Frame.

Die Ziel-IP bleibt dabei weiterhin 8.8.8.8.

Merksatz:

```
MAC ändert sich pro Hop.
IP bleibt grundsätzlich Ende-zu-Ende.
```

ARP-Tabelle

Ein Gerät speichert bekannte Zuordnungen von IP-Adresse zu MAC-Adresse in einer ARP-Tabelle.

Diese Tabelle wird auch genannt:

ARP-Cache

Beispiel:

IP-Adresse	MAC-Adresse
192.168.10.1	00:11:22:33:44:55
192.168.10.20	AA:BB:CC:11:22:33

Der Vorteil:

Das Gerät muss nicht vor jedem einzelnen Frame erneut eine ARP-Anfrage senden.

Merksatz:

ARP-Cache speichert IP-zu-MAC-Zuordnungen.

ARP-Cache ist zeitlich begrenzt

ARP-Einträge bleiben nicht dauerhaft gespeichert.

Nach einiger Zeit werden sie automatisch gelöscht oder erneuert.

Warum?

Geräte können ausgeschaltet werden.
Geräte können eine andere Netzwerkkarte nutzen.
IP-Adressen können neu vergeben werden.
Netzwerkstrukturen können sich ändern.

Merksatz:

ARP-Einträge altern und werden aktualisiert.

Statische und dynamische ARP-Einträge

ARP-Einträge können dynamisch oder statisch sein.

Art	Bedeutung
dynamischer ARP-Eintrag	automatisch durch ARP gelernt
statischer ARP-Eintrag	manuell fest eingetragen

In normalen Netzwerken werden meistens dynamische ARP-Einträge verwendet.

Statische Einträge sind Sonderfälle und können Wartung erschweren.

Merksatz:

> ARP ist normalerweise dynamisch.

ARP und Switches

Ein Switch leitet ARP-Frames wie andere Ethernet-Frames weiter.

Wichtig:

> Eine ARP-Anfrage ist ein Broadcast.
> Der Switch verteilt sie innerhalb des VLANs.
> Eine ARP-Antwort ist meistens Unicast.
> Der Switch leitet sie gezielt weiter, wenn die Ziel-MAC bekannt ist.

Dabei lernt der Switch weiterhin MAC-Adressen über die Quell-MAC-Adresse eingehender Frames.

Merksatz:

> ARP hilft Endgeräten,
> Switches lernen trotzdem über Quell-MACs.

ARP und VLANs

ARP bleibt innerhalb einer Broadcast-Domäne.

Da ein VLAN normalerweise eine eigene Broadcast-Domäne bildet, bleibt eine ARP-Anfrage innerhalb dieses VLANs.

Beispiel:

ARP-Anfrage in VLAN 10
bleibt in VLAN 10.

Sie wird nicht automatisch in VLAN 20 weitergeleitet.

Merksatz:

ARP-Broadcasts bleiben im VLAN.

ARP und Router

Router leiten ARP-Broadcasts normalerweise nicht in andere Netze weiter.

Warum?

Broadcasts sollen auf das lokale Netz begrenzt bleiben.

Wenn ein Router ein IP-Paket weiterleitet, nutzt er auf dem nächsten Netzwerkabschnitt selbst wieder ARP, um die nächste lokale Ziel-MAC zu finden.

Merksatz:

Router trennen ARP-Broadcasts.

ARP und DHCP

ARP und DHCP sind unterschiedliche Protokolle.

DHCP dient dazu, IP-Konfiguration automatisch zu vergeben.

ARP dient dazu, zu einer IP-Adresse die passende MAC-Adresse im lokalen Netz zu finden.

Protokoll	Aufgabe
DHCP	IP-Adresse und Netzwerkkonfiguration vergeben
ARP	MAC-Adresse zu einer IP-Adresse finden

Beide nutzen Broadcasts im lokalen Netz.

Merksatz:

```
DHCP vergibt IP.
ARP findet MAC zu IP.
```

ARP und DNS

ARP und DNS werden häufig verwechselt, weil beide etwas „auflösen“.

Aber sie lösen unterschiedliche Dinge auf.

Protokoll	Auflösung
DNS	Name zu IP-Adresse
ARP	IP-Adresse zu MAC-Adresse

Beispiel:

```
DNS:
www.example.com → 93.184.216.34

ARP:
192.168.10.1 → 00:11:22:33:44:55
```

Merksatz:

```
DNS findet IP zu Name.
ARP findet MAC zu IP.
```

Ablauf: Webseite im Internet öffnen

Beispiel:

```
PC öffnet eine Webseite im Internet.
```

Vereinfacht passiert:

```
1. DNS löst den Namen zur IP-Adresse auf.
2. PC erkennt:
   Ziel-IP liegt nicht im eigenen Subnetz.
```

3. PC braucht das Standard-Gateway.
4. PC sucht per ARP die MAC-Adresse des Gateways.
5. PC sendet Ethernet-Frame an die MAC-Adresse des Gateways.
6. Im IP-Paket steht die Ziel-IP des Webservers.
7. Router leitet das IP-Paket weiter.

Merksatz:

Zum Internetziel geht der erste Frame lokal an das Gateway.

Ablauf: Gerät im gleichen LAN erreichen

Beispiel:

PC A will PC B im gleichen Subnetz erreichen.

Vereinfacht passiert:

1. PC A prüft:
   Ziel-IP liegt im eigenen Subnetz.
2. PC A sucht per ARP die MAC-Adresse von PC B.
3. PC B antwortet mit seiner MAC-Adresse.
4. PC A speichert die Zuordnung im ARP-Cache.
5. PC A sendet Ethernet-Frames direkt an die MAC-Adresse von PC B.

Merksatz:

Im gleichen Subnetz wird direkt an die Ziel-MAC gesendet.

Ablauf: Gerät in anderem VLAN erreichen

Beispiel:

PC in VLAN 10 will Server in VLAN 30 erreichen.

VLANs sind getrennte Broadcast-Domänen.

PC kann nicht direkt per ARP die MAC-Adresse des Servers in VLAN 30 ermitteln.

Stattdessen:

```
PC sendet an das Gateway von VLAN 10.
Das Gateway routet Richtung VLAN 30.
Dort wird für den nächsten lokalen Abschnitt wieder ARP verwendet.
```

Merksatz:

```
Zwischen VLANs braucht man Routing,
nicht direkte ARP-Auflösung zum Zielgerät.
```

Gratuitous ARP

Gratuitous ARP bedeutet:

```
Ein Gerät sendet eine ARP-Information über sich selbst,
ohne dass vorher jemand danach gefragt hat.
```

Mögliche Zwecke:

```
- ARP-Cache anderer Geräte aktualisieren
- IP-Adresskonflikte erkennen
- Failover-Szenarien unterstützen
- neue MAC-Zuordnung bekannt machen
```

Für AP1/AP2 reicht meist:

```
Gratuitous ARP informiert das lokale Netz über eine IP-MAC-Zuordnung.
```

Merksatz:

```
Gratuitous ARP = ARP-Information ohne direkte Anfrage.
```

ARP-Probe

Eine ARP-Probe kann verwendet werden, um zu prüfen, ob eine IP-Adresse bereits im lokalen Netz verwendet wird.

Beispiel:

```
Ein Gerät möchte eine IP-Adresse nutzen.
Vorher fragt es im Netz,
ob jemand diese IP-Adresse bereits verwendet.
```

Das hilft, IP-Adresskonflikte zu vermeiden.

Merksatz:

```
ARP kann helfen,
doppelte IP-Adressen zu erkennen.
```

IP-Adresskonflikt

Ein IP-Adresskonflikt entsteht, wenn zwei Geräte dieselbe IP-Adresse im gleichen Netz verwenden.

Mögliche Folgen:

```
- Verbindungsabbrüche
- wechselnde Erreichbarkeit
- ARP-Einträge ändern sich ständig
- falsches Gerät antwortet
- Netzwerkprobleme schwer nachvollziehbar
```

ARP kann Hinweise auf solche Konflikte liefern.

Merksatz:

```
Doppelte IP-Adressen können ARP-Probleme verursachen.
```

ARP-Spoofing

ARP-Spoofing ist ein Angriff auf ARP.

Dabei sendet ein Angreifer falsche ARP-Informationen ins Netzwerk.

Ziel:

```
Andere Geräte sollen eine falsche MAC-Adresse zu einer IP-Adresse speichern.
```

Beispiel:

```
Angreifer behauptet:
Ich bin das Gateway.
```

Dann senden Clients ihre Frames möglicherweise an den Angreifer.

Merksatz:

```
ARP-Spoofing = falsche IP-MAC-Zuordnung einschleusen.
```

ARP-Poisoning

ARP-Poisoning ist eng mit ARP-Spoofing verwandt.

Dabei wird der ARP-Cache anderer Geräte mit falschen Informationen „vergiftet“.

Mögliche Folgen:

```
- Man-in-the-Middle-Angriff
- Datenverkehr wird umgeleitet
- Verbindungsausfall
- Abhören oder Manipulation von Daten
```

Merksatz:

```
ARP-Poisoning manipuliert ARP-Caches.
```

Warum ist ARP angreifbar?

ARP wurde für lokale Netze entwickelt und vertraut Antworten im lokalen Netzwerk relativ stark.

Problem:

```
Geräte prüfen ARP-Antworten nicht immer ausreichend.
Auch ungefragte ARP-Informationen können übernommen werden.
```

Angreifer im lokalen Netz können falsche Zuordnungen senden.

Deshalb ist Netztrennung und Zugriffskontrolle wichtig.

Merksatz:

ARP ist im lokalen Netz nützlich,
aber nicht besonders stark gegen Manipulation geschützt.

Schutzmaßnahmen gegen ARP-Angriffe

Mögliche Schutzmaßnahmen:

- VLAN-Trennung
- 802.1X
- Port Security
- Dynamic ARP Inspection
- DHCP Snooping
- statische ARP-Einträge in Sonderfällen
- Monitoring
- sichere Switch-Konfiguration
- keine unnötigen Geräte im internen Netz

Für AP1/AP2 ist besonders wichtig:

ARP-Angriffe werden durch saubere Netztrennung und Switch-Sicherheitsfunktionen erschwert.

Merksatz:

ARP-Schutz beginnt mit sauberer Layer-2-Sicherheit.

Dynamic ARP Inspection

Dynamic ARP Inspection ist eine Switch-Sicherheitsfunktion.

Sie kann ARP-Nachrichten prüfen und gefälschte ARP-Informationen blockieren.

Häufig arbeitet sie zusammen mit DHCP Snooping.

Für AP1/AP2 reicht:

```
Dynamic ARP Inspection schützt vor gefälschten ARP-Antworten.
```

Merksatz:

```
Dynamic ARP Inspection prüft ARP auf dem Switch.
```

DHCP Snooping

DHCP Snooping ist eine Switch-Sicherheitsfunktion.

Sie unterscheidet vertrauenswürdige und nicht vertrauenswürdige Ports für DHCP.

Ziel:

```
unerlaubte DHCP-Server verhindern
und Informationen über IP-MAC-Zuordnungen sammeln
```

Diese Informationen können wiederum für Dynamic ARP Inspection genutzt werden.

Merksatz:

```
DHCP Snooping hilft gegen falsche DHCP-Server und unterstützt ARP-Schutz.
```

ARP und IPv6

ARP wird bei IPv4 verwendet.

Bei IPv6 wird ARP nicht mehr verwendet.

IPv6 nutzt stattdessen:

```
Neighbor Discovery Protocol
```

Abkürzung:

```
NDP
```

NDP übernimmt ähnliche Aufgaben in IPv6-Netzen.

Merksatz:

> IPv4 nutzt ARP.
> IPv6 nutzt NDP.

ARP in der Fehlersuche

ARP ist sehr hilfreich bei der Fehlersuche im lokalen Netzwerk.

Typische Prüffragen:

> Gibt es einen ARP-Eintrag für das Gateway?
> Stimmt die MAC-Adresse zum erwarteten Gerät?
> Ändert sich ein ARP-Eintrag ständig?
> Gibt es doppelte IP-Adressen?
> Wird die MAC-Adresse des Ziels gelernt?
> Liegt das Ziel im gleichen Subnetz?
> Ist das richtige VLAN aktiv?

Merksatz:

> ARP zeigt,
> ob IP und MAC lokal zusammenfinden.

Typische ARP-Fehlerbilder

Fehlerbild	mögliche Ursache
kein ARP-Eintrag für Gateway	Gateway nicht erreichbar, falsches VLAN, Schicht-1-Problem
wechselnde MAC-Adresse zu einer IP	IP-Konflikt oder ARP-Spoofing
ARP klappt, aber Ping nicht	Firewall, ICMP blockiert, Routing oder Zielproblem
keine ARP-Antwort	Ziel aus, falsches VLAN, falsches Subnetz
falsche MAC im ARP-Cache	ARP-Spoofing oder veralteter Eintrag

Merksatz:

ARP-Fehler können auf VLAN-, IP- oder Sicherheitsprobleme hinweisen.

ARP-Cache anzeigen

Auf vielen Systemen kann man den ARP-Cache anzeigen.

Beispiele:

```
Windows:
arp -a

Linux:
ip neigh

macOS:
arp -a
```

Diese Befehle zeigen bekannte IP-MAC-Zuordnungen.

Wichtig:

Die genaue Ausgabe hängt vom Betriebssystem ab.

Merksatz:

ARP-Cache zeigt bekannte lokale IP-MAC-Zuordnungen.

ARP-Cache leeren

Manchmal kann es sinnvoll sein, alte ARP-Einträge zu entfernen.

Beispiele:

```
Gerät wurde ausgetauscht.
Gateway hat neue MAC-Adresse.
ARP-Eintrag ist veraltet.
IP-Konflikt wurde behoben.
```

Danach kann das Gerät die MAC-Adresse neu per ARP lernen.

Merksatz:

> ARP-Cache leeren erzwingt neue ARP-Auflösung.

Einordnung in das OSI-Modell

ARP liegt zwischen Schicht 2 und Schicht 3.

Warum?

> ARP fragt zu einer IP-Adresse die passende MAC-Adresse ab.

Thema	Schicht
MAC-Adresse	2
Ethernet-Frame	2
ARP-Nachricht im LAN	2 / 3-Bezug
IP-Adresse	3
Routing	3
TCP-Port	4
DNS	7

Prüfungstauglich:

> ARP wird meist im Zusammenhang mit Schicht 2 und 3 betrachtet.

Merksatz:

> ARP verbindet Schicht 3 mit Schicht 2.

Was ARP nicht macht

ARP macht nicht:

- DNS-Namen auflösen
- IP-Adressen vergeben
- zwischen VLANs routen
- TCP-Verbindungen aufbauen
- Internetseiten laden
- Firewall-Regeln prüfen
- Verschlüsselung bereitstellen

ARP hat eine sehr konkrete Aufgabe:

IP-Adresse zu MAC-Adresse im lokalen Netz auflösen.

Merksatz:

ARP ist keine Namensauflösung,
sondern Adressauflösung im LAN.

Typische IHK-Fragen

In AP1 und AP2 kann zum Beispiel gefragt werden:

- Was bedeutet ARP?
- Welche Aufgabe hat ARP?
- Warum braucht man ARP?
- Was ist eine ARP-Anfrage?
- Warum ist die ARP-Anfrage ein Broadcast?
- Warum ist die ARP-Antwort meist ein Unicast?
- Was steht im ARP-Cache?
- Was passiert, wenn das Ziel in einem anderen Netz liegt?
- Welche MAC-Adresse wird verwendet, wenn das Ziel nicht im eigenen Subnetz liegt?
- Was ist der Unterschied zwischen ARP und DNS?
- Was ist der Unterschied zwischen ARP und DHCP?
- Was ist ARP-Spoofing?
- Warum verwendet IPv6 kein ARP?

Typische Prüfungsfallen

ARP findet MAC-Adresse zu IP-Adresse.

DNS findet IP-Adresse zu Name.

DHCP vergibt IP-Konfiguration.

ARP-Anfrage ist Broadcast.

ARP-Antwort ist meistens Unicast.

ARP funktioniert lokal innerhalb der Broadcast-Domäne.

ARP-Broadcasts werden normalerweise nicht über Router weitergeleitet.

Bei Ziel im gleichen Subnetz wird die MAC des Zielgeräts gesucht.

Bei Ziel in anderem Subnetz wird die MAC des Gateways gesucht.

MAC-Adresse ändert sich pro Netzwerkabschnitt.

IP-Adresse bleibt grundsätzlich über Router hinweg erhalten.

IPv4 nutzt ARP.

IPv6 nutzt NDP.

ARP kann durch Spoofing manipuliert werden.

Wichtige Begriffe kurz erklärt

Begriff	Kurze Erklärung
ARP	Address Resolution Protocol
ARP-Anfrage	Anfrage nach der MAC-Adresse zu einer IP-Adresse
ARP-Antwort	Antwort mit IP-MAC-Zuordnung
ARP-Cache	gespeicherte IP-MAC-Zuordnungen
Broadcast	Nachricht an alle Geräte im lokalen Netz
Unicast	Nachricht an ein bestimmtes Gerät

Begriff	Kurze Erklärung
MAC-Adresse	lokale Hardwareadresse
IP-Adresse	logische Adresse auf Schicht 3
Standard-Gateway	Router ins andere Netz
Gratuitous ARP	ungefragte ARP-Information über eigene IP-MAC-Zuordnung
ARP-Probe	Prüfung, ob eine IP-Adresse bereits verwendet wird
IP-Adresskonflikt	zwei Geräte nutzen gleiche IP-Adresse
ARP-Spoofing	falsche ARP-Informationen senden
ARP-Poisoning	ARP-Cache mit falschen Informationen manipulieren
Dynamic ARP Inspection	Switch-Schutz gegen gefälschte ARP-Informationen
DHCP Snooping	Switch-Schutz gegen unerlaubte DHCP-Server
NDP	Neighbor Discovery Protocol bei IPv6

IHK-sichere Kurzformulierung

ARP steht für Address Resolution Protocol und wird in IPv4-Netzen verwendet, um zu einer bekannten IP-Adresse die passende MAC-Adresse im lokalen Netzwerk zu ermitteln. Eine ARP-Anfrage wird als Broadcast gesendet, weil die Ziel-MAC-Adresse noch unbekannt ist. Das Gerät mit der gesuchten IP-Adresse antwortet normalerweise per Unicast mit seiner MAC-Adresse. Wenn sich das Ziel im gleichen Subnetz befindet, wird die MAC-Adresse des Zielgeräts gesucht. Befindet sich das Ziel in einem anderen Netz, wird die MAC-Adresse des Standard-Gateways ermittelt. ARP arbeitet lokal innerhalb einer Broadcast-Domäne und verbindet die IP-Adressierung auf Schicht 3 mit der MAC-Adressierung auf Schicht 2.

Merksätze

```
ARP = Address Resolution Protocol.

ARP findet MAC-Adresse zu IP-Adresse.

ARP gehört zu IPv4.

IPv6 nutzt NDP statt ARP.

ARP verbindet Schicht 3 mit Schicht 2.

IP-Adresse = Schicht 3.
```

MAC-Adresse = Schicht 2.

ARP-Anfrage = Broadcast.

ARP-Antwort = meistens Unicast.

Broadcast-MAC = FF:FF:FF:FF:FF:FF.

ARP bleibt im lokalen Netz.

Router leiten ARP-Broadcasts nicht weiter.

Gleiches Subnetz:
ARP sucht Ziel-MAC.

Anderes Subnetz:
ARP sucht Gateway-MAC.

MAC-Adresse ändert sich pro Netzwerkabschnitt.

IP-Adresse bleibt grundsätzlich erhalten.

ARP-Cache speichert IP-MAC-Zuordnungen.

DNS ist nicht ARP.

DHCP ist nicht ARP.

ARP-Spoofing manipuliert IP-MAC-Zuordnungen.

Erst ARP verstehen,
dann Switching und Routing wirklich verstehen.