3.5 ARP und IPv6 Neighbor Discovery analysieren

Damit ein Endgerät ein IP-Paket innerhalb eines lokalen Ethernetnetzes übertragen kann, benötigt es die zugehörige MAC-Adresse des nächsten direkten Kommunikationspartners.

Bei IPv4 übernimmt diese Zuordnung das Address Resolution Protocol, kurz ARP. IPv6 verwendet dafür Neighbor Discovery, kurz NDP beziehungsweise ND, auf Basis von ICMPv6.

> **Grundregel:** Für ein Ziel im lokalen Subnetz wird die MAC-Adresse des Zielsystems benötigt. Für ein Ziel in einem entfernten Subnetz wird normalerweise die MAC-Adresse des nächsten Routers benötigt – nicht die MAC-Adresse des entfernten Zielsystems.

---

1. Welche Aufgabe erfüllt ARP?

ARP ordnet eine lokale IPv4-Adresse einer MAC-Adresse zu.

Beispiel im selben Subnetz

```
CLIENT-023
IPv4: 192.0.2.23/24
MAC:  00-11-22-33-44-55

SERVER-01
IPv4: 192.0.2.80/24
MAC:  AA-BB-CC-DD-EE-FF
```

Der Client kennt zunächst nur die IPv4-Adresse des Servers und sendet eine ARP-Anfrage:

```
Wer hat 192.0.2.80?
Antwort bitte an 192.0.2.23.
```

Die Anfrage wird als Ethernet-Broadcast gesendet:

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

Der Server antwortet normalerweise per Unicast:

```
192.0.2.80 befindet sich unter AA:BB:CC:DD:EE:FF.
```

Der Client kann die Zuordnung anschließend vorübergehend in seiner Nachbartabelle speichern.

2. Welche MAC-Adresse wird bei einem entfernten IPv4-Ziel aufgelöst?

Ausgangslage

```
Client:  192.0.2.23/24
Gateway: 192.0.2.1
Ziel:    198.51.100.20
```

Das Ziel liegt nicht im lokalen Subnetz `192.0.2.0/24`.

Der Client ermittelt daher normalerweise nicht die MAC-Adresse von `198.51.100.20`, sondern die MAC-Adresse des nächsten Routers:

```
ARP-Anfrage:
Wer hat 192.0.2.1?
```

Anschließend entsteht vereinfacht folgender Frame:

```
Ethernet-Ziel-MAC: MAC-Adresse des Gateways
IP-Zieladresse:    198.51.100.20
```

Ebene	Ziel
Ethernet	nächster Router
IPv4	entferntes Zielsystem

Die Ethernetadressen können sich an jedem gerouteten Abschnitt ändern. Die IP-Zieladresse bleibt ohne NAT normalerweise bis zum Ziel bestehen.

3. Welche Symptome sprechen für ein ARP- oder Neighbor-Discovery-Problem?

- Gateway ist trotz korrekter IP-Konfiguration nicht erreichbar,
- Ziel im selben Subnetz ist nicht erreichbar,
- Nachbareintrag bleibt unvollständig,
- dieselbe IP-Adresse erscheint mit wechselnden MAC-Adressen,
- Verbindung funktioniert nur sporadisch,
- IP-Adresskonflikt wird gemeldet,
- ARP-Anfragen werden gesendet, aber nicht beantwortet,
- Neighbor Solicitation wird nicht beantwortet,
- IPv6-Adresse bleibt im Zustand `tentative`,
- IPv6 Duplicate Address Detection schlägt fehl,
- falscher statischer Nachbareintrag ist vorhanden,
- Proxy ARP oder Proxy NDP antwortet unerwartet,
- Switchport befindet sich im falschen VLAN,
- WLAN-Client-Isolation verhindert direkte Kommunikation,
- Security-Funktion blockiert ARP- oder NDP-Nachrichten,
- virtuelle Maschinen oder Container verwenden unerwartete Nachbareinträge.

4. Wie wird entschieden, ob ARP für das Ziel oder für das Gateway verwendet wird?

Zuerst wird die ausgewählte Route geprüft.

Windows

```
[RO] Find-NetRoute -RemoteIPAddress 198.51.100.20
```

Linux

```
[RO] ip route get 198.51.100.20
```

macOS

```
[RO] route -n get 198.51.100.20
```

Bewertung

Routenergebnis	Aufzulösender direkter Nachbar
Ziel gilt als direkt verbunden	Ziel-IP-Adresse
Route enthält ein Gateway beziehungsweise Next Hop	Gateway-Adresse
Route verwendet Tunnelinterface	Verhalten abhängig vom Tunnel

Routenergebnis	Aufzulösender direkter Nachbar
Route fehlt	keine reguläre Weiterleitung möglich
Ziel wird fälschlich als lokal behandelt	möglicherweise falsches Präfix

Eine falsche Subnetzmaske kann dazu führen, dass ein Client ARP-Anfragen für ein eigentlich entferntes Ziel sendet.

5. Wie wird die IPv4-Nachbartabelle unter Windows angezeigt?

PowerShell

```
[RO] Get-NetNeighbor -AddressFamily IPv4
```

Übersichtliche Darstellung

```
[RO] Get-NetNeighbor -AddressFamily IPv4 |
    Sort-Object InterfaceIndex, IPAddress |
    Format-Table InterfaceAlias,
                 InterfaceIndex,
                 IPAddress,
                 LinkLayerAddress,
                 State,
                 PolicyStore
```

Ein bestimmter Nachbar

```
[RO] Get-NetNeighbor `
    -InterfaceAlias 'Ethernet' `
    -IPAddress '192.0.2.1'
```

Klassischer Befehl

```
[RO] arp -a
```

Bestimmte IP-Adresse suchen:

```
[RO] arp -a 192.0.2.1
```

Die PowerShell-Ausgabe zeigt zusätzlich den Zustand des Eintrags. `arp -a` unterscheidet hauptsächlich zwischen dynamischen und statischen Einträgen.

6. Welche Neighbor-Zustände zeigt Windows?

Mögliche Zustände von `Get-NetNeighbor`:

Zustand	Bedeutung
`Unreachable`	Nachbar gilt als nicht erreichbar
`Incomplete`	Auflösung wurde begonnen, aber noch nicht abgeschlossen
`Probe`	Erreichbarkeit wird aktiv geprüft
`Delay`	Prüfung wird kurz verzögert
`Stale`	Eintrag ist vorhanden, wurde aber länger nicht bestätigt
`Reachable`	Nachbar wurde kürzlich als erreichbar bestätigt
`Permanent`	statischer beziehungsweise dauerhafter Eintrag
`Unknown`	Zustand konnte nicht eindeutig bestimmt werden

Ein Eintrag im Zustand `Stale` ist nicht automatisch fehlerhaft. Er kann bei der nächsten Verwendung erneut geprüft werden.

Ein dauerhaft `Incomplete` bleibender Eintrag deutet darauf hin, dass die Adressauflösung nicht erfolgreich abgeschlossen wird.

7. Wie wird die IPv4-Nachbartabelle unter Linux angezeigt?

Alle IPv4-Nachbarn

```
[RO] ip -4 neighbour show
```

Kurzform:

```
[RO] ip -4 neigh
```

Bestimmte Schnittstelle

```
[RO] ip -4 neighbour show dev eth0
```

Bestimmte IP-Adresse

```
[RO] ip -4 neighbour show 192.0.2.1
```

Änderungen live beobachten

```
[RO] ip monitor neigh
```

Beenden mit:

```
Strg+C
```

Klassischer ARP-Befehl

```
[RO] arp -an
```

Der ältere Befehl `arp` ist nicht auf jeder Linux-Installation standardmäßig vorhanden. Für moderne Systeme ist `ip neighbour` vorzuziehen.

8. Welche Neighbor-Zustände zeigt Linux?

Zustand	Bedeutung
`INCOMPLETE`	Adressauflösung läuft, aber MAC-Adresse fehlt
`REACHABLE`	Nachbar wurde kürzlich als erreichbar bestätigt
`STALE`	Eintrag ist bekannt, Bestätigung ist aber älter
`DELAY`	Erreichbarkeitsprüfung wird verzögert
`PROBE`	Nachbar wird aktiv geprüft
`FAILED`	Auflösung beziehungsweise Erreichbarkeitsprüfung ist fehlgeschlagen
`NOARP`	für diesen Eintrag wird keine normale Nachbarauflösung durchgeführt

Zustand	Bedeutung
`PERMANENT`	statischer, dauerhafter Eintrag

Beispiel

```
192.0.2.1 dev eth0 lladdr 00:11:22:33:44:01 REACHABLE
```

Bestandteil	Bedeutung
`192.0.2.1`	IPv4-Adresse des Nachbarn
`dev eth0`	verwendete Schnittstelle
`lladdr`	Link-Layer-Adresse folgt
`00:11:22:33:44:01`	MAC-Adresse
`REACHABLE`	aktueller Zustand

Fehlgeschlagener Eintrag

```
192.0.2.80 dev eth0 FAILED
```

Dies bedeutet, dass die Nachbarauflösung beziehungsweise Erreichbarkeitsprüfung fehlgeschlagen ist. Die genaue Ursache kann weiterhin bei VLAN, Zielgerät, Switch, WLAN-Isolation oder Filterung liegen.

9. Wie wird die IPv4-Nachbartabelle unter macOS angezeigt?

Alle ARP-Einträge

```
[RO] arp -an
```

Bestimmte IP-Adresse

```
[RO] arp -n 192.0.2.1
```

Routingtabelle mit Link-Layer-Einträgen

```
[RO] netstat -rn -f inet
```

Beispiel eines vollständigen Eintrags:

```
? (192.0.2.1) at 00:11:22:33:44:01 on en0 ifscope [ethernet]
```

Beispiel eines unvollständigen Eintrags:

```
? (192.0.2.80) at (incomplete) on en0 ifscope [ethernet]
```

Ein unvollständiger Eintrag bedeutet, dass keine verwendbare MAC-Adresse ermittelt wurde.

10. Wie wird ein Nachbareintrag kontrolliert erzeugt?

Wenn noch kein Eintrag vorhanden ist, kann eine normale Kommunikation zum direkten Nachbarn die Auflösung auslösen.

Windows

```
[TEST] Test-Connection 192.0.2.1 -Count 1
```

Danach:

```
[RO] Get-NetNeighbor `
    -InterfaceAlias 'Ethernet' `
    -IPAddress '192.0.2.1'
```

Linux

```
[TEST] ping -c 1 192.0.2.1
```

Danach:

```
[RO] ip neighbour show 192.0.2.1
```

macOS

```
[TEST] ping -c 1 192.0.2.1
```

Danach:

```
[RO] arp -n 192.0.2.1
```

Auch wenn das Ziel ICMP nicht beantwortet, kann durch die lokale Zustellung ein ARP-Eintrag entstehen. Voraussetzung ist, dass das Betriebssystem das Ziel als direkten Nachbarn behandelt.

11. Wie wird ARP mit arping aktiv geprüft?

`arping` sendet aktive ARP-Anfragen auf einer lokalen Ethernetverbindung. Das Werkzeug ist nicht unter jedem Betriebssystem standardmäßig vorhanden.

Linux-Beispiel

```
[TEST][PRIV] sudo arping \
    -I eth0 \
    -c 4 \
    192.0.2.1
```

Option	Bedeutung
`-I eth0`	Schnittstelle
`-c 4`	vier Anfragen
Zieladresse	direkt zu prüfende lokale IPv4-Adresse

Einsatzmöglichkeiten

- direkte lokale Erreichbarkeit prüfen,
- Antwort-MAC-Adresse bestimmen,
- erkennen, ob mehrere Geräte antworten,
- ARP unabhängig von ICMP testen.

Einschränkungen

- funktioniert nur für direkt erreichbare IPv4-Nachbarn,
- prüft kein geroutetes entferntes Ziel,
- kann Sicherheitsüberwachung auslösen,
- verschiedene `arping`-Implementierungen besitzen unterschiedliche Optionen,
- eine Antwort beweist nicht die Funktion höherer Protokolle.

Vor der Verwendung muss die lokale Syntax geprüft werden:

```
[RO] arping --help
```

oder:

```
[RO] man arping
```

12. Wie wird ARP mit Wireshark oder TShark untersucht?

Wireshark-Display-Filter

```
arp
```

Nur Anfragen:

```
arp.opcode == 1
```

Nur Antworten:

```
arp.opcode == 2
```

Bestimmte IPv4-Adresse:

```
arp.src.proto_ipv4 == 192.0.2.1 || arp.dst.proto_ipv4 == 192.0.2.1
```

Capture-Filter

```
arp
```

TShark-Liveanzeige

```
[TEST][PRIV][SENS] tshark \
  -i INTERFACE \
  -f "arp"
```

Zeitlich begrenzte Aufnahme

```
[TEST][PRIV][FILE][SENS] dumpcap \
  -i INTERFACE \
  -f "arp" \
  -a duration:30 \
  -w arp-diagnose.pcapng
```

ARP-Felder anzeigen

```
[RO][SENS] tshark \
  -r arp-diagnose.pcapng \
  -Y "arp" \
  -T fields \
  -e frame.time \
  -e eth.src \
  -e eth.dst \
  -e arp.opcode \
  -e arp.src.proto_ipv4 \
  -e arp.src.hw_mac \
  -e arp.dst.proto_ipv4 \
  -e arp.dst.hw_mac
```

Die lokal verfügbaren Feldnamen können geprüft werden:

```
[RO] tshark -G fields |
    grep -E $'\tarp\.'
```

13. Wie wird eine erfolglose ARP-Auflösung im Paketmitschnitt erkannt?

Typisches Muster:

```
Client → Broadcast: Who has 192.0.2.80?
Client → Broadcast: Who has 192.0.2.80?
Client → Broadcast: Who has 192.0.2.80?
Keine Antwort
```

Mögliche Ursachen:

- Zielsystem ist ausgeschaltet,
- Ziel besitzt eine andere IP-Adresse,
- Ziel befindet sich nicht im selben VLAN,
- Client befindet sich im falschen VLAN,
- Switchport ist falsch konfiguriert,
- WLAN-Client-Isolation ist aktiv,
- Layer-2-Sicherheitsmechanismus blockiert den Verkehr,
- falsche Subnetzmaske lässt ein entferntes Ziel lokal erscheinen,
- virtuelle Bridge oder Netzwerkschnittstelle ist falsch verbunden,
- Ziel antwortet aufgrund eines lokalen Netzwerkproblems nicht.

Wichtiger Gegencheck

Wenn der Client ARP für eine entfernte Zieladresse sendet, muss zuerst Präfix und Route geprüft werden. Die Ursache liegt dann möglicherweise nicht bei ARP, sondern in einer falschen Subnetzkonfiguration.

14. Was ist Gratuitous ARP?

Gratuitous ARP ist eine ARP-Nachricht, bei der ein Gerät eine eigene IPv4-/MAC-Zuordnung ohne vorherige normale Anfrage bekannt gibt oder prüft.

Mögliche Zwecke:

- Erkennung eines Adresskonflikts,
- Aktualisierung von Nachbartabellen,
- Übernahme einer virtuellen IP-Adresse,
- Hochverfügbarkeits-Failover,
- Mitteilung nach einem MAC- oder Portwechsel,
- Aktualisierung von Switch- und Hostinformationen.

Typisches Szenario

```
Firewall A besitzt virtuelle IP 192.0.2.1.
Firewall A fällt aus.
Firewall B übernimmt 192.0.2.1.
Firewall B sendet Gratuitous ARP mit ihrer MAC-Adresse.
```

Clients sollen dadurch die neue Zuordnung lernen.

Viele Gratuitous-ARP-Nachrichten sind nicht automatisch schädlich. Sie müssen im Zusammenhang mit Hochverfügbarkeit, Clusterbetrieb, Virtualisierung und Adresskonflikten bewertet werden.

15. Was ist Proxy ARP?

Beim Proxy ARP antwortet ein Gerät auf eine ARP-Anfrage für eine andere IPv4-Adresse mit seiner eigenen MAC-Adresse.

Vereinfacht:

```
Client fragt:
Wer hat 192.0.2.80?

Router antwortet:
192.0.2.80 befindet sich unter meiner MAC-Adresse.
```

Der Router übernimmt anschließend die Weiterleitung zum eigentlichen Ziel.

Proxy ARP kann bewusst eingesetzt werden, beispielsweise für bestimmte Netzdesigns oder Übergangslösungen. Es kann aber auch Fehlkonfigurationen verbergen.

Hinweise auf Proxy ARP

- mehrere IP-Adressen werden derselben Router-MAC zugeordnet,
- ein vermeintlich lokales Ziel wird über einen Router erreicht,
- Kommunikation funktioniert trotz ungewöhnlicher Subnetzkonfiguration,
- Paketmitschnitt zeigt Antworten eines Routers für fremde IP-Adressen.

Proxy ARP darf nicht ohne Prüfung der Netzwerkarchitektur als Angriff oder Fehlfunktion bewertet werden.

16. Welche Aufgabe erfüllt IPv6 Neighbor Discovery?

IPv6 verwendet kein ARP. Neighbor Discovery arbeitet mit ICMPv6 und übernimmt mehrere Funktionen:

- Auflösung von IPv6-Adresse zu MAC-Adresse,
- Erreichbarkeitsprüfung von Nachbarn,
- Routererkennung,
- Präfixinformationen,

- Duplicate Address Detection,
- Weiterleitung auf einen besseren Router,
- teilweise automatische Adresskonfiguration.

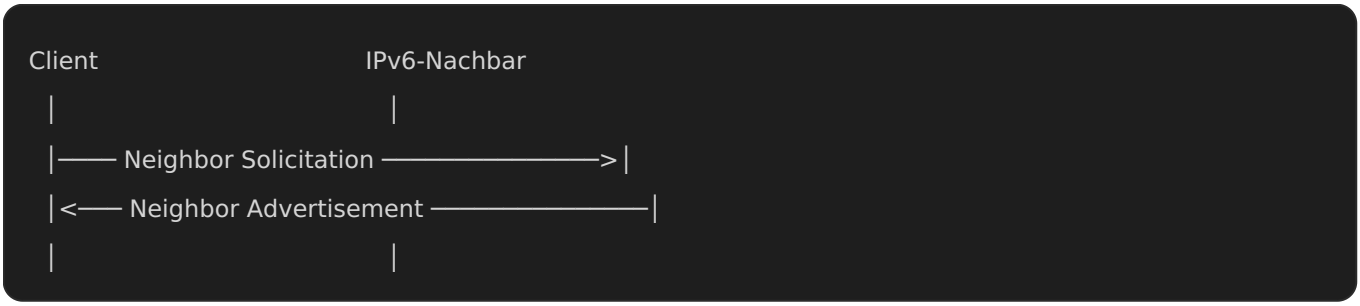
Wichtige ICMPv6-Nachrichten:

Typ	Nachricht	Aufgabe
133	Router Solicitation	Client fordert Routerinformationen an
134	Router Advertisement	Router teilt Präfixe und Parameter mit
135	Neighbor Solicitation	Nachbarauflösung oder Erreichbarkeitsprüfung
136	Neighbor Advertisement	Antwort beziehungsweise Ankündigung eines Nachbarn
137	Redirect	Router weist auf einen besseren nächsten Hop hin

NDP verwendet Multicast statt des aus IPv4 bekannten Broadcasts.

17. Wie funktioniert die IPv6-Nachbarauflösung?

Vereinfachter Ablauf:



Die Neighbor Solicitation wird normalerweise an eine zur Zieladresse gehörende Solicited-Node-Multicast-Adresse gesendet.

Wichtiger Unterschied zu ARP

IPv4	IPv6
ARP	ICMPv6 Neighbor Discovery
Ethernet-Broadcast	IPv6-Multicast
separate ARP-Nachricht	Teil von ICMPv6

IPv4	IPv6
ARP-Tabelle	IPv6-Nachbartabelle

ICMPv6 darf nicht pauschal blockiert werden. Viele ICMPv6-Nachrichten sind für die grundlegende IPv6-Funktion erforderlich.

18. Wie wird die IPv6-Nachbartabelle unter Windows angezeigt?

```
[RO] Get-NetNeighbor -AddressFamily IPv6
```

Übersicht:

```
[RO] Get-NetNeighbor -AddressFamily IPv6 |
    Sort-Object InterfaceIndex, IPAddress |
    Format-Table InterfaceAlias,
                 InterfaceIndex,
                 IPAddress,
                 LinkLayerAddress,
                 State
```

Bestimmte Link-Local-Adresse:

```
[RO] Get-NetNeighbor `
    -InterfaceAlias 'Ethernet' `
    -IPAddress 'fe80::1'
```

Bei Link-Local-Adressen ist die Schnittstelle beziehungsweise Scope-ID entscheidend, da `fe80::/10` auf mehreren Interfaces verwendet werden kann.

Alternative klassische Anzeige

```
[RO] netsh interface ipv6 show neighbors
```

19. Wie wird die IPv6-Nachbartabelle unter Linux angezeigt?

Alle IPv6-Nachbarn

```
[RO] ip -6 neighbour show
```

Bestimmte Schnittstelle

```
[RO] ip -6 neighbour show dev eth0
```

Bestimmte Adresse

```
[RO] ip -6 neighbour show 2001:db8:20::20
```

Änderungen beobachten

```
[RO] ip monitor neigh
```

Router und Standardroute

```
[RO] ip -6 route show default
```

IPv6-Adressen und deren Zustand

```
[RO] ip -6 address show dev eth0
```

Auf folgende Zustände achten:

```
tentative
dadfailed
deprecated
```

`dadfailed` weist darauf hin, dass Duplicate Address Detection für diese Adresse fehlgeschlagen ist.

20. Wie wird die IPv6-Nachbartabelle unter macOS angezeigt?

IPv6-Nachbartabelle

```
[RO] ndp -an
```

Bestimmten Nachbarn anzeigen

```
[RO] ndp -n fe80::1%en0
```

Die Schnittstellenangabe `%en0` ist bei Link-Local-Adressen häufig erforderlich.

IPv6-Routingtabelle

```
[RO] netstat -rn -f inet6
```

IPv6-Konfiguration einer Schnittstelle

```
[RO] ifconfig en0
```

Zu prüfen sind:

- Link-Local-Adresse,
- globale beziehungsweise interne IPv6-Adressen,
- Präfixlängen,
- Adresszustände,
- Standardrouter,
- Nachbareinträge und deren MAC-Adressen.

21. Wie wird IPv6 Neighbor Discovery mit Wireshark untersucht?

Alle Neighbor-Discovery-Nachrichten

```
icmpv6.type >= 133 && icmpv6.type <= 137
```

Router Solicitation

```
icmpv6.type == 133
```

Router Advertisement

```
icmpv6.type == 134
```

Neighbor Solicitation

```
icmpv6.type == 135
```

Neighbor Advertisement

```
icmpv6.type == 136
```

Redirect

```
icmpv6.type == 137
```

Bestimmte IPv6-Adresse

```
ipv6.addr == 2001:db8:20::20
```

Capture-Filter für relevante ICMPv6-Nachrichten

```
icmp6
```

Zeitlich begrenzte Aufnahme

```
[TEST][PRIV][FILE][SENS] dumpcap \
  -i INTERFACE \
  -f "icmp6" \
  -a duration:30 \
  -w ipv6-nd.pcapng
```

TShark-Auswertung

```
[RO][SENS] tshark \
  -r ipv6-nd.pcapng \
  -Y "icmpv6.type >= 133 && icmpv6.type <= 137" \
```

```
-T fields \
-e frame.time \
-e eth.src \
-e eth.dst \
-e ipv6.src \
-e ipv6.dst \
-e icmpv6.type
```

22. Was ist Duplicate Address Detection bei IPv6?

Bevor eine neue IPv6-Adresse regulär verwendet wird, prüft der Host normalerweise, ob sie bereits auf dem lokalen Link verwendet wird.

Vereinfacht:

```
Neuer Host
  → Neighbor Solicitation für die eigene geplante Adresse
  → keine widersprechende Antwort: Adresse kann verwendet werden
```

Antwortet ein anderes Gerät, kann die Adresse als doppelt erkannt werden.

Mögliche Zustände

Zustand	Bedeutung
`tentative`	Prüfung läuft
`preferred`	Adresse kann normal verwendet werden
`deprecated`	Adresse wird nicht mehr für neue Verbindungen bevorzugt
`dadfailed` beziehungsweise `Duplicate`	Konflikt erkannt

Mögliche Ursachen eines DAD-Fehlers

- tatsächlich doppelte statische IPv6-Adresse,
- fehlerhafte virtuelle Netzwerkkonfiguration,
- Loop oder reflektierte Pakete,
- fehlerhaftes Proxy-NDP-Verhalten,
- duplizierte virtuelle Maschine mit identischer Konfiguration,
- Sicherheitsgerät beantwortet Anfragen unerwartet.

Ein DAD-Fehler darf nicht durch dauerhaftes Abschalten der Konflikterkennung verdeckt werden.

23. Wie werden Router Advertisements in die Diagnose einbezogen?

Router Advertisements können unter anderem mitteilen:

- verfügbare Router,
- Präfixinformationen,
- Präfixlänge,
- Gültigkeitsdauer,
- bevorzugte Dauer,
- ob SLAAC verwendet werden kann,
- Hinweise auf DHCPv6,
- MTU,
- Routeninformationen,
- weitere IPv6-Parameter.

Typische Fehlerbilder

- Client erhält nur Link-Local-Adresse,
- IPv6-Standardroute fehlt,
- falsches Präfix wird angekündigt,
- nicht autorisierter Router sendet Advertisements,
- mehrere Router kündigen widersprüchliche Informationen an,
- Router Advertisement erreicht bestimmte VLANs nicht,
- ICMPv6 wird gefiltert,
- Präfix ist abgelaufen oder falsch konfiguriert.

Windows-Routen

```
[RO] Get-NetRoute -AddressFamily IPv6
```

Linux

```
[RO] ip -6 route
```

macOS

```
[RO] netstat -rn -f inet6
```

Ein vorhandener DHCPv6-Server ersetzt nicht automatisch die Router Advertisements für die Standardrouterinformation.

24. Warum dürfen Nachbartabellen nicht vorschnell geleert werden?

Das Leeren einer Nachbartabelle:

- verändert den Diagnosezustand,
- entfernt möglicherweise den Beleg einer falschen Zuordnung,
- erzwingt neue ARP- oder NDP-Auflösungen,
- kann Verbindungen kurzfristig unterbrechen,
- behebt eine falsche Zuordnung möglicherweise nur vorübergehend,
- beseitigt nicht die eigentliche Ursache.

Vorher sollten gespeichert werden:

Windows

```
[RO][FILE][SENS] Get-NetNeighbor |
    Export-Csv 'C:\Temp\nachbartabelle-vorher.csv' `
    -NoTypeInformation `
    -Encoding UTF8
```

Linux

```
[RO][FILE][SENS] ip neighbour show \
    > /tmp/nachbartabelle-vorher.txt
```

macOS

```
[RO][FILE][SENS] arp -an \
    > /tmp/arp-vorher.txt
```

```
[RO][FILE][SENS] ndp -an \
    > /tmp/ndp-vorher.txt
```

Die Speicherorte müssen den betrieblichen Datenschutz- und Sicherheitsvorgaben entsprechen.

25. Welche eingreifenden Befehle existieren?

Windows – IPv4-Nachbartabelle leeren

```
[PRIV][CHANGE][DISRUPT] netsh interface ip delete arpcache
```

Linux – dynamische IPv4-Nachbarn einer Schnittstelle leeren

```
[PRIV][CHANGE][DISRUPT] sudo ip -4 neighbour flush dev eth0
```

Linux – IPv6-Nachbarn einer Schnittstelle leeren

```
[PRIV][CHANGE][DISRUPT] sudo ip -6 neighbour flush dev eth0
```

macOS – einzelnen ARP-Eintrag entfernen

```
[PRIV][CHANGE][DISRUPT] sudo arp -d 192.0.2.1
```

macOS – einzelnen IPv6-Nachbareintrag entfernen

```
[PRIV][CHANGE][DISRUPT] sudo ndp -d fe80::1%en0
```

> Diese Befehle sind keine ersten Diagnoseschritte. Bei Remotezugriff kann insbesondere das Entfernen des Gatewayeintrags die aktive Verbindung kurzfristig beeinträchtigen. Syntax und unterstützte Optionen müssen lokal mit der jeweiligen Hilfeseite geprüft werden.

26. Wie werden statische Nachbareinträge bewertet?

Statische Einträge können bewusst eingerichtet sein, beispielsweise für:

- besondere Appliances,
- Hochverfügbarkeitslösungen,
- Sicherheitskonzepte,
- Testumgebungen,
- feste Nachbarzuordnungen.

Sie können jedoch veraltet sein, wenn:

- Netzwerkkarte ersetzt wurde,
- virtuelle Maschine verschoben wurde,
- Failover stattgefunden hat,
- Gerät eine neue MAC-Adresse verwendet,
- Netzwerkarchitektur geändert wurde.

Windows

```
[RO] Get-NetNeighbor |
    Where-Object State -eq 'Permanent'
```

Linux

```
[RO] ip neighbour show nud permanent
```

macOS

```
[RO] arp -an
```

Statische Einträge dürfen nicht gelöscht werden, bevor Eigentümer, Zweck, Konfigurationsquelle und Rückweg geklärt sind.

27. Wie werden ARP-Spoofing und Neighbor-Discovery-Manipulation erkannt?

Mögliche Hinweise:

- Gateway-IP wechselt unerwartet zwischen MAC-Adressen,
- eine fremde MAC-Adresse beansprucht viele IP-Adressen,
- unerwartete Gratuitous-ARP-Nachrichten,
- nicht autorisierte Router Advertisements,
- mehrere Geräte antworten auf dieselbe Adresse,
- Verbindung wird über ein unbekanntes Gerät umgeleitet,
- Zertifikatswarnungen treten gleichzeitig auf,
- Netzwerküberwachung meldet Dynamic-ARP-Inspection- oder RA-Guard-Verstöße.

Sicheres Vorgehen

1. aktuelle Nachbartabelle sichern,
2. Zeitpunkt dokumentieren,

3. Switch-MAC-Tabelle und Portzuordnung prüfen,
4. DHCP- und Netzwerkdokumentation vergleichen,
5. Paketmitschnitt nur mit Freigabe erstellen,
6. Hochverfügbarkeits- und Proxyfunktionen ausschließen,
7. Informationssicherheit einbeziehen,
8. verdächtiges Gerät nicht unkoordiniert verändern.

Eine gemeinsame MAC-Adresse für mehrere IP-Adressen ist nicht automatisch ein Angriff. Router, Load Balancer, Firewalls, Proxy ARP und Cluster können dieses Muster beabsichtigt erzeugen.

28. Wie wird zwischen Client-, VLAN- und Zielproblem unterschieden?

Beobachtung	Wahrscheinlichere Richtung
nur ein Client erhält keine ARP-Antwort	Client, Port oder lokale Sicherheitsregel
mehrere Clients im VLAN betroffen	VLAN, Switch oder Zielsystem
andere VLANs erreichen das Ziel	betroffenes VLAN oder Gatewayinterface
ARP-Anfrage verlässt Client nicht	Clientstack oder Schnittstelle
Anfrage sichtbar, Antwort fehlt	Ziel, VLAN-Pfad oder Filter
Antwort erreicht Switch, aber nicht Client	Port, WLAN oder Sicherheitsfunktion
falsche MAC antwortet	Proxy, Konflikt oder Manipulation
Gateway wird aufgelöst, Ziel nicht erreichbar	Problem liegt wahrscheinlich nach Layer 2
Ziel wird fälschlich per ARP gesucht	falsches Präfix oder falsche Route
IPv6 NS ohne NA	Ziel, VLAN, Filter oder NDP-Konfiguration
nur IPv6 betroffen	ICMPv6, RA, NDP oder IPv6-VLAN-Pfad

29. Welche typischen Fehlinterpretationen müssen vermieden werden?

Beobachtung	Falscher Schluss	Richtige Einordnung
ARP-Tabelle ist leer	Netzwerk ist defekt	möglicherweise wurde noch kein lokaler Nachbar angesprochen
Eintrag ist `Stale`	Ziel ist nicht erreichbar	Eintrag wird bei Nutzung erneut geprüft
Eintrag ist `Incomplete`	Ziel ist ausgeschaltet	VLAN, Präfix und Filter bleiben mögliche Ursachen

Beobachtung	Falscher Schluss	Richtige Einordnung
entfernte Ziel-IP fehlt in ARP	Fehler liegt vor	nur der lokale Next Hop wird benötigt
viele IPs haben dieselbe MAC	Angriff	Router, Proxy ARP oder Cluster möglich
MAC-Adresse wechselt	Angriff	Failover oder Gerätewechsel möglich
Ping funktioniert nicht	ARP funktioniert nicht	Nachbartabelle getrennt prüfen
ARP funktioniert	Anwendung funktioniert	nur lokale Adressauflösung bestätigt
IPv6 hat keine ARP-Tabelle	IPv6 benötigt keine Auflösung	IPv6 verwendet NDP
ICMPv6 wird blockiert	nur Ping ist betroffen	zentrale IPv6-Funktionen können ausfallen
Nachbartabelle wurde geleert und es funktioniert	Ursache wurde behoben	Problem kann nur vorübergehend verdeckt sein
Gratuitous ARP sichtbar	Manipulation	Konfliktprüfung oder Failover möglich

30. Wie sieht der systematische Prüfablauf aus?

Schritt	Prüfung
1	IP-Adresse und Präfix des Clients bestätigen
2	ausgewählte Route zum Ziel bestimmen
3	direkt aufzulösenden Nachbarn identifizieren
4	vorhandene Nachbartabelle unverändert sichern
5	Zustand und MAC-Adresse des Eintrags prüfen
6	mit funktionierendem Referenzclient vergleichen
7	normale Kommunikation zum direkten Nachbarn auslösen
8	Nachbartabelle erneut prüfen
9	bei Bedarf ARP beziehungsweise NDP kontrolliert mitschneiden
10	Anfrage und Antwort auf Client- und Netzseite verfolgen
11	Switchport, VLAN und MAC-Zuordnung prüfen
12	Proxy-, Cluster- und Hochverfügbarkeitsfunktionen berücksichtigen
13	Konflikt oder Manipulationsverdacht eskalieren

Schritt	Prüfung
14	Tabelle nur nach Beweissicherung gezielt verändern
15	ursprüngliches Fehlerbild erneut testen
16	Ursache und Ergebnis dokumentieren

Merksatz

Route bestimmen → direkten Nachbarn bestimmen

→ Tabelle prüfen → Anfrage verfolgen → Antwort verfolgen

31. Kompakte Befehlsübersicht für Windows, Linux und macOS

Aufgabe	Windows	Linux	macOS
IPv4-Nachbarn	`[RO] Get-NetNeighbor -AddressFamily IPv4`	`[RO] ip -4 neighbour`	`[RO] arp -an`
IPv6-Nachbarn	`[RO] Get-NetNeighbor -AddressFamily IPv6`	`[RO] ip -6 neighbour`	`[RO] ndp -an`
einzelner IPv4-Nachbar	`[RO] Get-NetNeighbor -IPAddress ZIEL`	`[RO] ip neighbour show ZIEL`	`[RO] arp -n ZIEL`
einzelne IPv6-Adresse	`[RO] Get-NetNeighbor -IPAddress ZIEL`	`[RO] ip -6 neighbour show ZIEL`	`[RO] ndp -n ZIEL%INTERFACE`
Route zum Ziel	`[RO] Find-NetRoute -RemoteIPAddress ZIEL`	`[RO] ip route get ZIEL`	`[RO] route -n get ZIEL`
Nachbaränderungen live	PowerShell wiederholt abfragen	`[RO] ip monitor neigh`	wiederholt `arp` beziehungsweise `ndp`
ARP aktiv testen	normales `Test-Connection`	`[TEST][PRIV] sudo arping -I INTERFACE -c 4 ZIEL`	abhängig von installiertem Werkzeug
ARP mitschneiden	`[TEST][PRIV][SENS] tshark -i INTERFACE -f "arp"`	gleicher Befehl	gleicher Befehl
NDP mitschneiden	`[TEST][PRIV][SENS] tshark -i INTERFACE -f "icmp6"`	gleicher Befehl	gleicher Befehl
ARP-Cache leeren	`[PRIV][CHANGE][DISRUPT] netsh interface ip delete arpcache`	`[PRIV][CHANGE][DISRUPT] sudo ip -4 neigh flush dev INTERFACE`	`[PRIV][CHANGE][DISRUPT] sudo arp -d ZIEL`
IPv6-Nachbarn leeren	nur gezielt nach lokaler Dokumentation	`[PRIV][CHANGE][DISRUPT] sudo ip -6 neigh flush dev INTERFACE`	`[PRIV][CHANGE][DISRUPT] sudo ndp -d ZIEL%INTERFACE`

Die Platzhalter `ZIEL` und `INTERFACE` müssen durch vorher eindeutig bestimmte Werte ersetzt werden.

32. Dokumentationsvorlage

Ticketnummer:

Prüfzeitpunkt:

Zeitzone:

Betroffener Client:

Betriebssystem:

Schnittstelle:

MAC-Adresse:

VLAN:

IP-KONFIGURATION

Client-IPv4:

IPv4-Präfix:

Client-IPv6:

IPv6-Präfix:

Standardgateway IPv4:

Standardrouter IPv6:

ZIEL

Zielname:

Ziel-IPv4:

Ziel-IPv6:

Ziel laut Präfix lokal: Ja / Nein

Ausgewählte Route:

Ausgewählte Quelladresse:

Next Hop:

Direkt aufzulösender Nachbar:

NACHBARTABELLE VOR DEM TEST

IPv4-Nachbar:

MAC-Adresse:

Schnittstelle:

Zustand:

Dynamisch oder statisch:

IPv6-Nachbar:

MAC-Adresse:

Schnittstelle:

Zustand:

Dynamisch oder statisch:

AKTIVER TEST

Verwendeter Test:

Startzeit:

Endzeit:

Anfragen gesendet:

Antworten empfangen:

PAKETMITSCHNITT

ARP Request sichtbar:

ARP Reply sichtbar:

Neighbor Solicitation sichtbar:

Neighbor Advertisement sichtbar:

Router Advertisement sichtbar:

Quell-MAC:

Antwort-MAC:

Mehrere Antworten:

Gratuitous ARP:

Proxy ARP vermutet:

DAD fehlgeschlagen:

NETZWERKSEITE

Switch:

Switchport:

Port-VLAN:

Gelernte Client-MAC:

Gelernte Ziel-MAC:

MAC wechselt zwischen Ports:

Port-Security-Ereignisse:

ARP-/NDP-Schutzereignisse:

```
REFERENZCLIENT

Hostname:
Gleiches VLAN:
Nachbar-IP:
Nachbar-MAC:
Nachbarzustand:
Relevante Abweichungen:

Arbeitshypothese:
Begründung:
Originaltabelle gesichert:
Durchgeführte Änderung:
Rückweg:
Abschlussprüfung:
Ermittelte Ursache:
Sicherheitseskalation erforderlich: Ja / Nein
```

33. Offizielle Quellen und weiterführende Dokumentation

Microsoft

- Get-NetNeighbor
- Find-NetRoute
- netsh interface
- IPv6 Neighbor Discovery

Linux

- ip-neighbour – Linux Manual Page
- ip-monitor – Linux Manual Page
- ip-route – Linux Manual Page
- Lokale Befehlsreferenz: `man arping`

Apple

- Lokale Befehlsreferenzen: `man arp`, `man ndp`, `man route`, `man netstat` und `man ifconfig`

Wireshark

- ARP Display Filter Reference
- ICMPv6 Display Filter Reference
- dumpcap Manual Page
- tshark Manual Page

Standards

- RFC 826 – Address Resolution Protocol
- RFC 5227 – IPv4 Address Conflict Detection
- RFC 4861 – Neighbor Discovery for IPv6
- RFC 4862 – IPv6 Stateless Address Autoconfiguration
- RFC 6980 – Security Implications of IPv6 Fragmentation with NDP

> Nachbarzustände, Zeitlimits und verfügbare Diagnosefelder hängen vom Betriebssystem, Treiber und Netzwerkdesign ab. Eine fehlende Antwort muss immer zusammen mit Route, Präfix, VLAN und tatsächlichem Messpunkt bewertet werden.