3.4 DHCP-Fehler analysieren

DHCP stellt Clients automatisch Netzwerkparameter zur Verfügung. Dazu gehören typischerweise IP-Adresse, Präfix beziehungsweise Subnetzmaske, Standardgateway, DNS-Server, DNS-Suchdomäne und Lease-Dauer.

Eine erfolgreiche DHCP-Zuweisung beweist jedoch nicht automatisch, dass alle übermittelten Parameter korrekt sind. Ein Client kann eine technisch gültige Adresse aus dem falschen Subnetz oder von einem nicht vorgesehenen DHCP-Server erhalten.

> **Grundregel:** Zuerst die vorhandene Lease und deren Herkunft dokumentieren. Erst danach darf eine Freigabe oder Erneuerung durchgeführt werden.

---

1. Welche Symptome sprechen für ein DHCP-Problem?

- IPv4-Adresse aus `169.254.0.0/16`,
- keine reguläre IPv4-Adresse,
- Adresse aus einem falschen Subnetz,
- falsches Standardgateway,
- falsche DNS-Server,
- fehlende DHCP-Optionen,
- Lease kann nicht erneuert werden,
- Verbindung funktioniert erst nach langer Wartezeit,
- neue Geräte erhalten keine Adresse,
- bestehende Geräte funktionieren noch,
- Fehler betrifft nur ein VLAN,
- Fehler betrifft nur einen Standort,
- ein Client erhält wechselnde Konfigurationen,
- DHCP-Adresskonflikt wird gemeldet,
- Lease-Dauer ist ungewöhnlich kurz,
- nicht autorisierter DHCP-Server antwortet,
- DHCP funktioniert über LAN, aber nicht über WLAN,
- DHCP funktioniert im Server-VLAN, aber nicht über den Relay-Agenten.

2. Welche Informationen müssen vor einer Veränderung erfasst werden?

Information	Beispiel
Clienthostname	`CLIENT-023`

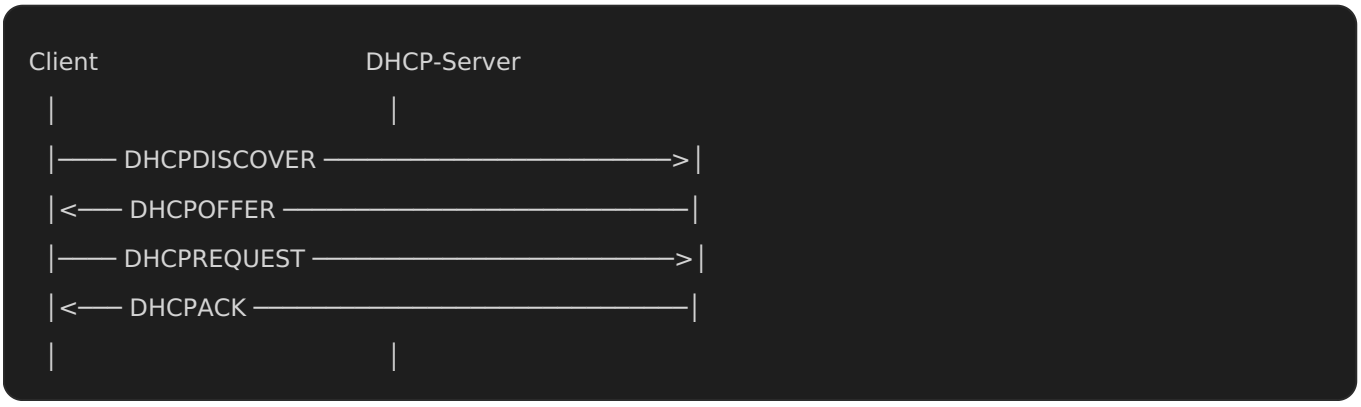
Information	Beispiel
MAC-Adresse	`00-11-22-33-44-55`
Schnittstelle	Ethernet
VLAN	20
aktuelle IPv4-Adresse	`192.0.2.23`
Präfix beziehungsweise Maske	`/24` beziehungsweise `255.255.255.0`
Standardgateway	`192.0.2.1`
DNS-Server	`192.0.2.53`, `192.0.2.54`
DHCP aktiviert	Ja
DHCP-Server	`192.0.2.10`
Lease erhalten	`2026-07-31 08:00 CEST`
Lease läuft ab	`2026-08-01 08:00 CEST`
erwarteter DHCP-Bereich	`192.0.2.20–192.0.2.200`
Fehlerbeginn	`2026-07-31 09:42 CEST`

Vor einer Lease-Erneuerung sollten zusätzlich gespeichert werden:

- vollständige IP-Konfiguration,
- Routingtabelle,
- DNS-Konfiguration,
- DHCP-Clientprotokolle,
- relevante Netzwerkereignisse,
- Vergleichsdaten eines funktionierenden Clients.

3. Wie funktioniert DHCPv4 grundsätzlich?

Der klassische erstmalige DHCPv4-Ablauf wird häufig als DORA bezeichnet:



Nachricht	Absender	Bedeutung
`DHCPDISCOVER`	Client	sucht verfügbare DHCP-Server
`DHCPOFFER`	Server	bietet Adresse und Parameter an
`DHCPREQUEST`	Client	fordert ein bestimmtes Angebot an
`DHCPACK`	Server	bestätigt die Lease
`DHCPNAK`	Server	lehnt angeforderte Konfiguration ab
`DHCPDECLINE`	Client	meldet angebotene Adresse als problematisch
`DHCPRELEASE`	Client	gibt eine Lease frei
`DHCPINFORM`	Client	fordert Optionen an, ohne eine neue Adresse zu beziehen

DHCPv4 verwendet grundsätzlich:

Richtung	UDP-Port
Server	67
Client	68

Die erste Kommunikation erfolgt häufig per Broadcast, weil der Client zunächst noch keine reguläre IPv4-Adresse und keinen bekannten DHCP-Server besitzt.

4. Wie wird eine bestehende DHCP-Konfiguration unter Windows geprüft?

Vollständige Konfiguration

```
[RO][SENS] ipconfig /all
```

Zu prüfen sind insbesondere:

```
DHCP aktiviert
IPv4-Adresse
Subnetzmaske
Lease erhalten
Lease läuft ab
Standardgateway
DHCP-Server
```

```
DNS-Server
Verbindungsspezifisches DNS-Suffix
```

DHCP-Status der Schnittstellen

```
[RO] Get-NetIPInterface -AddressFamily IPv4 |
    Select-Object InterfaceAlias,
                  InterfaceIndex,
                  Dhcp,
                  ConnectionState,
                  InterfaceMetric
```

Adressursprung

```
[RO] Get-NetIPAddress -AddressFamily IPv4 |
    Select-Object InterfaceAlias,
                  InterfaceIndex,
                  IPAddress,
                  PrefixLength,
                  PrefixOrigin,
                  SuffixOrigin,
                  AddressState
```

Konfiguration sichern

```
[RO][FILE][SENS] ipconfig /all |
    Out-File 'C:\Temp\ipconfig-vor-dhcp-test.txt'
```

```
[RO][FILE][SENS] Get-NetIPConfiguration |
    Format-List * |
    Out-File 'C:\Temp\netipconfig-vor-dhcp-test.txt'
```

Die Verzeichnisse müssen vorhanden und für Diagnoseinformationen freigegeben sein.

5. Wie werden DHCP-Clientereignisse unter Windows gelesen?

Verfügbare DHCP-bezogene Protokolle suchen

```
[RO] Get-WinEvent -ListLog '*DHCP*' |
    Select-Object LogName,
                  IsEnabled,
                  RecordCount
```

Je nach Windows-Version und aktivierten Kanälen können unter anderem DHCP-Client-Protokolle unter folgendem Bereich vorhanden sein:

```
Anwendungs- und Dienstprotokolle
→ Microsoft
  → Windows
    → Dhcp-Client
```

Aktivierte DHCP-Protokolle auslesen

```
[RO] Get-WinEvent -ListLog '*DHCP*' |
    Where-Object {
        $_.IsEnabled -and $_.RecordCount -gt 0
    } |
    ForEach-Object {
        Get-WinEvent -LogName $_.LogName -MaxEvents 50 -ErrorAction SilentlyContinue
    } |
    Sort-Object TimeCreated -Descending |
    Select-Object TimeCreated,
                  LogName,
                  Id,
                  LevelDisplayName,
                  ProviderName,
                  Message
```

Systemprotokoll nach DHCP-Meldungen durchsuchen

```
[RO] Get-WinEvent -LogName System -MaxEvents 1000 |
    Where-Object {
        $_.ProviderName -Match 'Dhcp' -or
```

```
    $_.Message -Match 'DHCP'
} |
Sort-Object TimeCreated -Descending |
Select-Object TimeCreated,
              Id,
              LevelDisplayName,
              ProviderName,
              Message
```

Protokollname, Provider und Ereignis-ID können sich zwischen Windows-Versionen unterscheiden. Deshalb sollte zuerst mit `Get-WinEvent -ListLog '*DHCP*'` geprüft werden, welche Kanäle tatsächlich vorhanden sind.

6. Wie wird eine bestehende DHCP-Konfiguration unter Linux geprüft?

Grundlegende IP-Konfiguration

```
[RO] ip -4 address
```

```
[RO] ip -4 route
```

Mit NetworkManager

Gerätestatus:

```
[RO] nmcli device status
```

Ausführliche Gerätedaten:

```
[RO][SENS] nmcli device show eth0
```

Aktive Verbindungen:

```
[RO] nmcli connection show --active
```

Verbindungsprofil:

```
[RO][SENS] nmcli connection show "VERBINDUNGSNAME"
```

Zu prüfen sind insbesondere Eigenschaften wie:

- IPv4-Konfigurationsmethode,
- aktuelle IPv4-Adresse,
- Gateway,
- DNS-Server,
- DHCP-Server beziehungsweise DHCP-Optionen,
- Domänen- und Suchinformationen.

Die tatsächlich verfügbaren Felder hängen von NetworkManager-Version und Backend ab.

Mit systemd-networkd

```
[RO] networkctl status eth0
```

```
[RO] networkctl status --all
```

Lease-Dateien

Speicherort und Format von Lease-Dateien hängen von Distribution und Netzwerkmanager ab. Es sollte nicht von einem festen Pfad ausgegangen werden. Vorhandene Dateien können gesucht werden, ohne sie zu verändern:

```
[RO][PRIV][SENS] sudo find /run /var/lib \
    -maxdepth 4 \
    -type f \
    \( -iname '*lease*' -o -iname '*dhcp*' \) \
    2>/dev/null
```

Gefundene Dateien dürfen nicht gelöscht oder verändert werden, bevor Netzwerkmanager und Zweck eindeutig bestimmt wurden.

7. Wie werden DHCP-Clientprotokolle unter Linux geprüft?

NetworkManager

```
[RO][PRIV] sudo journalctl -b -u NetworkManager
```

Nach DHCP-Meldungen filtern:

```
[RO][PRIV] sudo journalctl -b -u NetworkManager |
    grep -Ei 'dhcp|lease|offer|request|ack|nak|timeout'
```

systemd-networkd

```
[RO][PRIV] sudo journalctl -b -u systemd-networkd
```

Nach DHCP-Meldungen filtern:

```
[RO][PRIV] sudo journalctl -b -u systemd-networkd |
    grep -Ei 'dhcp|lease|offer|request|ack|nak|timeout'
```

Allgemeine Protokollsuche

```
[RO][PRIV] sudo journalctl -b |
    grep -Ei 'dhcp|lease|dhclient|NetworkManager|systemd-networkd'
```

Kernelmeldungen zur Schnittstelle

```
[RO][PRIV] sudo journalctl -k -b |
    grep -E 'eth0|link.*(up|down)|carrier'
```

Vor der Interpretation muss bekannt sein, welcher Dienst die Schnittstelle verwaltet. Meldungen eines installierten, aber nicht verwendeten DHCP-Clients sind möglicherweise irrelevant.

8. Wie wird eine bestehende DHCP-Konfiguration unter macOS geprüft?

Netzwerkdienste auflisten

```
[RO] networksetup -listallnetworkservices
```

Hardwareports zuordnen

```
[RO] networksetup -listallhardwareports
```

Konfiguration eines Dienstes

```
[RO] networksetup -getinfo "Ethernet"
```

DHCP-Paketinformationen einer Schnittstelle

```
[RO][SENS] ipconfig getpacket en0
```

Diese Ausgabe kann unter anderem enthalten:

- angebotene IPv4-Adresse,
- Subnetzmaske,
- Router,
- DHCP-Serverkennung,
- Lease-Dauer,
- DNS-Server,
- Domainnamen,
- weitere DHCP-Optionen.

Nur die aktuelle IPv4-Adresse

```
[RO] ipconfig getifaddr en0
```

DNS-Konfiguration

```
[RO][SENS] scutil --dns
```

Systemprotokolle nach DHCP durchsuchen

```
[RO] log show \
    --last 1h \
    --style compact \
    --predicate 'process == "bootp" OR eventMessage CONTAINS[c] "DHCP"'
```

Je nach macOS-Version können Prozessname, Subsystem und verfügbare Meldungen abweichen. Eine leere Ausgabe beweist nicht, dass kein DHCP-Vorgang stattgefunden hat.

9. Wie wird geprüft, ob der Client überhaupt DHCP verwendet?

Ein Client kann eine statische Adresse besitzen und deshalb keine reguläre DHCP-Lease anfordern.

Windows

```
[RO] Get-NetIPInterface -AddressFamily IPv4 |
    Select-Object InterfaceAlias,
                  Dhcp,
                  ConnectionState
```

Linux mit NetworkManager

```
[RO] nmcli connection show "VERBINDUNGSNAME" |
    grep -E '^ipv4\.method'
```

Typische Werte:

Wert	Bedeutung
`auto`	automatische IPv4-Konfiguration, typischerweise DHCP
`manual`	statische Konfiguration
`disabled`	IPv4 deaktiviert
`shared`	geteilte Verbindung mit eigener Adressbereitstellung

macOS

```
[RO] networksetup -getinfo "Ethernet"
```

Die Ausgabe zeigt die verwendete Konfigurationsmethode.

Prüffragen

- Soll diese Schnittstelle DHCP verwenden?
- Ist möglicherweise ein altes statisches Profil aktiv?

- Verwaltet eine zusätzliche Software die Konfiguration?
- Ist ein VPN- oder MDM-Profil beteiligt?
- Wird die richtige physische oder virtuelle Schnittstelle untersucht?

10. Wie wird eine DHCPv4-Störung anhand der Nachrichten eingegrenzt?

Sichtbare Nachrichten	Mögliche Untersuchungsrichtung
kein `DHCPDISCOVER`	DHCP-Client, Schnittstelle oder Capture-Punkt prüfen
`DISCOVER`, aber kein `OFFER`	VLAN, Relay, Filter, Server oder Bereich prüfen
mehrere `OFFER`	mehrere DHCP-Server vorhanden; Berechtigung prüfen
`OFFER`, aber kein `REQUEST`	Clientzustand oder nicht gewähltes Angebot prüfen
`REQUEST`, aber kein `ACK`	Server, Relay, Filter oder Adressprüfung untersuchen
`REQUEST` gefolgt von `NAK`	angeforderte Adresse ist für Server nicht gültig
`ACK` mit falschen Optionen	Scope-, Policy- oder Optionskonfiguration prüfen
wiederholte DORA-Sequenzen	Lease wird nicht übernommen oder Verbindung bricht ab
`DECLINE`	Client vermutet Adresskonflikt
Lease funktioniert nur im Server-VLAN	DHCP-Relay oder Routing prüfen

Die Interpretation muss anhand von Transaktions-ID, Client-MAC beziehungsweise Client-Identifier und Zeitstempel erfolgen. Gleichzeitige DHCP-Vorgänge anderer Clients dürfen nicht verwechselt werden.

11. Wie wird DHCP-Verkehr sicher mit Wireshark oder TShark geprüft?

Wireshark-Display-Filter für DHCPv4

```
dhcp
```

Je nach Wireshark-Version wird auch weiterhin der ältere Protokollname `bootp` in Feldern oder Filtern verwendet. Der folgende Filter ist deshalb ebenfalls verbreitet:

```
bootp
```

Nur DHCPv4-Ports

```
udp.port == 67 || udp.port == 68
```

TShark-Liveanzeige

```
[TEST][PRIV][SENS] tshark \
  -i INTERFACE \
  -f "udp port 67 or udp port 68"
```

Zeitlich begrenzte Aufnahme mit dumpcap

```
[TEST][PRIV][FILE][SENS] dumpcap \
  -i INTERFACE \
  -f "udp port 67 or udp port 68" \
  -a duration:60 \
  -w dhcp-test.pcapng
```

DHCP-Nachrichtentypen aus einer Datei anzeigen

```
[RO][SENS] tshark \
  -r dhcp-test.pcapng \
  -Y "bootp" \
  -T fields \
  -e frame.time \
  -e eth.src \
  -e ip.src \
  -e ip.dst \
  -e bootp.option.dhcp
```

Feldnamen können sich zwischen Wireshark-Versionen ändern. Die lokal verfügbaren Felder sollten geprüft werden:

```
[RO] tshark -G fields |
    grep -Ei 'dhcp|bootp'
```

Ein Paketmitschnitt darf nur mit Freigabe und unter Beachtung der Regeln aus Seite 2.14 erstellt werden.

12. Wie wird ein fehlendes DHCPOFFER untersucht?

Wenn der Client `DHCPDISCOVER` sendet, aber kein Angebot erhält, wird der Kommunikationsweg geprüft:

```
Client
  → Switchport
    → Client-VLAN
      → DHCP-Relay oder direktes Broadcastsegment
        → Netzwerkpfad
          → DHCP-Server
```

Prüffragen

1. Ist der Client im richtigen VLAN?
2. Wird das `DHCPDISCOVER` am Client gesendet?
3. Wird es am Switch beziehungsweise Relay empfangen?
4. Ist für dieses VLAN ein DHCP-Relay konfiguriert?
5. Verwendet das Relay die richtige Serveradresse?
6. Ist der DHCP-Server vom Relay aus erreichbar?
7. Ist UDP 67/68 auf dem Weg erlaubt?
8. Existiert ein aktiver DHCP-Bereich für das Clientnetz?
9. Besitzt der Bereich noch freie Adressen?
10. Ist der Serverdienst aktiv?
11. Wird die Anfrage durch eine Policy abgelehnt?
12. Enthält die Relay-Anfrage die erwarteten Informationen?
13. Wird ein Angebot zurückgesendet?
14. Erreicht das Angebot wieder den Client?

Wenn nur ein Client betroffen ist, während andere Clients am selben Anschlussbereich neue Leases erhalten, ist ein vollständiger Ausfall des DHCP-Servers weniger wahrscheinlich.

13. Welche Aufgabe hat ein DHCP-Relay?

IPv4-Broadcasts werden normalerweise nicht durch Router weitergeleitet. Befindet sich der DHCP-Server in einem anderen Netz, nimmt ein DHCP-Relay die Clientanfrage entgegen und leitet sie an den Server weiter.

```
Client-VLAN 20
192.0.2.0/24
```

```
│
├─ DHCPDISCOVER als Broadcast
│
└─ Gateway/DHCP-Relay
   │
   └─ Weiterleitung zum DHCP-Server
      198.51.100.10
```

Der Server muss anhand der Relayinformationen erkennen können, für welches Clientnetz eine Adresse vergeben werden soll.

Typische Relay-Probleme

- Relay fehlt auf dem VLAN-Interface,
- falsche DHCP-Serveradresse,
- neues VLAN wurde nicht ergänzt,
- Route zum DHCP-Server fehlt,
- Rückroute zum Relay fehlt,
- Firewall blockiert DHCP-Verkehr,
- falsche Relay- beziehungsweise Gatewayadresse,
- Policy behandelt Relayinformationen falsch,
- redundante Relays verhalten sich unterschiedlich.

Typisches Muster

```
DHCP funktioniert im selben Netz wie der Server,
aber nicht in einem entfernten VLAN.
```

Dies ist ein starker Hinweis auf Relay, Routing, Firewall oder fehlenden Scope für das entfernte Netz.

14. Wie wird ein erschöpfter DHCP-Bereich erkannt?

Mögliche Symptome:

- bestehende Clients funktionieren weiterhin,
- neue Clients erhalten keine Adresse,
- nach Ablauf alter Leases können weitere Geräte ausfallen,
- Server meldet keine verfügbaren Adressen,
- freie Adressen liegen nahe null,
- viele veraltete oder ungewöhnlich lange Leases,

- Adressen sind durch Reservierungen belegt,
- Bereich ist zu klein für die tatsächliche Gerätezahl.

Zu prüfen

Bereich	Prüffrage
Adresspool	Wie viele Adressen enthält er?
aktive Leases	Wie viele Adressen sind vergeben?
freie Adressen	Wie viele können noch vergeben werden?
Ausschlüsse	Welche Adressen sind ausgeschlossen?
Reservierungen	Welche Adressen sind fest zugeordnet?
Lease-Dauer	Passt sie zur Nutzung des Netzes?
veraltete Einträge	Sind Leases nicht mehr aktiver Geräte vorhanden?
Konflikterkennung	Wurden Adressen als problematisch markiert?

Eine Vergrößerung des Bereichs ist eine Netzwerkänderung. Präfix, Gateway, VLAN, Routing, Ausschlüsse und mögliche Überschneidungen müssen vorher geprüft werden.

15. Wie wird ein nicht autorisierter DHCP-Server erkannt?

Ein nicht vorgesehener DHCP-Server kann Clients falsche Netzwerkparameter liefern.

Mögliche Hinweise:

- verschiedene Clients erhalten unterschiedliche Gateways,
- DNS-Server weichen voneinander ab,
- Lease stammt von einer unbekannten Serveradresse,
- mehrere `DHCPOFFER` werden sichtbar,
- Fehler betrifft nur einen Switchbereich,
- Clients erhalten Adressen aus einem fremden Subnetz,
- Internetzugriff funktioniert, interne Dienste jedoch nicht.

Prüfung mit einem Paketmitschnitt

```
DHCPDISCOVER
  ← DHCPOFFER von Server A
  ← DHCPOFFER von Server B
```

Zu dokumentieren sind:

- Server-Identifier,
- Quell-IP-Adresse,
- Quell-MAC-Adresse,
- angebotene IP-Adresse,
- Gateway,
- DNS-Server,
- Lease-Dauer,
- Switchport der Server-MAC-Adresse.

Wichtig

Mehrere DHCP-Server können absichtlich zur Redundanz eingesetzt werden. Mehrere Angebote sind deshalb nicht automatisch ein Sicherheitsvorfall. Die Server müssen mit der vorgesehenen Architektur verglichen werden.

Ein tatsächlich unbekannter DHCP-Server ist umgehend an Netzwerk- und Informationssicherheitsverantwortliche zu eskalieren.

16. Wie werden falsche DHCP-Optionen erkannt?

Eine Lease kann erfolgreich bestätigt werden und trotzdem falsche Parameter enthalten.

Typische DHCP-Optionen:

Option	Zweck
1	Subnetzmaske
3	Router beziehungsweise Standardgateway
6	DNS-Server
15	Domainname
42	NTP-Server
51	Lease-Dauer
54	DHCP-Server-Identifier
58	Renewal Time T1
59	Rebinding Time T2
66	TFTP- beziehungsweise Servername, abhängig vom Einsatz
67	Bootdateiname
119	Domain Search List

Option	Zweck
121	Classless Static Routes

Nicht jede Option wird in jeder Umgebung verwendet.

Typische Fehler

- falsche Subnetzmaske,
- Gateway aus einem anderen Netz,
- veralteter DNS-Server,
- falsches DNS-Suffix,
- fehlerhafte statische Route,
- falscher Zeitserver,
- falsche Bootinformationen,
- Scope-Option wird durch Server-, Policy- oder Reservierungsoption überschrieben.

Die wirksame Option kann aus mehreren Konfigurationsebenen stammen. Deshalb muss die tatsächlich an den Client übertragene DHCP-Antwort geprüft werden.

17. Wie funktionieren Verlängerung und Rebinding einer Lease?

Eine DHCP-Lease besitzt eine begrenzte Gültigkeitsdauer.

Vereinfacht:

```
Leasebeginn
  │
  ├─ T1: Client versucht Erneuerung beim bisherigen Server
  │
  ├─ T2: Client versucht Erneuerung über weitere erreichbare Server
  │
  └─ Leaseende: Adresse darf nicht unbegrenzt weiterverwendet werden
```

Typische Standardbeziehungen, sofern der Server nichts anderes vorgibt:

```
T1 ungefähr 50 % der Lease-Dauer
T2 ungefähr 87,5 % der Lease-Dauer
```

Die tatsächlich übertragenen Werte sind entscheidend.

Mögliche Fehlerbilder

Situation	Auswirkung
Erstanfrage funktioniert, Verlängerung nicht	bestehende Verbindung kann bis zum Leaseende bestehen
Server zeitweise nicht erreichbar	Client versucht weitere Erneuerungen
DHCPNAK bei Erneuerung	Client muss Konfiguration verwerfen und neu anfordern
Netzwerkwechsel	alte Adresse passt möglicherweise nicht zum neuen VLAN
sehr kurze Lease	häufige DHCP-Kommunikation und höhere Serverlast
sehr lange Lease	Änderungen werden langsamer wirksam

18. Wann dürfen Lease-Freigabe und -Erneuerung durchgeführt werden?

Erst nachdem der Ausgangszustand dokumentiert wurde und geklärt ist, dass die Schnittstelle DHCP verwenden soll.

Windows

Lease freigeben:

```
[PRIV][CHANGE][DISRUPT] ipconfig /release
```

Lease erneuern:

```
[PRIV][CHANGE][DISRUPT] ipconfig /renew
```

Nur einen benannten Adapter ansprechen:

```
[PRIV][CHANGE][DISRUPT] ipconfig /release "Ethernet"
```

```
[PRIV][CHANGE][DISRUPT] ipconfig /renew "Ethernet"
```

Die Behandlung von Platzhaltern und Adapternamen sollte auf dem konkreten Windows-System mit `ipconfig /?` geprüft werden.

Linux mit NetworkManager

Verbindung erneut aktivieren:

```
[PRIV][CHANGE][DISRUPT] sudo nmcli connection down "VERBINDUNGSNAME"
```

```
[PRIV][CHANGE][DISRUPT] sudo nmcli connection up "VERBINDUNGSNAME"
```

Abhängig von NetworkManager-Version und Profil kann auch eine erneute Anwendung vorhandener Einstellungen möglich sein:

```
[PRIV][CHANGE][DISRUPT] sudo nmcli device reapply eth0
```

Dies erzwingt nicht in jedem Fall einen vollständigen neuen DHCP-DORA-Ablauf.

macOS

DHCP-Konfiguration auf einer Schnittstelle anfordern:

```
[PRIV][CHANGE][DISRUPT] sudo ipconfig set en0 DHCP
```

Dieser Befehl setzt die Schnittstelle auf DHCP und darf nicht verwendet werden, wenn eine statische Konfiguration vorgesehen ist.

> Bei Remotezugriff kann die Freigabe einer Lease die eigene Administrationsverbindung sofort beenden.

19. Warum sollte dhclient nicht ungeprüft parallel gestartet werden?

Der Befehl `dhclient` ist nicht auf jeder Linux-Installation vorhanden. Außerdem kann die Schnittstelle bereits durch NetworkManager, systemd-networkd oder einen anderen Netzwerkdienst verwaltet werden.

Ein zusätzlich gestarteter DHCP-Client kann:

- mit dem bestehenden Netzwerkmanager konkurrieren,
- eine vorhandene Lease verändern,
- Routen und DNS-Einstellungen überschreiben,
- die Remoteverbindung unterbrechen,

- Diagnoseergebnisse verfälschen.

Vor einer Verwendung muss geprüft werden:

```
[RO] ps -ef |
    grep -E '[d]hclient|[N]etworkManager|[s]ystemd-networkd'
```

```
[RO] systemctl --type=service --state=running |
    grep -Ei 'network|dhcp'
```

`dhclient` sollte nur verwendet werden, wenn er tatsächlich der vorgesehene DHCP-Client dieser Schnittstelle ist und seine lokale Dokumentation geprüft wurde.

20. Wie unterscheidet sich DHCPv6 von DHCPv4?

DHCPv6 ist kein direkter identischer Ersatz für DHCPv4.

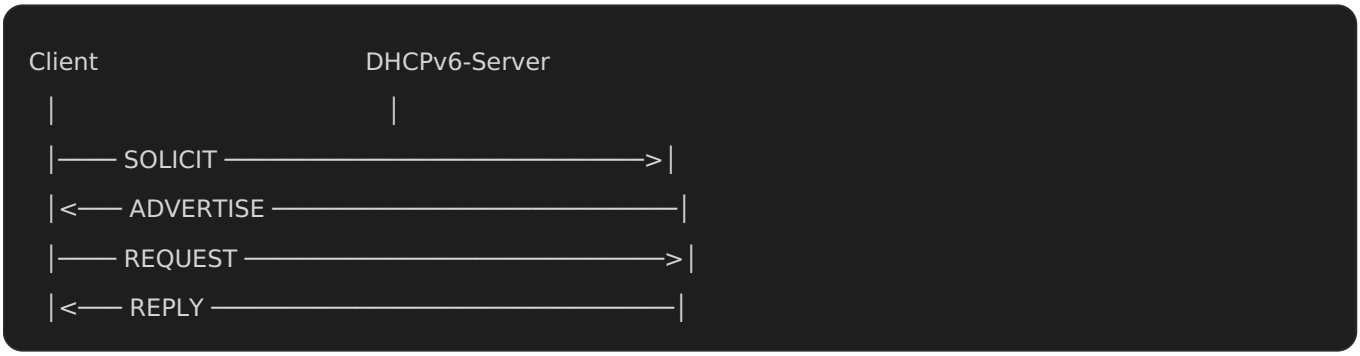
IPv6-Clients können Konfigurationen unter anderem erhalten durch:

- Router Advertisements,
- Stateless Address Autoconfiguration,
- zustandsbehaftetes DHCPv6,
- zustandsloses DHCPv6,
- statische Konfiguration.

DHCPv6 verwendet:

Richtung	UDP-Port
Client	546
Server	547

Vereinfachter DHCPv6-Ablauf:



Typische Nachrichten:

- `SOLICIT`,
- `ADVERTISE`,
- `REQUEST`,
- `REPLY`,
- `RENEW`,
- `REBIND`,
- `RELEASE`,
- `INFORMATION-REQUEST`.

Wireshark-Filter

```
dhcpv6
```

Capture-Filter:

```
udp port 546 or udp port 547
```

> Das IPv6-Standardgateway wird üblicherweise über Router Advertisements und nicht als klassische DHCPv6-Gatewayoption bezogen. Deshalb müssen DHCPv6 und Neighbor Discovery beziehungsweise Router Advertisements gemeinsam betrachtet werden.

21. Wie wird zwischen Client-, Netz- und Serverproblem unterschieden?

Beobachtung	Wahrscheinlichere Richtung
nur ein Client betroffen	Clientzustand, Profil, Adapter oder MAC-bezogene Policy
alle Clients an einem Port betroffen	Port, VLAN oder lokale Infrastruktur
alle neuen Clients eines VLANs betroffen	Relay, Scope oder Filter
alle VLANs betroffen	DHCP-Dienst oder zentrale Infrastruktur
bestehende Leases funktionieren	Bereich erschöpft oder Neuanfrage gestört
DISCOVER verlässt Client nicht	Client oder Schnittstelle
DISCOVER sichtbar, aber nicht am Relay	VLAN- oder Switchingpfad
DISCOVER erreicht Server, kein OFFER	Server, Scope oder Policy

Beobachtung	Wahrscheinlichere Richtung
OFFER verlässt Server, erreicht Client nicht	Rückweg, Relay oder Filter
ACK erreicht Client, Konfiguration fehlt	Client übernimmt Lease nicht
ACK enthält falsche Werte	Server-, Scope-, Policy- oder Reservierungsoption
mehrere OFFER von unbekannten Servern	möglicher Rogue-DHCP-Server

Diese Zuordnung bildet eine Arbeitshypothese und muss durch Logs, Paketmitschnitte und Vergleichstests bestätigt werden.

22. Welche Serverprüfungen sind erforderlich?

Die konkreten Befehle hängen vom DHCP-Serverprodukt ab. Unabhängig vom Produkt sollten folgende Punkte geprüft werden:

1. Läuft der DHCP-Dienst?
2. Ist der Server autorisiert beziehungsweise betrieblich freigegeben?
3. Ist der richtige Bereich aktiv?
4. Passt der Bereich zum Clientnetz?
5. Sind freie Adressen vorhanden?
6. Stimmen Präfix und Subnetzmaske?
7. Stimmen Gateway- und DNS-Optionen?
8. Existiert eine Reservierung für den Client?
9. Gibt es Ausschlussbereiche?
10. Wurde die Adresse als Konflikt markiert?
11. Greift eine Policy oder Geräteklassifizierung?
12. Sind Failover- beziehungsweise Redundanzpartner synchron?
13. Erreichen Anfragen den Server?
14. Verlässt die Antwort den Server?
15. Sind Relayinformationen korrekt?
16. Enthalten Serverlogs einen Ablehnungsgrund?

Wichtig

Die Oberfläche eines DHCP-Servers zeigt möglicherweise einen freien Bereich, während Policies, Reservierungen oder Failoverzustände die tatsächliche Vergabe beeinflussen. Die Serverprotokolle und die reale DHCP-Antwort sind deshalb ebenfalls zu prüfen.

23. Welche typischen Fehlinterpretationen müssen vermieden werden?

Beobachtung	Falscher Schluss	Richtige Einordnung

`169.254.x.x` vorhanden	Netzwerkkarte ist defekt	reguläre DHCP-Konfiguration wurde vermutlich nicht bezogen
DHCP aktiviert	Lease ist korrekt	Server, Adresse und Optionen prüfen
DHCPOFFER sichtbar	DHCP funktioniert vollständig	REQUEST und ACK müssen folgen
DHCPACK sichtbar	Netzwerk funktioniert	übertragene Optionen können falsch sein
mehrere Angebote	Angriff liegt vor	redundante Server können beabsichtigt sein
bestehende Clients funktionieren	DHCP-Server ist gesund	nur Verlängerung oder freie Adressen können betroffen sein
Ping zum DHCP-Server scheitert	DHCP muss scheitern	Relay und ICMP-Regeln getrennt bewerten
Server befindet sich in anderem Netz	DHCP kann nicht funktionieren	Relay kann Broadcasts weiterleiten
Lease wurde erneuert	Ursache wurde behoben	Fehler kann nur vorübergehend verdeckt sein
statische Adresse funktioniert	DHCP-Fehler ist bewiesen	VLAN, Routing und Adresskonflikte bleiben möglich
keine DHCP-Logs vorhanden	keine Anfrage wurde gesendet	falscher Logkanal oder fehlende Protokollierung möglich
DNS funktioniert nicht	DHCP ist vollständig ausgefallen	möglicherweise nur Option 6 fehlerhaft

24. Wie sieht der systematische Prüfablauf aus?

Schritt	Prüfung
1	betroffene Schnittstelle und VLAN bestimmen
2	vorhandene Lease vollständig sichern
3	DHCP-Server, Leasezeiten und Optionen dokumentieren
4	mit funktionierendem Client im selben VLAN vergleichen
5	DHCP-Clientprotokolle untersuchen
6	Verfügbarkeit freier Adressen serverseitig prüfen
7	bei Bedarf autorisierten Paketmitschnitt vorbereiten
8	DHCP-Vorgang kontrolliert reproduzieren
9	DORA-Sequenz und Server-Identifier auswerten

Schritt	Prüfung
10	Relay-, Routing- und Firewallpfad kontrollieren
11	Serverlogs und Scope-Konfiguration prüfen
12	falsche oder fehlende Optionen bestimmen
13	nur eine begründete Änderung durchführen
14	neue Lease mit Ausgangswert vergleichen
15	Gateway, DNS und Zielverbindung testen
16	Ursache und Änderung dokumentieren

Merksatz

Lease lesen → Clientlog prüfen → DORA verfolgen
→ Relay prüfen → Server und Scope prüfen → kontrolliert erneuern

25. Kompakte Befehlsübersicht für Windows, Linux und macOS

Aufgabe	Windows	Linux	macOS
vollständige Konfiguration	`[RO][SENS] ipconfig /all`	`[RO] ip address show`	`[RO] ifconfig`
DHCP-Status	`[RO] Get-NetIPInterface -AddressFamily IPv4`	`[RO] nmcli device show`	`[RO] networksetup -getinfo "DIENST"`
Adressursprung	`[RO] Get-NetIPAddress -AddressFamily IPv4`	`[RO] nmcli connection show "NAME"`	`[RO] networksetup -getinfo "DIENST"`
DHCP-Paketdaten	in `ipconfig /all` teilweise sichtbar	abhängig vom Netzwerkmanager	`[RO][SENS] ipconfig getpacket en0`
Clientlogs	`[RO] Get-WinEvent -ListLog '*DHCP*'`	`[RO][PRIV] sudo journalctl -b -u NetworkManager`	`[RO] log show --last 1h --predicate 'eventMessage CONTAINS[c] "DHCP"'`
NetworkManager-Status	nicht zutreffend	`[RO] nmcli device status`	nicht zutreffend
networkd-Status	nicht zutreffend	`[RO] networkctl status`	nicht zutreffend
DHCPv4-Capture	`dumpcap -f "udp port 67 or udp port 68"`	gleicher Befehl	gleicher Befehl
DHCPv6-Capture	`dumpcap -f "udp port 546 or udp port 547"`	gleicher Befehl	gleicher Befehl
Lease freigeben	`[PRIV][CHANGE][DISRUPT] ipconfig /release`	abhängig vom Netzwerkmanager	kein direkt gleichwertiger allgemeiner Lesebefehl
Lease erneuern	`[PRIV][CHANGE][DISRUPT] ipconfig /renew`	Verbindung kontrolliert neu aktivieren	`[PRIV][CHANGE][DISRUPT] sudo ipconfig set en0 DHCP`

Die Platzhalter `DIENST`, `NAME`, `INTERFACE` und `en0` müssen durch die tatsächlich ermittelten Bezeichnungen ersetzt werden.

26. Dokumentationsvorlage

```
Ticketnummer:
Prüfzeitpunkt:
Zeitzone:
Betroffener Client:
Benutzer:
Standort:
Schnittstelle:
MAC-Adresse:
Switch:
Switchport:
VLAN:

VORHANDENE KONFIGURATION

DHCP aktiviert:
IPv4-Adresse:
Präfix/Subnetzmaske:
Adresszustand:
Standardgateway:
DNS-Server:
DNS-Suchdomäne:
DHCP-Server:
Lease erhalten:
T1:
T2:
Lease läuft ab:
Weitere DHCP-Optionen:

ERWARTETE KONFIGURATION

DHCP-Bereich:
Präfix/Subnetzmaske:
```

Standardgateway:

DNS-Server:

DHCP-Server:

Lease-Dauer:

Weitere Optionen:

VERGLEICHSCLIENT

Hostname:

Gleiches VLAN:

DHCP-Server:

IPv4-Adresse:

Präfix:

Gateway:

DNS-Server:

Lease erfolgreich:

Relevante Abweichungen:

CLIENTPROTOKOLL

Zeitpunkt:

Meldung:

Provider/Dienst:

Ereignis-ID:

PAKETABLAUF

DHCPDISCOVER sichtbar: Ja / Nein

DHCPOFFER sichtbar: Ja / Nein

Anzahl anbietender Server:

DHCPREQUEST sichtbar: Ja / Nein

DHCPACK sichtbar: Ja / Nein

DHCPNAK sichtbar: Ja / Nein

DHCPDECLINE sichtbar: Ja / Nein

Transaktions-ID:

Client-Identifier:

Server-Identifier:

Angebotene Adresse:

Übertragene Optionen:

RELAY

Relay erforderlich:
Relayadresse:
Anfrage erreicht Relay:
Anfrage erreicht Server:
Antwort erreicht Relay:
Antwort erreicht Client:

SERVER

Dienststatus:
Scope aktiv:
Freie Adressen:
Ausschlüsse:
Reservierungen:
Konflikte:
Policy:
Failoverstatus:
Serverlog:

Arbeitshypothese:
Begründung:
Gesicherter Ausgangszustand:
Durchgeführter Test:
Durchgeführte Änderung:
Rückweg:
Neue Lease:
Abschlussprüfung:
Ermittelte Ursache:

27. Offizielle Quellen und weiterführende Dokumentation

Microsoft

- DHCP – technische Übersicht
- DHCP-Bereitstellung und -Verwaltung

- Get-NetIPInterface
- Get-NetIPAddress
- Get-WinEvent
- ipconfig

Linux

- NetworkManager nmcli
- systemd-networkd
- networkctl
- ip-address – Linux Manual Page

Apple

- Lokale Befehlsreferenzen: `man ipconfig`, `man networksetup`, `man scutil` und `man log`
- Ändern der TCP/IP-Einstellungen auf dem Mac

Wireshark

- Wireshark DHCP Display Filter Reference
- dumpcap Manual Page
- tshark Manual Page

Standards

- RFC 2131 – Dynamic Host Configuration Protocol
- RFC 2132 – DHCP Options
- RFC 3046 – DHCP Relay Agent Information Option
- RFC 8415 – DHCP for IPv6

> DHCP-Serverbefehle und Verwaltungsoberflächen unterscheiden sich je nach Hersteller und Produkt. Änderungen an Scopes, Relays, Optionen oder Failoverkonfigurationen dürfen nur anhand der Dokumentation des tatsächlich eingesetzten Systems vorgenommen werden.