

10.4 DHCP und automatische IP-Konfiguration*

DHCP gehört zur OSI-Schicht 7.

DHCP steht für:

Dynamic Host Configuration Protocol

Die Hauptaufgabe von DHCP ist:

Netzwerkconfiguration automatisch an Clients verteilen.

Ein Client kann per DHCP zum Beispiel erhalten:

- IP-Adresse
- Subnetzmaske
- Standard-Gateway
- DNS-Server
- Domain-Suffix
- Lease-Zeit
- weitere DHCP-Optionen

Merksatz:

DHCP = automatische IP-Konfiguration.

Warum braucht man DHCP?

Ohne DHCP müsste jedes Gerät manuell konfiguriert werden.

Das wäre aufwendig und fehleranfällig.

Man müsste manuell eintragen:

- IP-Adresse
- Subnetzmaske
- Gateway
- DNS-Server

- weitere Einstellungen

DHCP automatisiert diese Vergabe.

Vorteile:

- weniger manuelle Arbeit
- weniger Tippfehler
- zentrale Verwaltung
- flexible Adressvergabe
- einfache Änderung von DNS oder Gateway
- bessere Übersicht über vergebene Adressen

Merksatz:

DHCP verhindert viele manuelle IP-Konfigurationsfehler.

DHCP im OSI-Modell

DHCP ist ein Anwendungsschicht-Protokoll.

Es gehört zu:

OSI-Schicht 7

Aber DHCP verteilt Informationen, die für Schicht 3 wichtig sind.

Beispiel:

IP-Adresse
Subnetzmaske
Gateway

Wichtig:

DHCP-Protokoll = Schicht 7
IP-Adresse und Gateway = Schicht 3

Merksatz:

DHCP ist Schicht 7,
liefert aber Schicht-3-Konfiguration.

DHCP und Ports

DHCP nutzt UDP.

Wichtige Ports:

Rolle	Protokoll	Port
DHCP-Server	UDP	67
DHCP-Client	UDP	68

Warum UDP?

Ein Client hat am Anfang oft noch keine vollständige IP-Konfiguration.
DHCP muss bereits funktionieren,
bevor der Client normal im IP-Netz arbeiten kann.

Merksatz:

DHCP nutzt UDP 67 und UDP 68.

DHCP-Client

Ein DHCP-Client ist ein Gerät, das automatisch eine Netzwerkkonfiguration anfordert.

Beispiele:

- PC
- Notebook
- Smartphone
- Drucker
- IP-Telefon
- Server
- virtuelle Maschine
- IoT-Gerät

Der Client fragt:

Gibt es einen DHCP-Server,
der mir eine IP-Konfiguration geben kann?

Merksatz:

DHCP-Client fordert IP-Konfiguration an.

DHCP-Server

Ein DHCP-Server vergibt IP-Konfigurationen an Clients.

Er verwaltet unter anderem:

- Adressbereiche
- Leases
- Reservierungen
- DHCP-Optionen
- verfügbare und vergebene IP-Adressen

Beispiele für DHCP-Server:

- Router
- Windows Server
- Linux-Server
- Firewall
- Netzwerk-Appliance

Merksatz:

DHCP-Server verteilt Netzwerkkonfiguration.

DHCP-Bereich

Ein DHCP-Bereich wird auch genannt:

DHCP-Scope

Er beschreibt, welche IP-Adressen ein DHCP-Server vergeben darf.

Beispiel:

Netz:

192.168.10.0/24

DHCP-Bereich:

192.168.10.100 bis 192.168.10.200

Der DHCP-Server vergibt dann Adressen aus diesem Bereich.

Merksatz:

DHCP-Scope = Adressbereich für automatische Vergabe.

DHCP-Lease

Eine per DHCP vergebene Adresse wird nicht dauerhaft vergeben, sondern für eine bestimmte Zeit.

Diese Zeit heißt:

Lease-Zeit

Beispiel:

Client erhält 192.168.10.120

für 8 Stunden.

Nach Ablauf muss der Client die Adresse erneuern oder eine neue Konfiguration erhalten.

Merksatz:

Lease = zeitlich begrenzte Adresszuweisung.

Warum gibt es Leases?

Leases sorgen dafür, dass IP-Adressen wieder frei werden können.

Beispiel:

Ein Notebook war im WLAN.
Es verlässt das Netzwerk.
Nach Ablauf der Lease kann die Adresse wieder vergeben werden.

Das ist besonders nützlich bei:

- WLANs
- Gastnetzen
- Schulen
- Unternehmen
- wechselnden Geräten
- mobilen Clients

Merksatz:

Lease-Zeit verhindert dauerhaft blockierte IP-Adressen.

DHCP-Ablauf: DORA

Der klassische DHCP-Ablauf wird oft mit DORA beschrieben.

DORA steht für:

Discover
Offer
Request
Acknowledge

Die vier Schritte:

Schritt	Richtung	Bedeutung
1	Client → Netzwerk	Discover
2	Server → Client	Offer
3	Client → Server	Request

Schritt	Richtung	Bedeutung
4	Server → Client	Acknowledge

Merksatz:

DHCP-Ablauf = DORA.

DHCP Discover

Beim DHCP Discover sucht der Client nach einem DHCP-Server.

Der Client hat zu diesem Zeitpunkt oft noch keine gültige IP-Adresse.

Deshalb wird die Anfrage als Broadcast gesendet.

Vereinfacht sagt der Client:

Gibt es hier einen DHCP-Server?

Merksatz:

Discover = Client sucht DHCP-Server.

DHCP Offer

Beim DHCP Offer bietet der DHCP-Server dem Client eine Konfiguration an.

Das Angebot enthält zum Beispiel:

- IP-Adresse
- Subnetzmaske
- Gateway
- DNS-Server
- Lease-Zeit

Vereinfacht sagt der Server:

Du kannst diese Adresse verwenden.

Merksatz:

Offer = Server bietet Konfiguration an.

DHCP Request

Beim DHCP Request nimmt der Client ein Angebot an.

Vereinfacht sagt der Client:

Ich möchte diese angebotene IP-Adresse verwenden.

Wenn mehrere DHCP-Server geantwortet haben, wählt der Client normalerweise ein Angebot aus.

Merksatz:

Request = Client fordert angebotene Adresse an.

DHCP Acknowledge

Beim DHCP Acknowledge bestätigt der Server die Vergabe.

Vereinfacht sagt der Server:

Die Adresse ist für dich reserviert.

Danach kann der Client die erhaltene IP-Konfiguration verwenden.

Merksatz:

Acknowledge = Server bestätigt die Vergabe.

DORA als Ablaufbild

Der Ablauf vereinfacht:

Client → Broadcast:
DHCP Discover

Server → Client:

DHCP Offer

Client → Server:

DHCP Request

Server → Client:

DHCP Acknowledge

Merksatz:

Discover, Offer, Request, Acknowledge.

Broadcast bei DHCP

DHCP nutzt am Anfang Broadcast, weil der Client noch nicht weiß:

welche IP-Adresse er selbst hat

welche IP-Adresse der DHCP-Server hat

welches Gateway zuständig ist

Broadcast bedeutet:

Nachricht an alle Geräte im lokalen Netz.

Wichtig:

Router leiten Broadcasts normalerweise nicht einfach in andere Netze weiter.

Merksatz:

DHCP startet häufig mit Broadcast im lokalen Netz.

DHCP und VLANs

In der Praxis gibt es häufig pro VLAN ein eigenes IP-Subnetz.

Beispiel:

VLAN	Subnetz	DHCP-Bereich
VLAN 10	192.168.10.0/24	192.168.10.100-200
VLAN 20	192.168.20.0/24	192.168.20.100-200
VLAN 30	192.168.30.0/24	192.168.30.100-200

Ein Client im VLAN 20 soll eine Adresse aus dem VLAN-20-Bereich bekommen.

Merksatz:

Jedes VLAN braucht passende DHCP-Konfiguration.

DHCP-Relay

Ein DHCP-Relay wird benötigt, wenn DHCP-Client und DHCP-Server in unterschiedlichen Netzen liegen.

Problem:

DHCP Discover ist Broadcast.
Router leiten Broadcasts normalerweise nicht weiter.

Lösung:

DHCP-Relay nimmt die Anfrage entgegen
und leitet sie gezielt an den DHCP-Server weiter.

Bei Cisco wird dafür oft der Begriff verwendet:

IP Helper Address

Merksatz:

DHCP-Relay bringt DHCP-Anfragen über Router-Grenzen.

Beispiel DHCP-Relay

Situation:

Client im VLAN 20
DHCP-Server im Servernetz VLAN 100

Ohne DHCP-Relay:

DHCP Discover bleibt im VLAN 20.
DHCP-Server sieht die Anfrage nicht.

Mit DHCP-Relay:

Router oder Layer-3-Switch leitet die Anfrage an den DHCP-Server weiter.

Merksatz:

DHCP-Server muss nicht in jedem VLAN stehen,
wenn DHCP-Relay korrekt eingerichtet ist.

DHCP-Optionen

DHCP kann neben der IP-Adresse weitere Informationen liefern.

Wichtige Optionen:

Option	Bedeutung
Subnetzmaske	Netzgröße
Router / Gateway	Standard-Gateway
DNS-Server	Server für Namensauflösung
Domainname	DNS-Suffix
NTP-Server	Zeitserver
Lease-Zeit	Gültigkeitsdauer
PXE-Boot-Optionen	Netzwerkstart

Merksatz:

DHCP liefert mehr als nur IP-Adressen.

Standard-Gateway per DHCP

DHCP kann das Standard-Gateway an den Client verteilen.

Das Gateway wird benötigt, wenn der Client andere Netze erreichen soll.

Beispiel:

Client:

192.168.10.120/24

Gateway:

192.168.10.1

Wichtig:

Das Gateway muss zum Subnetz des Clients passen.

Merksatz:

Falsches Gateway per DHCP erzeugt Routing-Probleme.

DNS-Server per DHCP

DHCP verteilt oft auch DNS-Server.

Beispiel:

DNS-Server:

192.168.10.10

Wenn hier ein falscher DNS-Server eingetragen ist, funktioniert IP-Kommunikation möglicherweise, aber Namensauflösung nicht.

Fehlerbild:

ping 8.8.8.8 funktioniert

ping www.example.com funktioniert nicht

Merksatz:

Falscher DNS per DHCP verursacht Namensprobleme.

DHCP-Reservierung

Eine DHCP-Reservierung ordnet einem bestimmten Gerät immer dieselbe IP-Adresse zu.

Typische Grundlage:

MAC-Adresse des Clients

Beispiel:

Drucker-MAC:

AA:BB:CC:11:22:33

reservierte IP:

192.168.10.50

Der Drucker bekommt dann per DHCP immer dieselbe Adresse.

Merksatz:

DHCP-Reservierung = gleiche IP für bestimmtes Gerät.

Reservierung und statische IP unterscheiden

Variante	Bedeutung
statische IP	direkt am Gerät manuell eingetragen
DHCP-Reservierung	zentral am DHCP-Server festgelegt

Vorteil der Reservierung:

zentrale Verwaltung

weniger Fehler am Gerät

DNS und Optionen bleiben konsistent

Typisch für:

- Drucker
- Server
- Netzwerkgeräte
- Kameras
- Spezialgeräte

Merksatz:

Reservierung ist zentraler als manuelle statische IP.

Ausschlussbereich

Ein Ausschlussbereich enthält IP-Adressen, die der DHCP-Server nicht automatisch vergeben soll.

Beispiel:

Netz:

192.168.10.0/24

DHCP-Bereich:

192.168.10.10 bis 192.168.10.250

ausgeschlossen:

192.168.10.1 bis 192.168.10.20

Warum?

Diese Adressen sind vielleicht für Gateway, Server oder Drucker reserviert.

Merksatz:

Ausschlussbereiche verhindern doppelte Vergabe wichtiger Adressen.

Adresskonflikt

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

Mögliche Ursachen:

- statische IP liegt im DHCP-Bereich
- DHCP-Reservierung doppelt
- zwei DHCP-Server vergeben gleiche Bereiche
- manuelle Fehlkonfiguration
- Gerät verwendet alte Adresse weiter

Folgen:

- instabile Verbindung
- wechselnde Erreichbarkeit
- ARP-Probleme
- Verbindungsabbrüche

Merksatz:

Doppelte IP-Adressen verursachen instabile Netzprobleme.

DHCP und APIPA

Wenn ein Windows-Client keine DHCP-Adresse erhält, kann er sich selbst eine APIPA-Adresse geben.

APIPA-Bereich:

169.254.0.0/16

Beispiel:

169.254.23.80

Das bedeutet häufig:

DHCP-Server nicht erreichbar
oder
DHCP-Vergabe fehlgeschlagen

Merksatz:

169.254.x.x weist oft auf DHCP-Probleme hin.

DHCP und DNS-Dynamik

In manchen Netzwerken werden DNS-Einträge automatisch mit DHCP aktualisiert.

Beispiel:

Client erhält per DHCP:
192.168.10.120

DNS wird aktualisiert:

client01.firma.local
→ 192.168.10.120

Das ist besonders in Windows- und Active-Directory-Umgebungen verbreitet.

Merksatz:

DHCP kann mit DNS zusammenarbeiten.

DHCP und Active Directory

In Windows-Umgebungen ist DHCP oft eng mit DNS und Active Directory verbunden.

Wichtig:

Clients brauchen richtigen DNS-Server,
um Domänencontroller zu finden.

Wenn per DHCP ein externer DNS-Server verteilt wird, kann die Domänenanmeldung fehlschlagen.

Merksatz:

In AD-Netzen muss DHCP den internen DNS-Server verteilen.

DHCP-Snooping

DHCP-Snooping ist eine Sicherheitsfunktion auf Switches.

Ziel:

Schutz vor unerlaubten DHCP-Servern.

Der Switch unterscheidet:

vertrauenswürdige Ports
nicht vertrauenswürdige Ports

DHCP-Antworten dürfen nur von vertrauenswürdigen Ports kommen.

Merksatz:

DHCP-Snooping schützt vor Rogue-DHCP-Servern.

Rogue-DHCP-Server

Ein Rogue-DHCP-Server ist ein unerlaubter DHCP-Server im Netzwerk.

Er kann falsche Informationen verteilen:

- falsches Gateway
- falscher DNS-Server
- falsche IP-Adressen
- falsches Subnetz

Folgen:

- Clients verlieren Netzwerkzugriff
- Datenverkehr wird umgeleitet
- Namensauflösung wird manipuliert
- Sicherheitsrisiko

Merksatz:

Unerlaubter DHCP-Server kann ein ganzes Netz stören.

DHCP-Starvation

DHCP-Starvation ist ein Angriff, bei dem sehr viele DHCP-Anfragen gestellt werden.

Ziel:

DHCP-Adressbereich erschöpfen.

Folge:

echte Clients bekommen keine IP-Adresse mehr.

Schutzmaßnahmen:

- Port Security
- DHCP-Snooping
- Netzwerkzugangskontrolle
- Monitoring
- ausreichend Segmentierung

Merksatz:

DHCP-Starvation leert den DHCP-Adresspool.

DHCP und IPv6

Bei IPv6 gibt es mehrere Möglichkeiten zur Adresskonfiguration.

Wichtige Begriffe:

- SLAAC
- DHCPv6
- Router Advertisements

SLAAC bedeutet:

Client bildet IPv6-Adresse selbst anhand von Router Advertisements.

DHCPv6 kann zusätzliche Informationen liefern, zum Beispiel DNS-Server.

Merksatz:

IPv6 nutzt nicht einfach DHCPv4,
sondern SLAAC, RA und DHCPv6.

DHCPv4 und DHCPv6 unterscheiden

Thema	DHCPv4	DHCPv6
Protokollfamilie	IPv4	IPv6
Adressvergabe	häufig zentral per DHCP	möglich, aber auch SLAAC
Broadcast	ja	nein, IPv6 nutzt Multicast
Gateway-Verteilung	per DHCP möglich	meist über Router Advertisements
DNS-Verteilung	per DHCP	per DHCPv6 oder RA-Optionen

Merksatz:

DHCPv6 funktioniert anders als DHCPv4.

DHCP-Fehlersuche

Typische Fragen:

Hat der Client überhaupt Link?
Ist der Client im richtigen VLAN?
Gibt es einen DHCP-Server?
Ist der DHCP-Bereich aktiv?
Sind noch freie Adressen vorhanden?
Funktioniert DHCP-Relay?
Werden UDP 67 und 68 blockiert?
Gibt es einen Rogue-DHCP-Server?
Ist die erhaltene IP im richtigen Subnetz?
Stimmen Gateway und DNS?

Merksatz:

DHCP-Fehlersuche beginnt bei Link, VLAN und DHCP-Server.

Fehlerbild: Client bekommt keine IP-Adresse

Mögliche Ursachen:

- kein Link
- falsches VLAN
- DHCP-Server nicht erreichbar
- DHCP-Dienst gestoppt
- DHCP-Bereich erschöpft
- DHCP-Relay fehlt
- Firewall blockiert UDP 67/68
- Rogue-DHCP oder Schutzfunktion stört
- Netzwerkkarte deaktiviert
- Clientproblem

Merksatz:

Keine IP-Adresse:
Link, VLAN, DHCP und Relay prüfen.

Fehlerbild: Client bekommt falsche IP-Adresse

Mögliche Ursachen:

- Client ist im falschen VLAN
- falscher DHCP-Bereich aktiv
- Rogue-DHCP-Server
- falsche SSID-VLAN-Zuordnung
- falscher Switch-Port
- fehlerhafte Reservierung
- falscher DHCP-Relay-Kontext

Merksatz:

Falsche DHCP-Adresse deutet oft auf falsches VLAN oder Rogue-DHCP hin.

Fehlerbild: Client bekommt IP, aber kein Internet

Mögliche Ursachen:

- falsches Gateway per DHCP
- Gateway nicht erreichbar
- DNS falsch
- Routing fehlt
- NAT fehlt
- Firewall blockiert
- falsche Subnetzmaske
- Client im falschen VLAN

Merksatz:

DHCP-Erfolg heißt nicht automatisch:
Internet funktioniert.

Fehlerbild: IP funktioniert, Name nicht

Mögliche Ursachen:

- falscher DNS-Server per DHCP verteilt
- DNS-Server nicht erreichbar
- DNS-Dienst gestört
- falsches DNS-Suffix
- Firewall blockiert DNS
- externer DNS statt interner DNS

Merksatz:

DHCP kann DNS-Probleme verursachen,
wenn falsche DNS-Optionen verteilt werden.

Fehlerbild: Manche Clients bekommen IP, andere nicht

Mögliche Ursachen:

- DHCP-Pool fast erschöpft
- bestimmte Switch-Ports in falschem VLAN
- WLAN-SSID falsch zugeordnet
- DHCP-Snooping blockiert bestimmte Ports
- MAC-Filter
- Reservierungen fehlerhaft
- Relay nur für manche VLANs eingerichtet

Merksatz:

Teilweise DHCP-Probleme nach Standort, VLAN und Port eingrenzen.

Fehlerbild: Nach Umzug in anderes VLAN keine IP

Mögliche Ursachen:

- DHCP-Bereich für neues VLAN fehlt
- DHCP-Relay im neuen VLAN fehlt
- VLAN nicht auf Trunk erlaubt
- Access-Port falsch
- Firewall blockiert DHCP-Relay
- Gateway-Schnittstelle im VLAN fehlt

Merksatz:

Neues VLAN braucht passenden DHCP-Bereich und Relay.

DHCP-Tools

Typische Werkzeuge und Prüfungen:

Werkzeug / Prüfung	Nutzen
IP-Konfiguration anzeigen	erhaltene Adresse prüfen
Lease erneuern	neue DHCP-Anfrage auslösen

Werkzeug / Prüfung	Nutzen
DHCP-Server-Konsole	Bereich, Leases, Reservierungen prüfen
DHCP-Logs	Vergaben und Fehler prüfen
Switch-Port prüfen	VLAN und Link kontrollieren
Packet Capture	DORA-Ablauf sichtbar machen
Firewall-Logs	UDP 67/68 prüfen
ARP-Tabelle	Adresskonflikte erkennen

Merksatz:

DHCP prüft man am Client,
am Server
und am Netzwerk dazwischen.

DHCP-Ablauf im Mitschnitt

In einem Paketmitschnitt erkennt man den DHCP-Ablauf:

Discover
Offer
Request
Acknowledge

Typische Fragen:

Sendet der Client Discover?
Kommt ein Offer zurück?
Sendet der Client Request?
Kommt ein Acknowledge?
Welche IP wird angeboten?
Welcher Server antwortet?

Merksatz:

Im Mitschnitt sieht man,
an welchem DORA-Schritt es scheitert.

DHCP und Firewall

DHCP kann durch Firewall-Regeln gestört werden.

Besonders relevant:

UDP 67

UDP 68

Bei DHCP-Relay kann auch Verkehr zwischen Relay und DHCP-Server betroffen sein.

Wichtig:

DHCP im gleichen LAN nutzt Broadcast.

DHCP über Relay muss gezielt erlaubt sein.

Merksatz:

Firewall kann DHCP verhindern,
wenn UDP 67/68 blockiert wird.

DHCP und Dokumentation

DHCP sollte sauber dokumentiert werden.

Wichtige Angaben:

- Subnetz
- VLAN
- DHCP-Bereich
- Ausschlüsse
- Reservierungen
- Gateway
- DNS-Server
- Lease-Zeit
- DHCP-Relay-Adresse
- zuständiger Server

Merksatz:

Gute DHCP-Dokumentation verhindert Fehlvergaben.

Was DHCP nicht macht

DHCP macht nicht:

- Kabelverbindung herstellen
- VLAN automatisch richtig setzen
- Routing garantieren
- NAT einrichten
- DNS-Namen zwingend korrekt auflösen
- Dienste starten
- Benutzer authentifizieren
- Firewall-Regeln ersetzen

DHCP liefert Konfigurationsdaten, aber andere Netzfunktionen müssen trotzdem korrekt eingerichtet sein.

Merksatz:

DHCP vergibt Konfiguration,
garantiert aber keine vollständige Erreichbarkeit.

Einordnung in das OSI-Modell

Thema	Schicht
DHCP-Protokoll	7
DHCP-Optionen	7 mit Schicht-3-Bezug
UDP 67 / 68	4
IP-Adresse	3
Subnetzmaske	3
Standard-Gateway	3
DNS-Server-Adresse	3 / 7-Bezug
VLAN	2
Broadcast	2 / 3-Bezug
DHCP-Relay	3 / 7-Bezug

Thema	Schicht
DHCP-Snooping	2-Sicherheitsfunktion

Merksatz:

DHCP gehört zu Schicht 7,
wirkt aber stark auf Schicht 3.

Typische IHK-Fragen

In AP1 und AP2 kann zum Beispiel gefragt werden:

- Wofür steht DHCP?
- Welche Aufgabe hat DHCP?
- Warum ist DHCP sinnvoll?
- Welche Informationen kann DHCP verteilen?
- Welche Ports nutzt DHCP?
- Welches Transportprotokoll nutzt DHCP?
- Was bedeutet DORA?
- Was passiert bei DHCP Discover?
- Was passiert bei DHCP Offer?
- Was passiert bei DHCP Request?
- Was passiert bei DHCP Acknowledge?
- Was ist ein DHCP-Scope?
- Was ist eine Lease?
- Was ist eine DHCP-Reservierung?
- Was ist ein DHCP-Relay?
- Warum braucht man DHCP-Relay bei mehreren VLANs?
- Was bedeutet APIPA?
- Was ist ein Rogue-DHCP-Server?
- Warum kann ein Client eine falsche IP-Adresse bekommen?

Typische Prüfungsfallen

DHCP gehört zu Schicht 7.

DHCP nutzt UDP.

DHCP-Server nutzt UDP 67.

DHCP-Client nutzt UDP 68.

DHCP vergibt nicht nur IP-Adressen.

DHCP kann auch Gateway und DNS verteilen.

DHCP-Ablauf = DORA.

Discover sucht DHCP-Server.

Offer bietet Konfiguration an.

Request fordert Angebot an.

Acknowledge bestätigt Vergabe.

DHCP startet häufig mit Broadcast.

Router leiten Broadcasts normalerweise nicht einfach weiter.

DHCP-Relay ist für DHCP über Netzgrenzen nötig.

Falsches VLAN führt oft zu falscher DHCP-Adresse.

APIPA 169.254.x.x deutet oft auf DHCP-Problem hin.

DHCP-Erfolg heißt nicht automatisch,
dass DNS oder Internet funktionieren.

Rogue-DHCP kann falsche Konfiguration verteilen.

DHCPv6 funktioniert anders als DHCPv4.

Wichtige Begriffe kurz erklärt

Begriff	Kurze Erklärung
---------	-----------------

DHCP	Dynamic Host Configuration Protocol
DHCP-Client	Gerät, das Konfiguration anfordert
DHCP-Server	Server, der Konfiguration vergibt
DHCP-Scope	Adressbereich für DHCP
Lease	zeitlich begrenzte Adressvergabe
DORA	Discover, Offer, Request, Acknowledge
Discover	Client sucht DHCP-Server
Offer	Server bietet Konfiguration an
Request	Client fordert Angebot an
Acknowledge	Server bestätigt Vergabe
DHCP-Option	zusätzliche Konfigurationsinformation
DHCP-Relay	Weiterleitung von DHCP-Anfragen in andere Netze
IP Helper	Begriff für DHCP-Relay bei manchen Herstellern
Reservierung	feste IP-Zuordnung über DHCP
Ausschlussbereich	Adressen, die nicht automatisch vergeben werden
APIPA	automatische 169.254.x.x-Adresse bei DHCP-Problem
Rogue-DHCP	unerlaubter DHCP-Server
DHCP-Snooping	Schutzfunktion gegen Rogue-DHCP
DHCP-Starvation	Angriff auf DHCP-Adresspool
DHCPv6	DHCP für IPv6

IHK-sichere Kurzformulierung

DHCP steht für Dynamic Host Configuration Protocol und gehört zur Anwendungsschicht des OSI-Modells. Es dient dazu, Clients automatisch mit Netzwerkkonfigurationen zu versorgen. Dazu gehören IP-Adresse, Subnetzmaske, Standard-Gateway, DNS-Server und weitere Optionen. DHCP nutzt UDP, der Server verwendet Port 67 und der Client Port 68. Der klassische DHCP-Ablauf wird mit DORA beschrieben: Discover, Offer, Request und Acknowledge. Befindet sich der DHCP-Server in einem anderen Netz als der Client, wird ein DHCP-Relay benötigt, weil DHCP-Anfragen anfangs häufig als Broadcast gesendet werden und Router Broadcasts nicht einfach weiterleiten.

Merksätze

DHCP = Dynamic Host Configuration Protocol.

DHCP gehört zu Schicht 7.

DHCP vergibt automatische Netzwerkkonfiguration.

DHCP liefert IP-Adresse,
Subnetzmaske,
Gateway
und DNS-Server.

DHCP nutzt UDP.

DHCP-Server = UDP 67.

DHCP-Client = UDP 68.

DHCP-Ablauf = DORA.

Discover = Client sucht Server.

Offer = Server bietet Konfiguration an.

Request = Client fordert Angebot an.

Acknowledge = Server bestätigt.

DHCP startet häufig mit Broadcast.

Router leiten Broadcasts normalerweise nicht weiter.

DHCP-Relay leitet DHCP über Netzgrenzen.

DHCP-Scope = Adressbereich.

Lease = zeitlich begrenzte Vergabe.

Reservierung = feste IP per DHCP.

Ausschlussbereich = nicht automatisch vergeben.

169.254.x.x = häufig DHCP-Problem.

Falsches VLAN kann falsche DHCP-Adresse verursachen.

Rogue-DHCP = unerlaubter DHCP-Server.

DHCP-Snooping schützt vor Rogue-DHCP.

DHCPv6 ist nicht einfach DHCPv4 mit IPv6.

DHCP-Erfolg bedeutet nicht automatisch:
Internet funktioniert.
