Netzwerke und Dienste bereitstellen (LF9)

ITS11_LS8_DHCP_20240604_Yf.docx

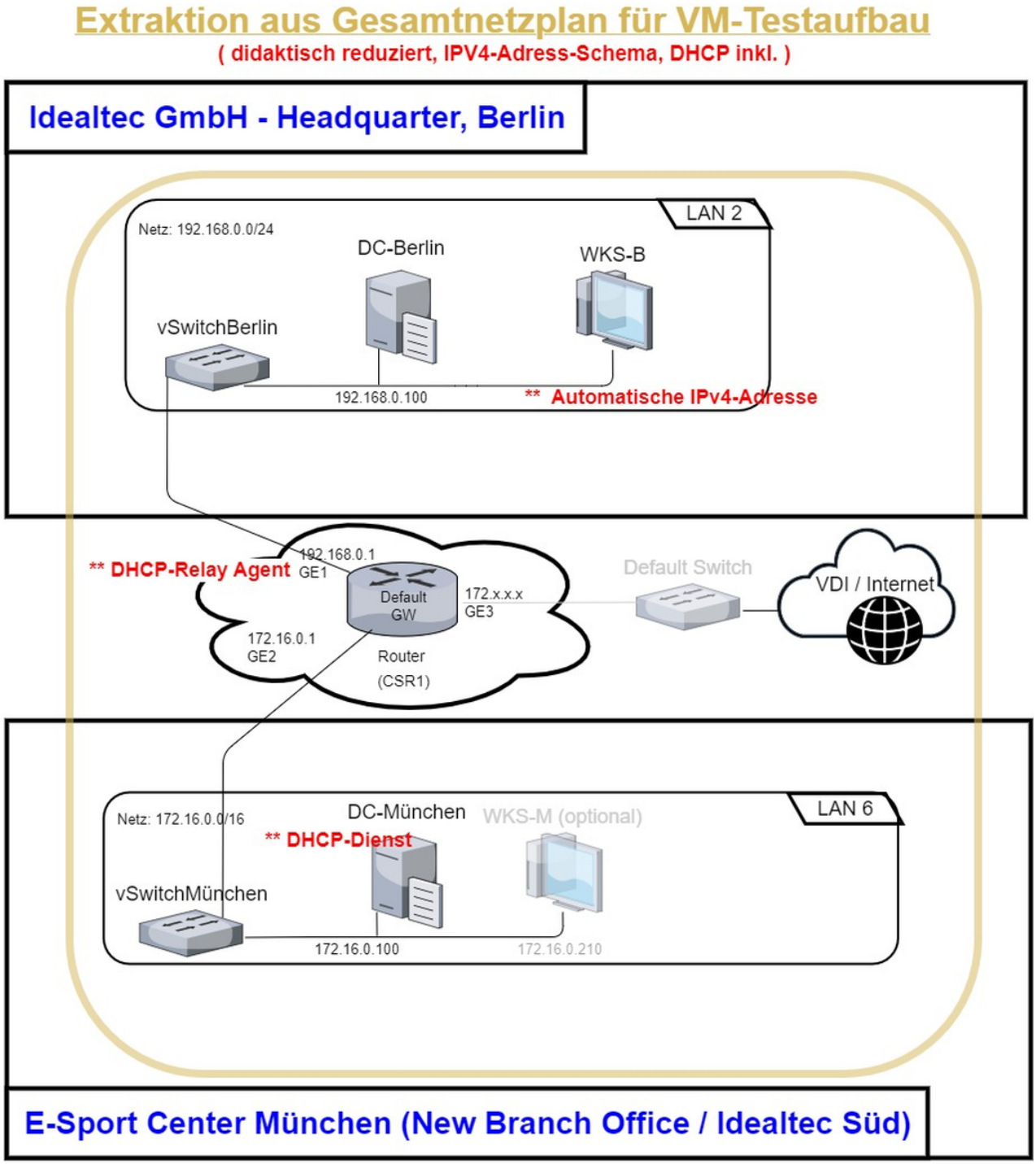
LS08 – DHCPv4

- Praxis-Teil:
  Einrichten DHCPv4-Dienst und DHCP-Relay-Agent

- Theorie-Teil:
  Grundlagen DHCPv4

Aufgabe

Idealtec GmbH benötigt DHCPv4-Dienst. Der DHCPv4-Dienst soll auf dem DC-Muenchen eingerichtet werden und die Netze Muenchen und Berlin bedienen.



Ihre Aufgaben (siehe auch Abbildung oben **) sind:

- DHCP-Dienst-Muenchen einrichten
- DHCP-Relay-Agent auf dem Router CSR1 einrichten.
- WKS-B automatische IP-Adresse zuweisen

1. DHCP-Dienst (Rolle) auf DC-Muenchen einrichten

- ☒ Erstellen Sie einen Prüfpunkt (Snapshot) von DC-Muenchen:
  Hyper-V-Manger → rechtsklick auf Virtuellen Computer „DC-München“ → Prüfpunkt

- ☒ Prüfpunkt umbenennen:
  Schreiben Sie zum Prüfpunkt-Namen zusätzlich noch: vor DHCP-Installation

- ☒ Melden Sie sich am DC-Muenchen an.

- ☒ Installieren Sie den Dienst (Rolle) DHCP auf DC-Muenchen inklusive aller erforderlichen Features, die bei der Installation nachgefragt werden:

  Server-Manager aufrufen (über Windows-Suchfunktion – Tipp: An Taskleiste anheften) → Verwalten (rechts oben) → Rolle und Features hinzufügen → Weiter → „Rollenbasierte oder featurebasierte Installation“ aktiviert lassen und Weiter → „Einen Server aus dem Serverpool auswählen“ aktiviert lassen und Weiter → „DHCP-Server“ Häkchen setzen → Features hinzufügen → Weiter → Weiter → Weiter → Installieren → Schließen (nach Installationsende)

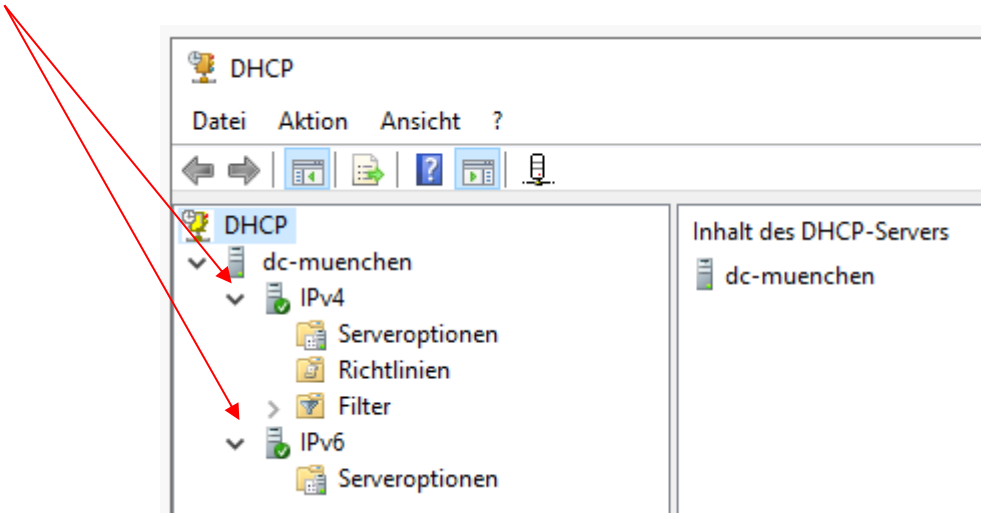
  Powershell (PS) – Commands

  Installation DHCP-Dienst:
  > Install-WindowsFeature DHCP -IncludeManagementTools

- ☒ Server-Manager → rechts oben gelbes Warnzeichen / Ausrufezeichen → DHCP-Konfiguration abschließen → Commit ausführen → Schließen

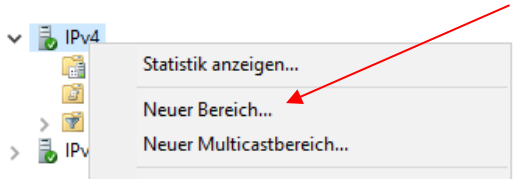
- ☒ Starten Sie den DHCP-Management-Tool:
  Server-Manager → Tools → DHCP

- ☒ Der DHCP-Dienst funktioniert einwandfrei, wenn Sie folgende Abbildung mit den grünen Häkchen sehen:



ITS11_LS8_DHCP_20240604_Yf.docx

☒ Wählen Sie mit der rechten Maustaste einen neuen IPv4-Bereich aus:



Powershell (PS) – Commands

Neuen IPv4-Bereich anlegen:
> Add-DHCPServerv4Scope 172.16.0.1 172.16.255.254 255.255.0.0 "IPv4_Adressbereich _Muenchen"

Achtung Zusammengeschrieben:
„IPv4_Adressbereich_Muenchen“

☒ Der neue IPv4-Adressbereich soll folgende Einstellungen haben:

	DHCP-Dienst-Muenchen
☒ Bereichsname	IPv4_Adressbereich_Muenchen
☒ Beschreibung	leer lassen
☒ IP-Adressbereich	Start-IP-Adresse: 172.16.0.1 End-IP-Adresse: 172.16.255.254
☒ Länge	16
☒ Subnetzmaske	255.255.0.0
☒ Ausschlüsse und Verzögerung	Schließen Sie die IP-Adressen des Routers (172.16.0.1) und die von DC-Muenchen (172.16.0.100) aus
☒ Subnetz-verzögerung	0
☒ Leasedauer	8 Tage (Standardwert lassen)
☒ DHCP-Optionen konfigurieren	ja
☒ Router-IP-Adresse (Standardgateway)	172.16.0.1 Tipp: „Hinzufügen“ klicken
☒ Domainname und DNS-Server	aktuell nicht erforderlich
☒ WINS-Server	nicht erforderlich
☒ Bereich aktivieren	ja

Powershell (PS) – Commands

IP-Adresse 172.16.0.1 ausschließen:
> Add-DhcpServerv4ExclusionRange -ScopeID 172.16.0.0 -StartRange 172.16.0.1 -EndRange 172.16.0.1

IP-Adresse 172.16.0.100 auch ausschließen (vorheriges Commando nochmals ausführen)

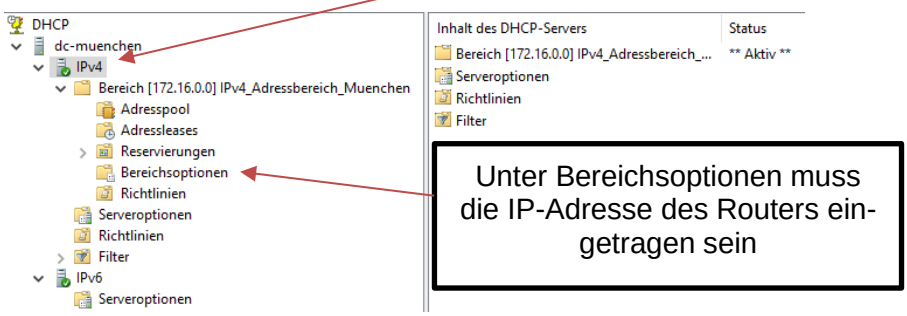
LeaseDuration 8 Tage setzen:
> Set-DhcpServerv4Scope -ScopeID 172.16.0.0 -LeaseDuration 8.00:00:00

Tipp LeaseDuration: Tage.Stunden:Minuten:Sekunden

Powershell (PS) – Commands

IP-Adresse Router und DNS:
>Set-DHCPServerv4OptionValue -ScopeID 172.16.0.0 -Router 172.16.0.1

☒ Überprüfen Sie ob der IPv4-Adressbereich angelegt worden ist und das grüne Häkchen vorhanden ist, ansonsten müssen Sie den IPv4-Adressbereich aktualisieren (rechte Maustaste → aktualisieren)



Unter Bereichsoptionen muss die IP-Adresse des Routers eingetragen sein

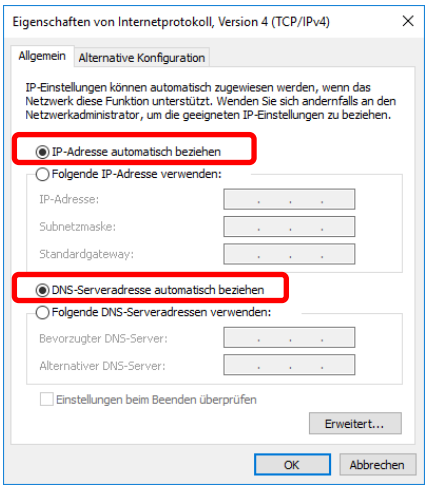
2. WKS-B automatische IP-Adresse beziehen einrichten

- ☒ Erstellen Sie einen Prüfpunkt (Snapshot) von WKS-B:
  Hyper-V-Manger → rechtsklick auf Virtuellen Computer „WKS-B“ → Prüfpunkt

- ☒ Prüfpunkt umbenennen:
  Schreiben Sie zum Prüfpunkt-Namen zusätzlich noch: vor DHCP-Installation

- ☒ Melden Sie sich am WKS-B an.

- ☒ Ändern Sie die die IP-Einstellungen von WKS-B auf IP-Adresse und DNS-Server automatisch beziehen.



3. Erster Versuch: WKS-B soll eine IPv4-Adresse vom DHCP-Dienst-Muenchen erhalten.

- ☒ Führen Sie das cmd-Fenster am WKS-B als Administrator aus, ansonsten haben Sie die notwendigen Rechte nicht:

  cmd-Fenster (nicht auf der Taskleiste) → rechte Maustaste → ausführen als Administrator

- ☒ Lesen Sie folgende Befehle und ihre Bedeutung durch, da sie wichtig sind.

Befehl	Bedeutung
ipconfig	Adressdaten des IP-Netzwerkes werden angezeigt
ipconfig /all	Adressdaten und weitere Informationen (Hostname, IP-DNS-Server…) werden angezeigt
ipconfig /release	IPv4-Adresse wird wieder freigegeben
ipconfig /renew	Ipv4-Adresse wird erneuert (Achtung: Der DHCP-Dienst vergibt dem Client aber immer wieder die selbe Ipv4-Adresse, da versucht wird Rechnern immer die gleiche Ipv4-Adresse im Netzwerk zu geben)
ipconfig /?	Hilfe mit allen Optionen und Beispielen für ipconfig

Nun wird versucht, ob die WKS-B eine IPv4-Adresse vom DHCP-Dienst-Muenchen erhalten kann.

ITS11_LS8_DHCP_20240604_Yf.docx

☒ Kreuzen Sie Ihre Vermutung an, ob das zum jetzigen Stand möglich ist:

[ ] ja [X] nein

☒ Erneuern Sie die IPv4-Adresse des WKS-B (ipconfig /renew), dieser Vorgang kann ein paar Minuten dauern.

☒ Lassen Sie sich die IPv4-Adresse des WKS-B anzeigen (ipconfig /all).

☒	Schreiben Sie die IPv4-Adresse des WKS-B auf:	169.254.255.6
☒	Schreiben Sie die Subnetzmaske des WKS-B auf:	255.255.0.0
☒	Ist die IPv4-Adresse des DHCP-Servers angegeben?	[ ] ja [X] nein
☒	Ist die IPv4-Adresse vom Standardgateway angegeben?	[ ] ja [X] nein

☒ Hat die WKS-B eine IPv4-Adresse, keine APIPA-Adresse (169.254.X.X /16), vom DHCP-Dienst-Muenchen erhalten?

[X] ja [ ] nein

Hintergrundinformation:

APIPA-Adresse bedeutet (169.254.X.X /16), dass der WKS-B keine IP-Adresse von einem DHCP-Server erhalten hat. In diesem Fall vergibt sich der WKS-B selber eine APIPA-Adresse. Mit der APIPA-Adresse kann der WKS-B nur im APIPA-Netz (169.254.X.X /16) kommunizieren und nicht mit den Standorten Berlin und München.

Beantworten Sie die unteren Fragen (durch den grauen Doppelpfeil gekennzeichnet) in schriftlicher Form mit „Quiz-1“. Das Quiz-1 befindet sich in Ihrem Klassenlaufwerk, wo auch dieses Dokument abgelegt ist.

Quiz-1

☒ Hat der DHCP-Dienst-Muenchen die IPv4-Anfrage (DHCP-Discover) des WKS-B erhalten?

[ ] ja [x] nein

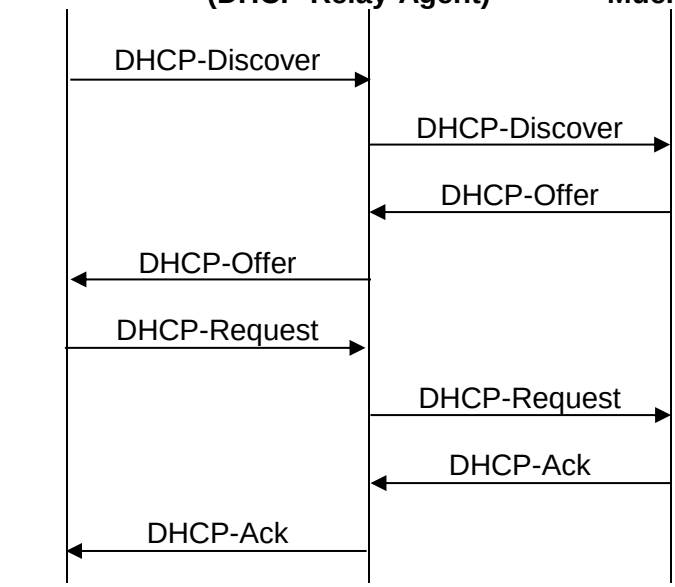
☒ Begründung:

Am Router ist das DHCP-Relay nicht richtig oder gar nicht konfiguriert / eingeschaltet

☒ Lösung:

Das DHCP-Relay am Router einrichten

☒ Kreuzen Sie an, ob die Pakete Unicast bzw. Broadcast sind:



	Paket	
	Unicast	**Broadcast**
DHCP-Discover	[ ]	[x]
DHCP-Discover	[x]	[ ]
DHCP-Offer	[x]	[ ]
DHCP-Offer	[ ]	[x]
DHCP-Request	[ ]	[x]
DHCP-Request	[x]	[ ]
DHCP-Ack	[x]	[ ]
DHCP-Ack	[ ]	[x]

ITS11_LS8_DHCP_20240604_Yf.docx

4. DHCP-Relay-Agent am Router einrichten:

- ☒ Wechseln Sie zum Router CSR1

  Tipp: Nehmen Sie als Hilfestellung die bereits bekannten Kommandos für den Cisco-Router aus den PDF-Dokumenten „Sheets IB_CheatSheet_Cisco-CLI…“ (siehe Klassenlaufwerk: Übung Inbetriebnahme_der_virtuellen_Systemplattform)

- ☒ Konfigurieren Sie am Router den DHCP-Relay-Agent auf der Schnittstelle „GigabitEthernet1“, damit die DHCP-Discover und DHCP-Request des WKS-B an den DHCP-Dienst-Muenchen weitergeleitet werden:

  Router(config-if)# ip helper-address 172.16.0.100

  Tipp 1:
  Sie können den installierten DHCP-Relay-Agent anzeigen:

  Router# show ip helper-address

  Tipp 2:
  Wenn Sie sich vertippt haben, können Sie den DHCP-Relay-Agent wieder löschen:

  Router(config-if)# no ip helper-address 172.16.0.100

- ☒ Speichern Sie die Konfiguration am Router

5. Zweiter Versuch mit DHCP-Relay-Agent: WKS-B soll eine IPv4-Adresse vom DHCP-Dienst-Muenchen erhalten.

- ☒ Melden Sie sich am WKS-B an.

- ☒ Führen Sie das cmd-Fenster am WKS-B als Administrator aus, ansonsten haben Sie die notwendigen Rechte nicht:

  cmd-Fenster (nicht auf der Taskleiste) → rechte Maustaste -> ausführen als Administrator

  Nun wird noch einmal versucht, ob WKS-B eine IPv4-Adresse vom DHCP-Dienst-Muenchen erhalten kann.

- ☒ Kreuzen Sie wieder Ihre Vermutung an, ob das zum jetzigen Stand möglich ist:

  [ ] ja [X] nein

- ☒ Erneuern Sie die IPv4-Adresse des WKS-B (ipconfig /renew), dieser Vorgang kann ein paar Minuten dauern.

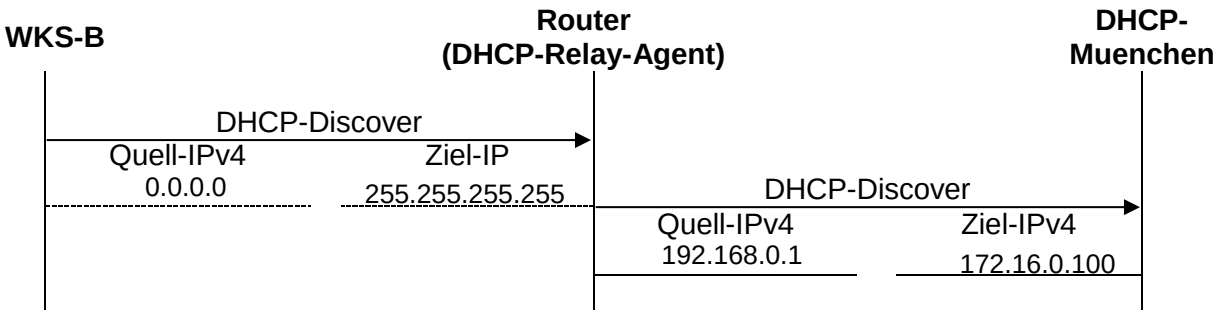
- ☒ Lassen Sie sich die IPv4-Adresse des WKS-B anzeigen (ipconfig /all).

☒ Hat die WKS-B eine IPv4-Adresse, keine APIPA-Adresse (169.254.X.X /16), vom DHCP-Dienst-Muenchen erhalten?

[ ] ja [X] nein

☐ Ergänzen Sie die untere Abbildung mit den entsprechenden Quell- und Ziel-IP-Adressen anhand Quiz-2. Das Quiz-2 befindet sich in Ihrem Klassenlaufwerk, wo auch dieses Dokument abgelegt ist.

Quiz-2



ITS11_LS8_DHCP_20240604_Yf.docx

Quiz-3

☒ Kontrollieren Sie zuerst mit Quiz-3 die oben angekreuzte ja-nein-Antwort. Sollte Ihre Antwort falsch gewesen sein, korrigieren Sie es bitte. Das Quiz-3 befindet sich in Ihrem Klassenlaufwerk, wo auch dieses Dokument abgelegt ist.

☒ Begründung:

Da der DHCP-Dienst-Muenchen den DHCP-Discorver vom Relay Agent aus dem 192.168.0.0 Netz erhält, kann der DHCP-Dienst-Muenchen dem WKS-B keine IPv4-Adresse vergeben. Der DHCP-Dienst-Muenchen kann aktuell nur IPv4-Adressen aus dem Bereich 172.16.0.0 vergeben.

☒ Lösung:

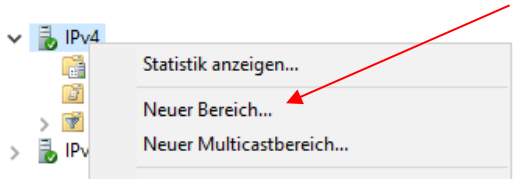
Am DHCP-Dienst-Muenchen muss auch der IPv4-Adressbereich vom DHCP-Dienst-Berlin (192.168.0.0) konfiguriert werden.

6. Einrichten des IPv4-Netz-Berlin (192.168.0.0 /24) am DHCP-Dienst-Muenchen

☐ Melden Sie sich am DC-Muenchen an.

☐ Starten Sie den DHCP-Management-Tool:
Server-Manager → Tools → DHCP

☐ Wählen Sie mit der rechten Maustaste einen neuen IPv4-Bereich aus:



Powershell (PS) – Commands

Neuen IPv4-Bereich anlegen:
> *Add-DHCPServerv4Scope 192.168.0.1 192.168.0.254 255.255.255.0 "IPv4_Adressbereich _Berlin"*

Achtung Zusammengeschrieben:
„IPv4_Adressbereich_Berlin“

☐ Der neue IPv4-Adressbereich soll folgende Einstellungen haben:

	DHCP-Dienst-Muenchen
☐ Bereichsname	IPv4_Adressbereich_Berlin
☐ Beschreibung	leer lassen
☐ IP-Adressbereich	Start-IP-Adresse: 192.168.0.1 End-IP-Adresse: 192.168.0.254
☐ Länge	24
☐ Subnetzmaske	255.255.255.0
☐ Ausschlüsse und Verzögerung	Schließen Sie die IP-Adressen des Routers (192.168.0.1) und die von DC-Berlin (192.168.0.100) aus
☐ Subnetz-verzögerung	0
☐ Leasedauer	8 Tage (Standardwert lassen)
☐ DHCP-Optionen konfigurieren	ja
☐ Router-IP-Adresse (Standardgateway)	192.168.0.1 Tipp: „Hinzufügen“ klicken
☐ Domainname und DNS-Server	aktuell nicht erforderlich
☐ WINS-Server	nicht erforderlich
☒ Bereich aktivieren	ja

Powershell (PS) – Commands

IP-Adresse 192.168.0.1 ausschließen:
> Add-DhcpServerv4ExclusionRange -ScopeID 192.168.0.0 -StartRange 192.168.0.1 -EndRange 192.168.0.1

IP-Adresse 192.168.0.100 auch ausschließen (vorheriges Commando nochmals ausführen)

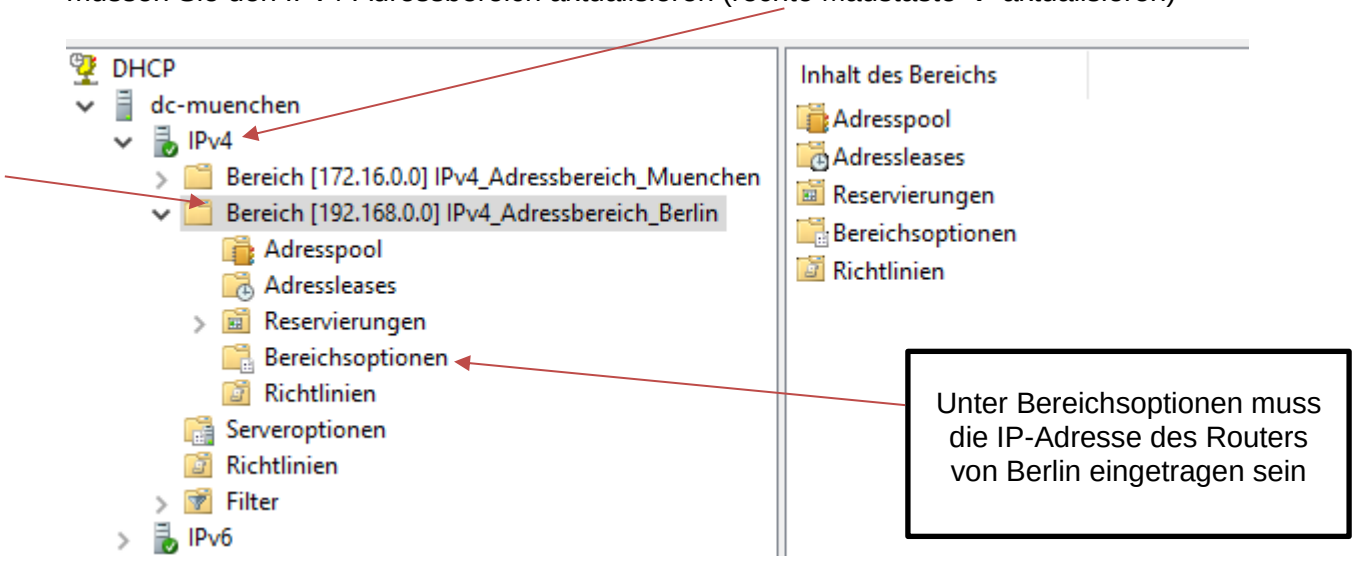
LeaseDuration 8 Tage setzen:
> *Set-DhcpServerv4Scope -ScopeID 192.168.0.0 -LeaseDuration 8.00:00:00*

Tipp LeaseDuration: Tage.Stunden:Minuten:Sekunden

Powershell (PS) – Commands

IP-Adresse Router und DNS:
>*Set-DHCPServerv4OptionValue -ScopeID 192.168.0.0 -Router 192.168.0.1*

☒ Überprüfen Sie, ob der IPv4_Adressbereich_Berlin (192.168.0.0) angelegt worden ist. Ansonsten müssen Sie den IPv4-Adressbereich aktualisieren (rechte Maustaste → aktualisieren)



ITS11_LS8_DHCP_20240604_Yf.docx

7. Dritter Versuch mit DHCP-Relay-Agent und IPv4_Adressbereich_Berlin: WKS-B soll eine IPv4-Adresse vom DHCP- Dienst-Muenchen erhalten

☒ Melden Sie sich am WKS-B an.

☒ Führen Sie das cmd-Fenster am WKS-B als Administrator aus, ansonsten haben Sie die notwendigen Rechte nicht:

cmd-Fenster (nicht auf der Taskleiste) → rechte Maustaste -> ausführen als Administrator

Nun wird versucht, ob die WKS-B eine IPv4-Adresse vom DHCP-Dienst-Muenchen erhalten kann.

☒ Kreuzen Sie wieder Ihre Vermutung an, ob das zum jetzigen Stand möglich ist:

[X] ja [ ] nein

☒ Erneuern Sie die IPv4-Adresse des WKS-B (ipconfig /renew).

X

☒ Lassen Sie sich die IPv4-Adresse des WKS-B anzeigen (ipconfig /all).

☒ Schreiben Sie die IPV4-Adresse des WKS-B auf:	192.168.0.2
☒ Schreiben Sie die Subnetzmaske des WKS-B auf:	255.255.255.0
☒ Schreiben Sie auf, wann die Lease erhalten wurde:	Do. 10.4.2025 15:25
☒ Schreiben Sie auf, wann die Lease abläuft wurde:	Freitag 18.4.25 15:25
☒ Schreiben Sie die IPV4-Adresse des DHCP-Servers auf:	192.168.0.1
☒ Schreiben Sie die IPV4-Adresse des Standardgateways auf:	172.16.0.100

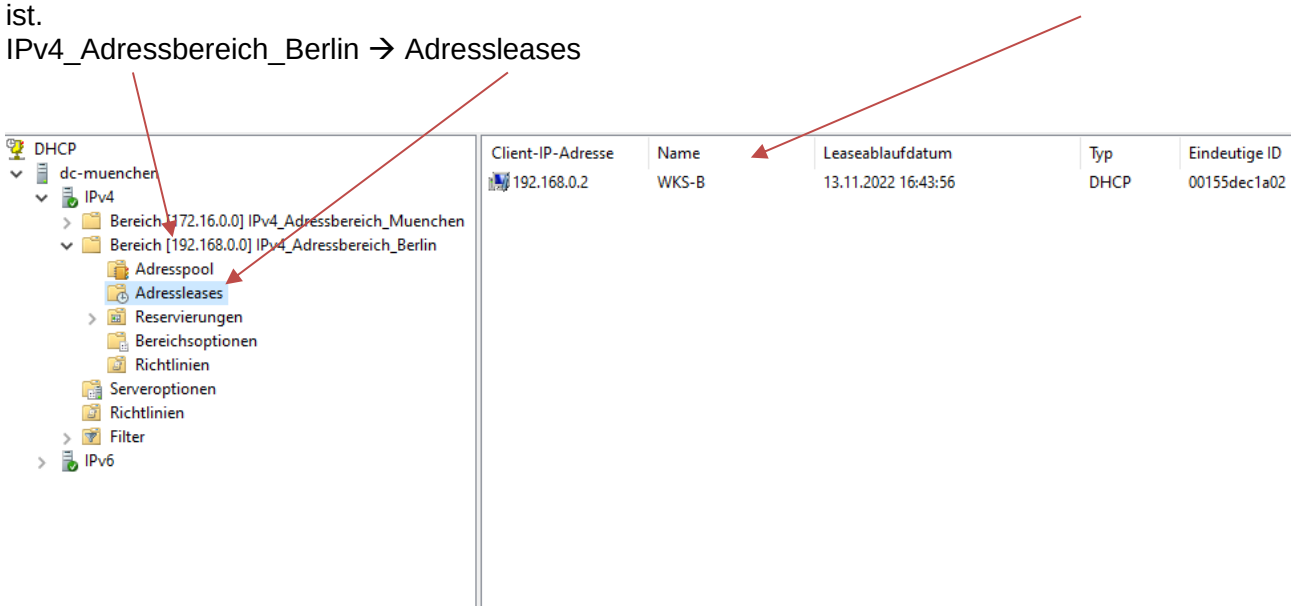
☒ Kreuzen Sie an, ob die WKS-B eine IPv4-Adresse aus dem Bereich IPv4_Adressbereich_berlin (192.168.0.0 /24) erhalten:

[X] ja [ ] nein

Wenn Sie mit nein angekreuzt haben, dann haben Sie einen Fehler gemacht. Finden und Verbessern Sie Ihren Fehler bis Sie mit ja antworten.

☒ Melden Sie sich am DC-Muenchen an.

☒ Überprüfen Sie am DHCP-Dienst-Muenchen, ob die IPv4-Adresse des WKS-B protokolliert ist.
IPv4_Adressbereich_Berlin → Adressleases



Herzlichen Glückwunsch! Sie haben erfolgreich einen DHCP-Dienst installiert und einen DHCP-Relay-Agent eingerichtet.

X

Theorie: DHCP für IPv4 (Dynamic Host Configuration Protocol)

1. Einführung

In einem TCP/IP-Netzwerk muss jedes angeschlossene Gerät (Arbeitsstationen, Server, Drucker, Router) mit einer eindeutigen IP-Adresse und anderen IP-Konfigurationen eingerichtet werden. Diese IP-Konfigurationen werden entweder manuell an jedem Client bzw. Computer eingerichtet oder automatisch von einem DHCP-Server bezogen.

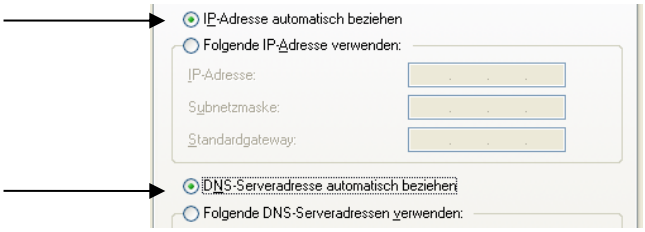
Nachteile der manuellen Einrichtung von IP-Konfigurationen durch den Menschen

- IP-Adressen können fälschlicherweise doppelt eingerichtet werden, da die bereits eingerichteten IP-Adressen nicht zentral verwaltet und protokolliert werden.
- Falls Veränderungen an den IP-Konfigurationen vorgenommen werden, sind manuelle Änderungen an den Clients erforderlich.
- Die manuelle Einrichtung an jedem Client ist sehr zeitaufwändig.
- …

Vorteile der automatischen Vergabe von IP-Konfigurationen durch einen DHCP-Server

- Die IP-Konfigurationen werden zentral verwaltet.
- Vergebene IP-Adressen werden protokolliert.
- Die doppelte Vergabe von IP-Adressen wird vermieden.
- Kein Zeitverlust mehr, da die IP-Konfiguration automatisch erfolgt.
- …

Am Windows-DHCP-Client müssen bei der Netzwerkkarte die IPv4-Einstellungen „IP-Adresse automatisch beziehen“ und „DNS-Serveradresse automatisch beziehen“ aktiviert werden, damit der Windows-DHCP-Client die IP-Konfigurationen vom DHCP-Server bezieht.



2. Mögliche IP-Konfigurationen

IP-Konfigurationen werden auf einem DHCP-Server in Scopes (IP-Adressbereich: Start-IP bis End-IP) verwaltet. Normalerweise wird pro Subnetz ein DHCP-Scope definiert. Auf einem DHCP-Server können in der Regel beliebig viele unterschiedliche Scopes definiert und verwaltet werden.

Ein Auszug für mögliche IP-Konfigurationswerte ist:

Pflicht
- **IP-Adresse**
- **Subnet-Maske**
- **IP-Lease-Time (Laufzeit der IP-Adresse und IP-Konfiguration)**

Optional
- **IP-Adressen des Routers (Standardgateway)**
- **IP-Adresse des DNS Servers**
- **DNS Domain Name**
- **IP-Adressen der NetBIOS Namensserver (typischerweise WINS Server)**
- **Node-Typ der NetBIOS Namensauflösung**
- **…**

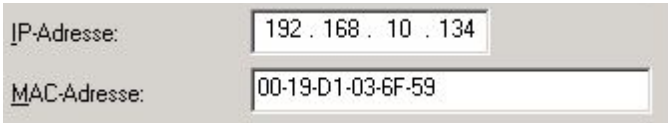
ITS11_LS8_DHCP_20240604_Yf.docx

3. IP-Adresszuordnung durch den DHCP-Servers

Folgende zwei Möglichkeiten der IP-Adresszuordnung durch den DHCP-Server werden in der Praxis angewendet:

a. Automatische IP-Zuweisung
In diesem Modus wird am DHCP-Server ein Bereich von IP-Adressen (range, z. B. 192.168.1.1 bis 192.168.1.254) festgelegt. Der DHCP-Server vergibt automatisch IP-Adressen aus dem IP-Adressbereich an die DHCP-Clients.

b. IP-Reservierung anhand der MAC-Adresse
In diesem Modus werden durch den Administrator am DHCP-Server die IP-Adressen zu bestimmten MAC-Adressen fest zugeordnet. Dadurch wird der DHCP-Client mit der entsprechenden MAC-Adresse immer diese IP-Adresse vom DHCP-Server zugewiesen bekommen.



Die IP-Reservierung ist notwendig, wenn der DHCP-Client immer unter der reservierten IP-Adresse erreichbar sein soll.

Beide Möglichkeiten können kombiniert werden.

4. Grundlagen DHCP

4.1 OSI-Schichten-Modell beim DHCP

OSI-Schichten		
Nummer	**Bezeichnung**	
5 bis 7	Anwendung	DHCP (IPv4-Config)
4	Transport	UDP DHCP-Server-Port: 67 DHCP-Client-Port: 68
3	Vermittlung	IPv4
2	Sicherung	MAC
1	Bitübertragung	Verkabelung

4.2 Kommunikationsablauf zwischen DHCP-Client und DHCP-Server

a. Erstmalige IP-Adresszuweisung für einen DHCP-Client

DHCP beruht auf einem Client-Server-Modell, bei welchem ein DHCP-Client bei jedem Startvorgang (Booten) mittels BOOTP (Bootstrap-Protokoll) mit einem DHCP-Server bezüglich der IP-Konfigurationen kommuniziert. Diese Kommunikation ist in vier Schritte aufgeteilt und wird als **DORA** (Discover, Offer, Request, Acknowledgement) bezeichnet. Erst nachdem das komplette DORA-Verfahren erfolgreich durchlaufen ist, aktiviert der DHCP-Client den TCP/IP-Protokollstack und verwendet erst danach die erhaltene IPv4-Adresse.

Wiresharkübung 1:
Folgende Übung können Sie an Ihrem Laptop oder an Ihrer VDI (Wireshark bereits vorinstalliert) durchführen. Sollten Sie Wireshark noch an Ihrem Laptop installieren müssen, finden Sie die Installationsdatei hier. Der Wireshark-Ausschnitt „Übung_1_DORA_Prinzip.pcap“ befindet sich in Ihrem Klassenlaufwerk, wo auch dieses Dokument abgelegt ist. Öffnen Sie den Wireshark-Ausschnitt „Übung_1_DORA_Prinzip.pcap“ mit dem Programm Wireshark und füllen Sie anhand des Ausschnittes die untere Grafik aus:

IPv4: ???
MAC: 00:0b:82:01:fc:42
DHCP-Client

DORA-Kommunikationsablauf

IPv4: 192.168.0.1
MAC: 00:08:74:ad:f1:9b
DHCP-Server

Q: Quelle = SRC :Source
Z: Ziel = DST: Destination

[ ] Unicast
[x] Broadcast
Discover

Q-IP	0.0.0.0	Z-IP	255.255.255.255
Q-MAC	00:0b:08:01:8c:41	Z-MAC	ff:ff:ff:ff:ff:ff

192.168.0.10	Z-IP	192.168.0.1	Q-IP
:42	Z-MAC	:9b	Q-MAC
Angebotene IPv4-Adresse:	01		
Subnetzmaske:	/24		
Leasetime:	1h		

[x] Unicast
[ ] Broadcast
Offer

[ ] Unicast
[x] Broadcast
Request

Q-IP	0.0.0.0	Z-IP	255.255.255.255
Q-MAC	:42	Z-MAC	ffffffffffff

10	Z-IP	1	Q-IP
	Z-MAC		Q-MAC

[ ] Unicast
[ ] Broadcast
Acknowledgement

ITS11_LS8_DHCP_20240604_Yf.docx

Zur Info:
In einigen Fällen muss der DHCP-Server Offer und Acknowledgement als Broadcast-Pakete senden. Das ist der Fall, wenn der DHCP-Client keine Unicast-Pakete annimmt, solange er keine gültige IPv4-Adresse hat. Siehe folgenden englischen Textausschnitt aus dem RFC 2131:

> *„Normally, DHCP servers and BOOTP relay agents attempt to deliver DHCPOFFER, DHCPACK and DHCPNAK messages directly to the client using uicast delivery. The IP destination address (in the IP header) is set to the DHCP 'yiaddr' address and the link-layer destination address is set to the DHCP 'chaddr' address. Unfortunately, some client implementations are unable to receive such unicast IP datagrams until the implementation has been configured with a valid IP address (leading to a deadlock in which the client's IP address cannot be delivered until the client has been configured with an IP address).*
>
> *A client that cannot receive unicast IP datagrams until its protocol software has been configured with an IP address SHOULD set the BROADCAST bit in the 'flags' field to 1 in any DHCPDISCOVER or DHCPREQUEST messages that client sends. The BROADCAST bit will provide a hint to the DHCP server and BOOTP relay agent to broadcast any messages to the client on the client's subnet. A client that can receive unicast IP datagrams before its protocol software has been configured SHOULD clear the BROADCAST bit to 0. The BOOTP clarifications document discusses the ramifications of the use of the BROADCAST bit [21].*
>
> *A server or relay agent sending or relaying a DHCP message directly to a DHCP client (i.e., not to a relay agent specified in the 'giaddr' field) SHOULD examine the BROADCAST bit in the 'flags' field. If this bit is set to 1, the DHCP message SHOULD be sent as an IP broadcast using an IP broadcast address (preferably 0xffffffff) as the IP destination address and the link-layer broadcast address as the link-layer destination address. If the BROADCAST bit is cleared to 0, the message SHOULD be sent as an IP unicast to the IP address specified in the 'yiaddr' field and the link-layer address specified in the 'chaddr' field. If unicasting is not possible, the message MAY be sent as an IP broadcast using an IP broadcast address (preferably 0xffffffff) as the IP destination address and the link-layer broadcast address as the link-layer destination address.“*

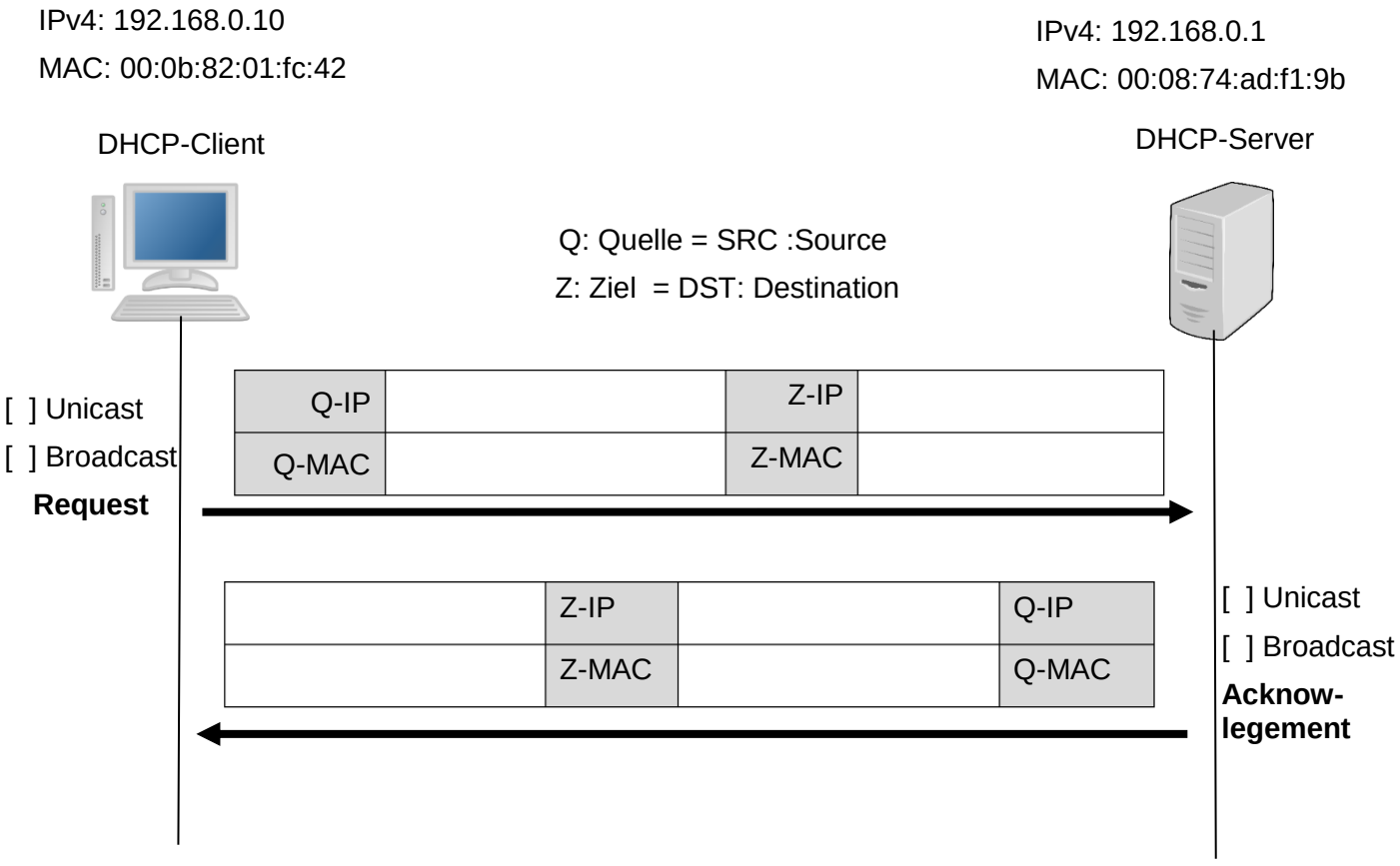
b. IP-Adresskonflikterkennung durch den Client

Der Client führt nach Durchlauf des DORA-Verfahrens bzw. nach Zuweisung der IP-Adresse eine Konflikterkennung der IP-Adresse nach ARP (Address Resolution Protocol) im Netz. Bei der Konflikterkennung über der Client im Netz, ob ein anderer Teilnehmer im Netz die gleiche IP-Adresse verwendet. Wenn der Client die gleiche IP-Adresse wie ein anderer Teilnehmer im Netz hat, sendet der Client ein DHCPDECLINE an den DHCP-Server und startet den DORA-Kommunikationsablauf nochmal neu.

c. Verlängern der Lease-Time (DHCP-Renewal) bei dynamischer IP-Zuordnung
Der DHCP Client kann seine Lease-Time, bevor diese abläuft, durch den DHCP-Server verlängern lassen. Die Lease-Time wird in der Regel bei 50% der abgelaufenen Zeit verlängert. Hierfür müssen gemäß dem Standard für DHCP-Renewal nur noch die Schritte Request und Acknowledgement durchlaufen werden:

- **Request**
  Der DHCP-Client sendet als Unicast eine DHCP-Request-Meldung, welche seine zuletzt bekommene IP-Adresse und die des entsprechenden DHCP Servers enthält.
- **Acknowledgement**
  Der entsprechende DHCP Server bestätigt dem DHCP Client die IP-Konfiguration mit einer DHCP-Acknowledgement-Meldung. Dabei können auch geänderte oder neue IP- Konfigurationswerte an den DHCP Client übergeben werden. Die Lease-Duration wird wieder erneuert.

DORA-Kommunikationsablauf für Lease-Time-Verlängerung



d. Lease-Time abgelaufen
Wenn der DHCP-Client auf seine DHCP-Request-Meldung gar keine Rückmeldung vom DHCP-Server bekommt und die Lease-Duration abgelaufen ist, darf der DHCP-Client die IP-Adresse nicht mehr verwenden. Aus diesem Grund wird daraufhin das volle vierstufige DHCP-Verfahren mit einem DHCP-Discover-Broadcast eingeleitet, um eine neue IP-Adresse von einem DHCP-Server zu erhalten.

ITS11_LS8_DHCP_20240604_Yf.docx

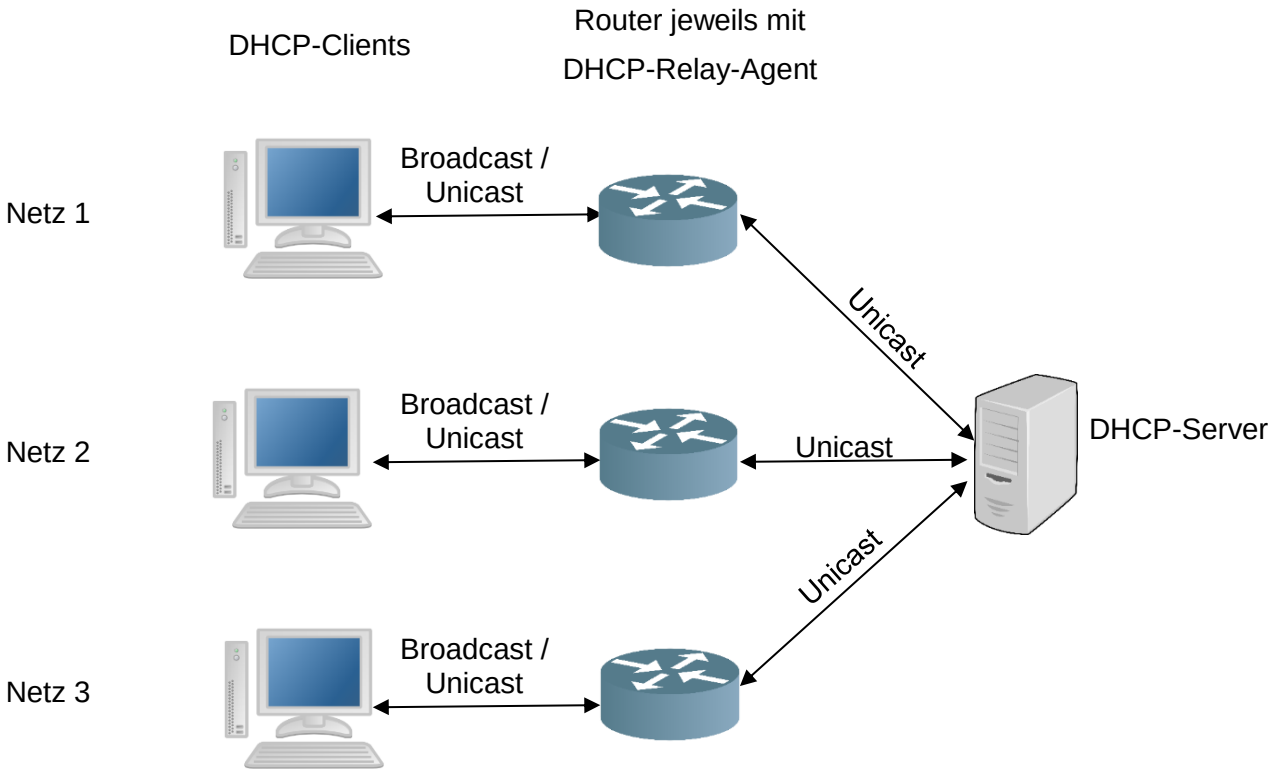
5. DHCP-Relay-Agent

Ein DHCP-Relay-Agent ermöglicht, dass ein DHCP-Server DHCP-Clients aus unterschiedlichen IP-Netzen bzw. Subnetzen bedient. Ohne den DHCP-Relay-Agent wären für jedes Netz bzw. Subnetz ein eigener DHCP-Server notwendig, da der Router die Broadcastpakete nicht in andere Netze bzw. Subnetze weiterleitet.

Funktionsweise:

Ein DHCP-Relay-Agent ist in einem Router implementiert. Der DHCP-Relay-Agent nimmt die DHCP-Broadcasts (Discover, Request) eines DHCP-Clients entgegen und leitet sie als Unicast an den DHCP-Server in einem anderen Netz bzw. Subnetz weiter. Der DHCP-Server antwortet (Offer, Acknowledgement) direkt an den DHCP-Relay-Agent als Unicast und der DHCP-Relay-Agent leitet diese Antwort (Offer, Acknowledgement) als Unicast weiter an den DHCP-Client.

Beispiel: Ein DHCP-Server ist für drei Netze bzw Subnetze zuständig



Broadcast: Paket geht an alle Teilnehmer im lokalen Netz

Unicast: Paket geht nur an einen Teilnehmer im lokalen Netz

Wiresharkübung 2 (Optionale Übung - Expertenwissen für Interessierte):

Füllen Sie den DORA-Kommunikationsablauf auf der nächsten Seite anhand der zwei Wireshark-Ausschnitte aus, die sich in Ihrem Klassenlaufwerk, wo auch dieses Dokument abgelegt ist, befinden:

- DHCP_Relay-From_DHCP-Client_to_Router.pcappng
- DHCP_Relay-From_Router_to_Central_DHCP-Server.pcappng

DORA-Kommunikationsablauf mit Relay-Agent

IPv4: ???

MAC: 50:00:22:22:22:22

DHCP-Client

Relay-Agent

IPv4: 192.168.1.1

MAC: 50:00:11:11:11:11

IPv4: 192.168.3.1

MAC: 50:48:00:01:00:02

Router

IPv4: 192.168.3.2

MAC: 50:48:00:04:00:00

DHCP-Server

Q: Quelle = SRC :Source

Z: Ziel = DST: Destination

Discover

Q-IP		Z-IP	
Q-MAC		Z-MAC	

Q-IP		Z-IP	
Q-MAC		Z-MAC	

Offer

	Z-IP		Q-IP
	Z-MAC		Q-MAC
Angebotene IPv4-Adresse:			
Subnetzmaske:			
Leasetime:			

	Z-IP		Q-IP
	Z-MAC		Q-MAC
Angebotene IPv4-Adresse:			
Subnetzmaske:			
Leasetime:			

Request

Q-IP		Z-IP	
Q-MAC		Z-MAC	

Q-IP		Z-IP	
Q-MAC		Z-MAC	

Acknow-ledgement

	Z-IP		Q-IP
	Z-MAC		Q-MAC

	Z-IP		Q-IP
	Z-MAC		Q-MAC

ITS11_LS8_DHCP_20240604_Yf.docx

6. APIPA (Automatic Private IP Addressing)

APIPA kommt zum Einsatz, wenn der Client keine gültige IPv4-Adresse hat, z. B. weil er

- ein IPv4-Adresskonflikt feststellt oder
- keine IPv4-Adresse vom DHCP-Server erhält.

In diesen Fällen vergibt sich der Client selbstständig eine IPv4-Adresse aus dem APIPA-Bereich.

Die Internet Assigned Numbers Authority (IANA) hat für APIPA den Klasse B-Adressbereich reserviert:

169.254.0.0 /16 → Hostadressbereich: 169.254.1.0 bis 169.254.254.255 (siehe RFC unten)

RFC 3927 2.1 (Textausschnitt)

> Link-Local Address Selection: When a host wishes to configure an IPv4 Link-Local address, it selects an address using a pseudo-random number generator with a uniform distribution in the range from 169.254.1.0 to 169.254.254.255 inclusive.
>
> The IPv4 prefix 169.254/16 is registered with the IANA for this purpose. The first 256 and last 256 addresses in the 169.254/16 prefix are reserved for future use and MUST NOT be selected by a host using this dynamic configuration mechanism.

Der Client sucht sich zufällig eine IPv4-Adresse aus APIPA-Bereich aus und prüft per ARP (Address Resolution Protocol) nach, ob die Adresse bereits verwendet wird.

Ein Rechner, der mit APIPA läuft und seine IPv4-Adresse vom DHCP-Server beziehen soll, hält alle fünf Minuten Ausschau nach einem DHCP-Server. Findet sich einer, verwirft der PC seine IP-Adresse und holt sich diese beim DHCP-Server.

Man kann durch Aufruf des Befehls ipconfig feststellen, welche IP-Adresse der Rechner zugewiesen bekommen hat. Man kann natürlich seinem Rechner auch manuell eine Adresse aus dem Bereich 169.254.0.0/16 zuweisen. Das hätte den Vorteil, dass man schnell dynamisch andere Rechner in das Netz integrieren kann. Ein Rechner, der APIPA aktiviert hat, kann mit Rechnern anderer Netznummern nicht kommunizieren.

APIPA abschalten

In Umgebungen, die auf einem DHCP-Server basieren, ist dieses Verhalten eventuell unerwünscht. Man kann es darum über die Registry abschalten.

Starten von Regedit.exe. Darin den folgenden Schlüssel anwählen:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces
Darin finden sich alle Interfaces. Hier wird das betroffene Interface gewählt. Darin wird aus dem Edit-Menü der Punkt New DWORD gewählt. Der Name muss IPAutoconfigurationEnabled lauten. Der Wert wird auf 0 gesetzt.

Einschränkungen

Aus naheliegenden Gründen, kann APIPA nicht über Router hinweg funktionieren. Die Anzahl der beteiligten Rechner sollte nicht zu hoch sein. In den Quellen findet man Empfehlungen von 25 bis 100 Rechnern maximal.

7. Anhang

DHCP-Nachrichten

DHCPDISCOVER	Ein Client ohne IP-Adresse sendet eine Broadcast-Anfrage nach Adress-Angeboten an alle DHCP-Server im lokalen Netz.
DHCPOFFER	Die DHCP-Server antworten mit entsprechenden Werten auf eine DHCPDISCOVER-Anfrage.
DHCPREQUEST	Der Client fordert eine der angebotenen IP-Adressen, weitere Daten sowie Verlängerung der Lease-Zeit von einem der antwortenden DHCP-Server.
DHCPACK	Bestätigung des DHCP-Servers zu einer DHCPREQUEST-Anforderung oder die Übermittlung von Konfigurationsparametern, die vorher durch DHCPINFORM vom Client angefordert wurden.
DHCPNAK	Ablehnung einer DHCPREQUEST-Anforderung durch den DHCP-Server.
DHCPDECLINE	Ablehnung durch den Client, da die IP-Adresse schon verwendet wird.
DHCPRELEASE	Der Client gibt die eigene Konfiguration frei, damit die Parameter wieder für andere Clients zur Verfügung stehen.
DHCPINFORM	Anfrage eines Clients nach weiteren Konfigurationsparametern, z. B. weil der Client eine statische IP-Adresse besitzt.

ITS11_LS8_DHCP_20240604_Yf.docx