

Titel: Labor03 – Stat. Routing & DHCP

Klasse: 4BHIF

Name: Haiden

Gruppe: 01

Aufgabe: 10.11.2020 **Abgabe:** 24.11.2020

Inhaltsverzeichnis

1	Theorie-Teil.....	1
1.1	Was ist DHCP?	1
1.2	Vergabevarianten des DHCP-Servers	1
1.3	Zuordnungsarten	1
1.3.1	Manuelle Zuordnung	2
1.3.2	Automatische Zuordnung.....	2
1.3.3	Dynamische Zuordnung.....	2
1.4	Nachrichten-Typen	2
1.5	Probleme bei DHCP	3
2	Übung	3
2.1	Konfigurieren Sie die Geräte damit benachbarte Geräte kommunizieren können (ping)	3
2.2	Tragen sie statische Routen ein damit alle Geräte kommunizieren können	3
2.2.1	Von 10er Subnet zu 30er Subnet und zurück	3
2.2.2	Von 30er Subnetz zu 50er Subnetz und zurück	5
2.2.3	Von 10er Subnetz in 50er Subnetz und zurück	6
2.3	Konfigurieren Sie am Router 1 einen DHCP Server für das 192.168.10.0er Netz	7
2.4	Analysieren Sie die Adresszuweisung mit dem Packettracer (genau!). Verwenden sie dazu den Simulationsmodus und zeigen sie die Paketdetails an.....	7
2.4.1	DHCP_DISCOVER	7
2.4.2	DHCP_OFFER	8
2.4.3	DHCP_REQUEST	8
2.4.4	DHCP_ACK (Acknowledge)	9
2.5	Konfigurieren Sie Pools für die anderen Netze. Wo müssen Sie die Helper-Adresse eintragen?	9

1 Theorie-Teil

<https://www.ip-insider.de/was-ist-dhcp-a-590923/>

https://doku.rz.tu-bs.de/doku.php?id=netz:dhcp:dhcp_fuer_alle

https://de.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol

<https://www.kunbus.de/dhcp.html>

1.1 Was ist DHCP?

DHCP steht für Dynamic Host Configuration Protocol und ist ein Kommunikationsprotokoll, mit dem sich automatisch Netzwerkkonfigurationen an einzelne Clients verteilen lassen können.

DHCP wurde im RFC 2131 („Dynamic Host Configuration Protocol“) und RFC 2132 („DHCP Options and BOOTP Vendor Extensions“) definiert, erstmals verwendet wurde es 1993. Es benützt die beiden UDP Ports 67 und 68. Seine Vorläufer waren das RARP (Reverse Address Resolution Protocol) und das Bootstrap Protocol (BOOTP), welches es weitestgehend in der heutigen Welt abgelöst hat. DHCP baut allerdings auf BOOTP auf und kann somit beschränkt mit BOOTP-Clients / Servern arbeiten.

DHCP-Server können beschränkt in manchen Implementierungen die Registrierung eines Gerätes bei einem DNS-Server übernehmen. DHCP findet sich auch im Verzeichnisdienst von Microsoft, AD (Active Directory) wieder, wo es für die Zuweisung von IP-Adressen an Domänenmitglieder sorgt.

1.2 Vergabevarianten des DHCP-Servers

op	Information, ob Anforderung (request = 1) oder antwort (reply = 2)
htype	Netztyp
hlen	Länge MAC-Adresse
Hops	Anzahl DHCP-Relay-Agents, optional
Xid	ID der Verbindung zwischen Client und Server
secs	Zeit in Sek. seit Start des Clients
flags	Zeigt an, ob Client noch gültige IP
ciaddr	Client-IP
yiaddr	Eigene IP
siaddr	Server-IP
giaddr	Relay-Agent-Adresse
chaddr	Client MAC-Adresse
sname	Name DHCP Server, optional
file	Name einer Datei, optional
options	bis zu 576 Bytes, verhandelbar, zusätzliche Optionen

32 Bit			
op	htype	hlen	hops
xid			
secs		flags	
ciaddr			
yiaddr			
siaddr			
giaddr			
chaddr			
sname			
file			
options			

1.3 Zuordnungsarten

Es kann zwischen manueller und dynamischer Zuordnung gewählt werden. Ist der Server gestartet worden, lauscht er auf UDP Port 67 auf etwaige Clients, die sich eine IP-Adresse holen möchten. In einer bearbeitbaren Konfigurationsdatei befinden sich Parameter, die zum Client gesendet werden, um ihn zu konfigurieren.

1.3.1 Manuelle Zuordnung

Wird auch statisches DHCP genannt. Dabei werden auf dem Server bestimmten MAC-Adressen eine feste IP-Adresse zugewiesen, welche auf unbestimmte Zeit festgelegt bleibt. Dies hat zur Folge, dass keine neuen Clients das Netzwerk betreten können. Dies hat den positiven Effekt, dass keine ungewollten Eindringlinge, z.B. Hacker, einfach in das Netzwerk können und sich dort umsehen können.

1.3.2 Automatische Zuordnung

Ist ähnlich dem manuellen System, hier erfolgt die Zuteilung der IP's zu den entsprechenden MACs allerdings automatisch. Wie bei dem manuellen System bleibt eine IP die mit ihrer MAC verknüpft ist auf unbestimmte Zeit verbunden.

1.3.3 Dynamische Zuordnung

Entspricht der automatischen Zuordnung, doch die Zuordnung ist auf eine bestimmte Zeit beschränkt. Besteht über der Lease-Time (Mietzeit) keine Verbindung, so löst der DHCP-Server die IP von ihrer MAC-Adresse und die IP wird frei für ein anderes Gerät, zu der sie zugewiesen werden kann. Die Lease-Time wird dem Client bei dem Verbindungsaufbau mitgeteilt. Aufgrund dieser Tatsache führt der Client nach der halben Zeit einen erneuten Request aus und zeigt so beim DHCP-Server das Interesse, die IP-Adresse zu behalten. Hat dieser Request nicht funktioniert, besteht die Verbindung trotzdem weiterhin, bis zu 7/8 der Lease-Time ein zweiter Request durchgeführt wird.

1.4 Nachrichten-Typen

DHCP-DISCOVER: Ein Client ohne gültige IP sendet einen Broadcast um Adress-Informationen über einen DHCP-Server zu bekommen

DHCP-OFFER: Der Server antwortet mit seinen entsprechenden Werten auf die DISCOVER-Anfrage

DHCP-REQUEST: Client fordert eine der angegebenen IP-Adressen, Lease-Time (Verlängerung)

DHCP-ACK: DHCP-Server bestätigt Anfrage

DHCP-NAK: DHCP-Server lehnt Anfrage von Client ab

DHCP-DECLINE: Ablehnung durch Client, wenn IP schon verwendet wird

DHCP-RELEASE: Client gibt seine Konfiguration frei, damit andere sie im Netzwerk verwenden können

DHCP-INFORM: Anfrage eines Clients nach weiteren Informationen, z.B. wenn er eine stat. IP besitzt

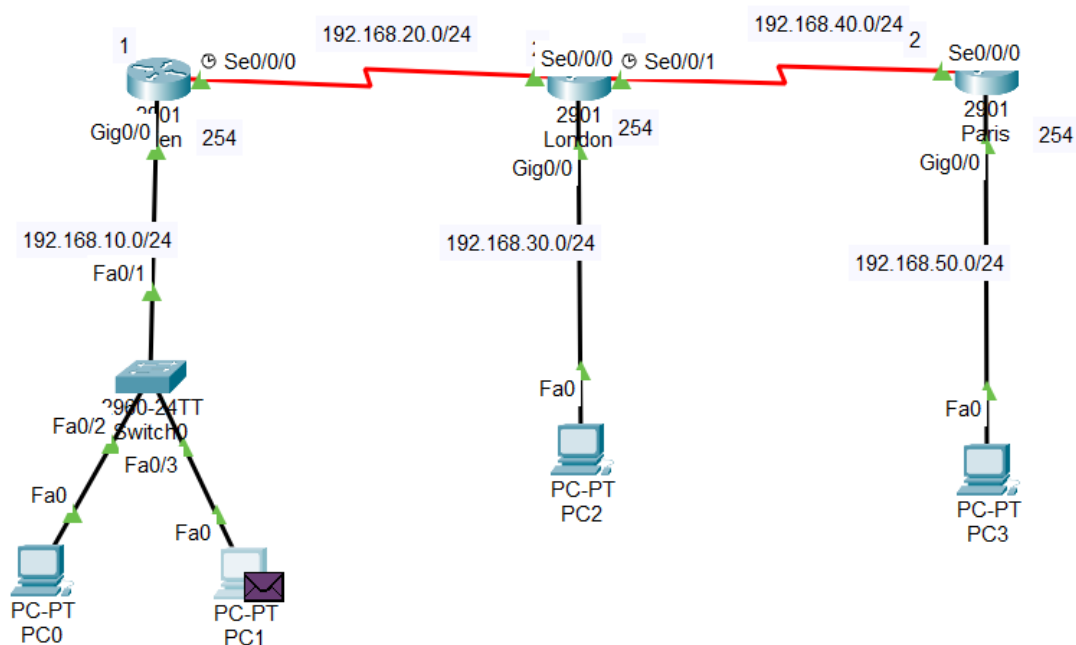
1.5 Probleme bei DHCP

DHCP kann man auf verschiedene Arten angreifen bzw. lahmlegen. Sind Server, welche die selbe IP-Range abdecken im Netzwerk, dann können diese doppelten Konfigurationen das Netzwerk lahmlegen.

Die manuellen und automatischen Zuweisungen von IP-Adressen kann auch relativ einfach durch gefälschte MAC-Adressen hervorgerufen werden.

2 Übung

2.1 Konfigurieren Sie die Geräte damit benachbarte Geräte kommunizieren können (ping)



2.2 Tragen sie statische Routen ein damit alle Geräte kommunizieren können

Mit dem ip-route Kommando kann man Routen zwischen einzelnen Subnets festlegen.

Pattern:

```
ip route <ZIEL-SUBNET> <SUBNETZ-MASKE> <HOP-DEVICE>
```

Das HOP-Device ist in diesem Fall das Gerät, welches einen Zugang zu dem Ziel-Subnet hat, so dass das Paket in das richtige Subnet kommt.

2.2.1 Von 10er Subnet zu 30er Subnet und zurück

Beim „Wien“-Router:

```
WIEN(config)#ip route 192.168.30.0 255.255.255.0 192.168.20.2
```

Damit Paket wieder zurück kommt, wird beim „London“ Router eine Route in der entgegengesetzten Richtung erstellt:

```
LONDON(config)#ip route 192.168.10.0 255.255.255.0 192.168.20.1
```

2.2.1.1 Test der Route

Nach dem wir die Routen definiert haben, versuchen wir, ob ein einfaches ICMP Paket von dem PC, der in Wien hängt und an den PC, der an dem Router in London hängt, hin und zurück geschickt bekommen.

7.014	--	PC0	ICMP
7.015	PC0	Switch0	ICMP
7.016	Switch0	Wien	ICMP
7.017	Wien	London	ICMP
7.018	London	PC2	ICMP
7.019	PC2	London	ICMP
7.020	London	Wien	ICMP
7.021	Wien	Switch0	ICMP
Visible 7.022	Switch0	PC0	ICMP

Wie man sieht, geht das Paket zuerst zum Switch, woraufhin es an den Router weitergeleitet wird. Dieser weiß nun dank der Hop-IP zu welchem Router er es schicken muss. So geht das Paket zu London und dort weiß der Router, an welches Device im Netzwerk, in dem Fall PC2, er das Paket schicken muss. Dort kommt es an und dann kommt unsere umgekehrte Route ins Spiel, welche es uns ermöglicht, das Paket wieder zurück zu schicken, nach demselben Schema, eben nur umgekehrt, wie oben beschrieben.

```
C:\>ping 192.168.30.2
```

```
Pinging 192.168.30.2 with 32 bytes of data:
```

```
Reply from 192.168.30.2: bytes=32 time=8ms TTL=126
```

```
Reply from 192.168.30.2: bytes=32 time=8ms TTL=126
```

Dieser Test funktioniert auch von PC2 zu PC0:

0.000	--	PC2	ICMP
0.001	PC2	London	ICMP
0.002	London	Wien	ICMP
0.003	Wien	Switch0	ICMP
0.004	Switch0	PC0	ICMP
0.005	PC0	Switch0	ICMP
0.006	Switch0	Wien	ICMP
0.007	Wien	London	ICMP
0.008	London	PC2	ICMP

```
C:\>ping 192.168.10.2
```

```
Pinging 192.168.10.2 with 32 bytes of data:
```

```
Reply from 192.168.10.2: bytes=32 time=8ms TTL=126
```

2.2.2 Von 30er Subnetz zu 50er Subnetz und zurück

Von 30er in 50er Subnetz:

Am London Router geben wir folgendes ein, nach dem selben Schema wie bei der ersten Route:

```
LONDON(config)#ip route 192.168.50.0 255.255.255.0 192.168.40.2
```

Danach müssen wir noch die Rück-Route wie beim ersten Beispiel definieren, damit Pakete zurückgelangen können:

```
PARIS(config)#ip route 192.168.30.0 255.255.255.0 192.168.40.1
```

2.2.2.1 Test der Route

Test von PC2 zu PC3:

12.010	--	PC2		ICMP
12.011	PC2	London		ICMP
12.012	London	Paris		ICMP
12.013	Paris	PC3		ICMP
12.014	PC3	Paris		ICMP
12.015	Paris	London		ICMP
12.016	London	PC2		ICMP

```
C:\>ping 192.168.50.2
```

```
Pinging 192.168.50.2 with 32 bytes of data:
```

```
Reply from 192.168.50.2: bytes=32 time=6ms TTL=126
```

Test von PC3 zu PC2:

0.000	--	PC3		ICMP
0.001	PC3	Paris		ICMP
0.002	Paris	London		ICMP
0.003	London	PC2		ICMP
0.004	PC2	London		ICMP
0.005	London	Paris		ICMP
0.006	Paris	PC3		ICMP

```
C:\>ping 192.168.30.2
```

```
Pinging 192.168.30.2 with 32 bytes of data:
```

```
Reply from 192.168.30.2: bytes=32 time=6ms TTL=126
```

2.2.3 Von 10er Subnetz in 50er Subnetz und zurück

Hier brauchen wir mehr als 2 Hops. Damit das Paket von einem PC, der sich im 10er Subnetz befindet, zu einem PC, der sich im 50er Subnet aufhält, kommen kann, muss das Paket über alle 3 Router (wien, London, Paris) hoppen. Da London bereits nach Paris und Wien routen kann, müssen wir nur den beiden Routern WIEN und PARIS sagen, wohin sie das Paket, welches sein Ziel-Subnetz erreichen will, leiten soll. Dies wäre in diesem Fall der London-Router, der den Mittelmännchen spielt.












Wien-Router:

```
WIEN(config)#ip route 192.168.50.0 255.255.255.0 192.168.20.2
```

Paris-Router:

```
PARIS(config)#ip route 192.168.10.0 255.255.255.0 192.168.40.1
```

Test von PC0 zu PC3:

0.000	--	PC0		ICMP
0.001	PC0	Switch0		ICMP
0.002	Switch0	Wien		ICMP
0.003	Wien	London		ICMP
0.004	London	Paris		ICMP
0.005	Paris	PC3		ICMP
0.006	PC3	Paris		ICMP
0.007	Paris	London		ICMP
0.008	London	Wien		ICMP
0.009	Wien	Switch0		ICMP
0.010	Switch0	PC0		ICMP

Von PC3 zu PC0:

Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	PC3	ICMP
	0.001	PC3	Paris	ICMP
	0.002	Paris	London	ICMP
	0.003	London	Wien	ICMP
	0.004	Wien	Switch0	ICMP
	0.005	Switch0	PC0	ICMP
	0.006	PC0	Switch0	ICMP
	0.007	Switch0	Wien	ICMP
	0.008	Wien	London	ICMP
	0.009	London	Paris	ICMP
	0.010	Paris	PC3	ICMP

2.3 Konfigurieren Sie am Router 1 einen DHCP Server für das 192.168.10.0er Netz

Mit `ip dhcp pool <NAME>` erstellt man einen neuen DHCP Pool, bzw. wechselt in einen existierenden.

Danach gibt man mit `network <SUBNET> <MASK>` das gewünschte Subnet sowie die zugehörige Subnetz-Maske an.

```
WIEN(config)#ip dhcp pool nvslab
WIEN(dhcp-config)#network 192.168.10.0 255.255.255.0
```

2.4 Analysieren Sie die Adresszuweisung mit dem Packettracer (genau!). Verwenden sie dazu den Simulationsmodus und zeigen sie die Paketdetails an.

2.4.1 DHCP_DISCOVER

Der PC, welcher ohne eine gültige IP da steht, sendet ein DHCP_Discover per Broadcast an alle Geräte im Netzwerk, um einen DHCP-Server zu finden.

Die Broadcast-Adresse ist zu erkennen an der Destination „255.255.255.255“.

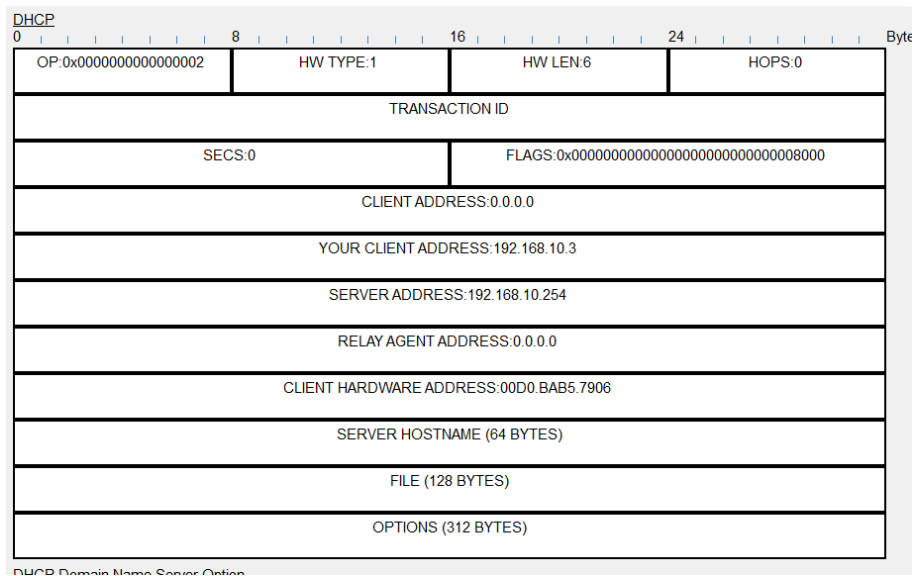
IP 0	4	8	16	20	24	Bits
VER:4	IHL:5	DSCP:0x00	TL:77			
	ID:0x0045	FLAGS:0x0	FRAG OFFSET:0x000			
TTL:128	PRO:0x11	CHKSUM				
SRC IP:0.0.0.0						
DST IP:255.255.255.255						
DATA (VARIABLE LENGTH)						

UDP

2.4.2 DHCP_OFFER

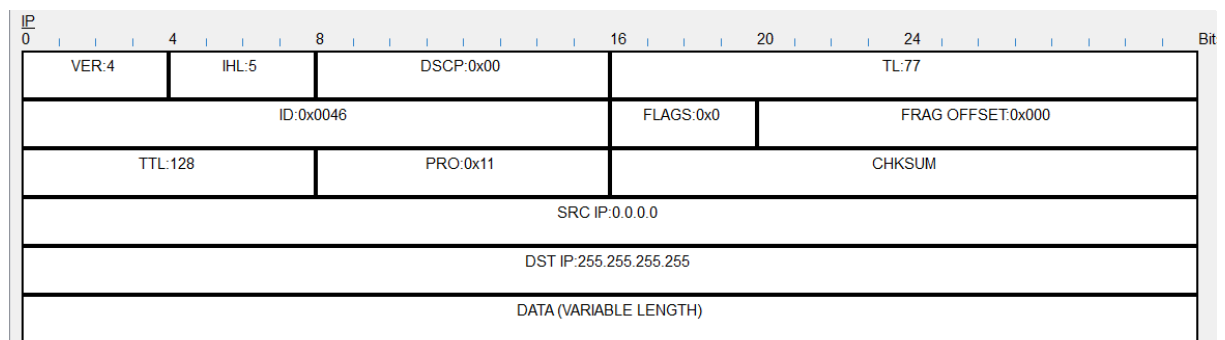
Der Router, welcher den Adressen-Pool beherbergt, antwortet und bietet eine IP-Adresse aus seinem Pool an.

Zu erkennen ist das OFFER anhand der SRC_IP „192.168.10.254“, dies ist die IP des Routers im Netzwerk, auf welchem der DHCP-Server läuft.



2.4.3 DHCP_REQUEST

Der Client fordert nun eine IP-Adresse an und sendet dafür wieder einen Broadcast hinaus.



2.4.4 DHCP_ACK (Acknowledge)

DHCP																																Bytes			
0								8								16								24											
OP:0x0000000000000002								HW TYPE:1								HW LEN:6								HOPS:0											
TRANSACTION ID																																			
SECS:0																FLAGS:0x000000000000000000000000000008000																			
CLIENT ADDRESS:0.0.0.0																																			
YOUR CLIENT ADDRESS:192.168.10.3																																			
SERVER ADDRESS:192.168.10.254																																			
RELAY AGENT ADDRESS:0.0.0.0																																			

Der DHCP-Server bestätigt die Anfrage und der Client erhält seine neue IP-Adresse (in dem Fall 192.168.10.3).

2.5 Konfigurieren Sie Pools für die anderen Netze. Wo müssen Sie die Helper-Adresse eintragen?

Helper-Adresse an Interface des angeschlossenen Netzes:

```
WIEN(config-if)#ip helper-address 192.168.20.1
```

Einrichten des Pools für das andere Netz

```
LONDON(config)#ip dhcp pool net2pool
```

```
LONDON(dhcp-config)#network 192.168.30.0 255.255.255.0
```

PC0:

```
C:\>ipconfig
```

```
FastEthernet0 Connection:(default port)
```

```
Connection-specific DNS Suffix...:
```

```
Link-local IPv6 Address.....: FE80::2D0:BAFF:FEB5:7906
```

```
IPv6 Address.....: ::
```

```
Autoconfiguration IPv4 Address...: 192.168.30.3
```

```
Subnet Mask.....: 255.255.255.0
```

```
Default Gateway.....: 192.168.30.254
```