

## Inhalt

Szenario .....	2
IST-Situation.....	2
Ziele und Einschränkungen .....	2
Planung der Migration.....	2
Ablauf der Migration aus der Sicht der DHCP-Server .....	2
Phase 1 – Vorbereitung .....	2
Phase 2 – Erstellen der neuen Scopes.....	3
Phase 3 – Deaktivierung der alten Scopes .....	3
Phase 4 – Portierung der Leases auf den neuen Server .....	4
Phase 5 – Aktivierung der neuen Scopes .....	5
Phase 6 – Aktivierung des DHCP-Failovers .....	5
Ablauf der Migration aus der Sicht eines Clients .....	6
Address-Lease vom alten DHCP .....	6
Lease-Renew zum alten DHCP .....	6
Lease-Renew nach der Migration .....	7

## Szenario

### IST-Situation

In meinem LAB werden Clients mit IPv4-Adressen über zwei DHCP-Server versorgt. Die Adressen der einzelnen Subnetze sind in zwei gleich große Adressräume aufgeteilt, von denen jeder jeweils einem DHCP-Server zugewiesen wurde (Split-Scope). So können Clients Adressen für jedes Subnetz erhalten – auch wenn mal ein Server ausfallen sollte.

Beide Server laufen mit Windows Server. Das Szenario wäre für alle Versionen ab Windows Server 2008 R2 denkbar.

Die Clients fragen die IPv4-Adressen nicht direkt an. Das übernehmen DHCP-Relayagents (iphelper) auf den Routern.

### Ziele und Einschränkungen

Die beiden alten Server sollen durch neue Server ersetzt werden. Unterbrechungen in der Adressvergabe sind zu vermeiden. Die neue Lösung soll ebenfalls höher verfügbar sein.

Die IP-Adressen der DHCP-Server können nicht wiederverwendet werden. (Das könnte z.B. durch andere Services verursacht werden, die auf den gleichen, alten Servern laufen, aber die jetzt noch nicht portiert werden können)

### Planung der Migration

Die neuen Server werden das Feature DHCP-Failover für die Verfügbarkeit verwenden. Dies steht seit Windows Server 2012 zur Verfügung.

Da die Altsysteme weiter als Nicht-DHCP-Server in Betrieb bleiben und die IP-Adresse der Server nicht mitgenommen werden kann, sind die Verfahren „Inplace-Upgrade“ (Aktualisierung des alten Betriebssystems) und „Wipe-and-Load“ (Austausch des Altsystems durch ein gleichkonfiguriertes mit gleichem Namen und gleicher IP-Adresse) nicht möglich. Es bleibt also nur eine Migration im „Side-by-Side“-Verfahren.

Die Migration teile ich in 6 Phasen. Diese können auf einzelne Scopes heruntergebrochen werden. Es muss also keine „Big-Bang“-Migration sein: man kann ein Netzwerksegment nach dem nächsten umziehen.

Bei der Migration werden je Scope mehrere Arbeitsschritte erforderlich:

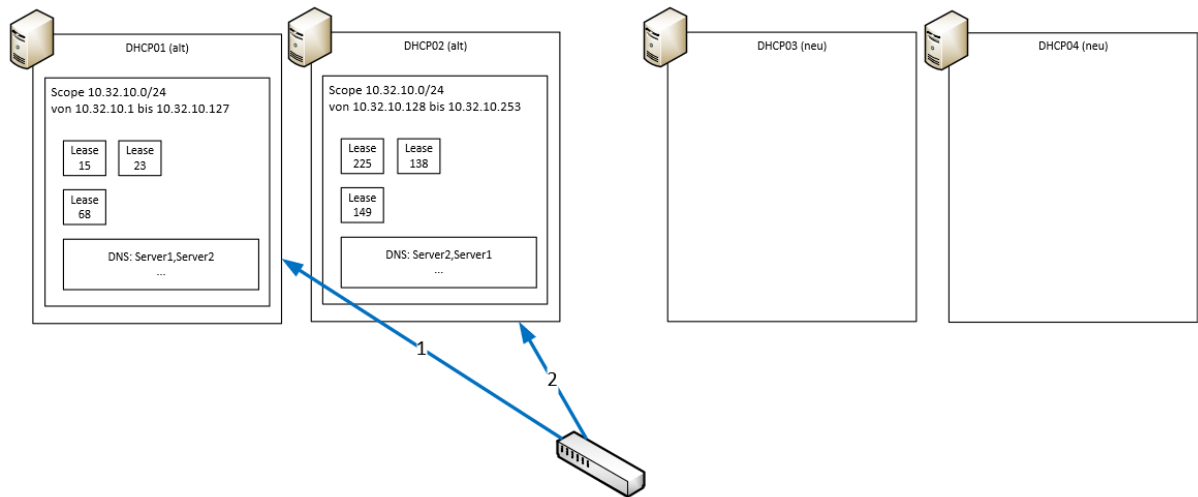
- 1) Der Scope auf dem alten DHCP-Server wird deaktiviert. So können keine weiteren IPv4-Adressen ausgestellt werden.
- 2) Alle aktiven Leases werden aus dem Scope des alten DHCP-Servers in den vorbereiteten Scope auf dem neuen DHCP-Server importiert.
- 3) Der Scope auf dem neuen Server wird aktiviert.
- 4) Optional müssen jetzt noch DHCP-RelayAgents auf den neuen DHCP-Server verweisen

## Ablauf der Migration aus der Sicht der DHCP-Server

In diesem Abschnitt erläutere ich die 6 Migrationsphasen, in denen ich die einzelnen Arbeitsschritte erläutere.

### Phase 1 – Vorbereitung

Schema:



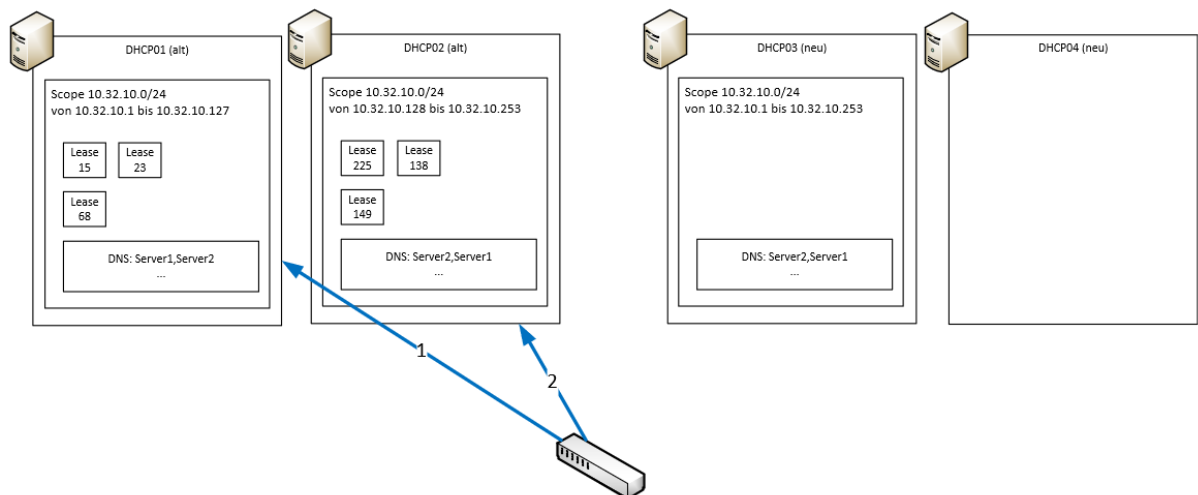
In dieser Phase werden parallel zu den beiden alten Servern zwei neue DHCP-Server aufgesetzt. Diese haben noch keine Scopes und sie verwenden andere IPv4-Adressen als die alten Server. Die DHCP-Relayagents (iphelper) auf den Switches zeigen auf die beiden alten Systeme.

Im Bestand ist der Adressraum je Subnetz geteilt (Split-Scope), damit der Ausfall eines DHCP kompensiert werden kann. Beide Server haben Leases vergeben.

In dieser Phase wird es keine Service-Unterbrechung geben.

### Phase 2 – Erstellen der neuen Scopes

Schema:



Auf dem ersten neuen Server werden die Scopes neu erstellt. Sie bleiben deaktiviert, damit eine Mehrfachvergabe ausgeschlossen werden kann. Die IP-Adressräume der beiden alten Server werden dabei zusammengefasst:

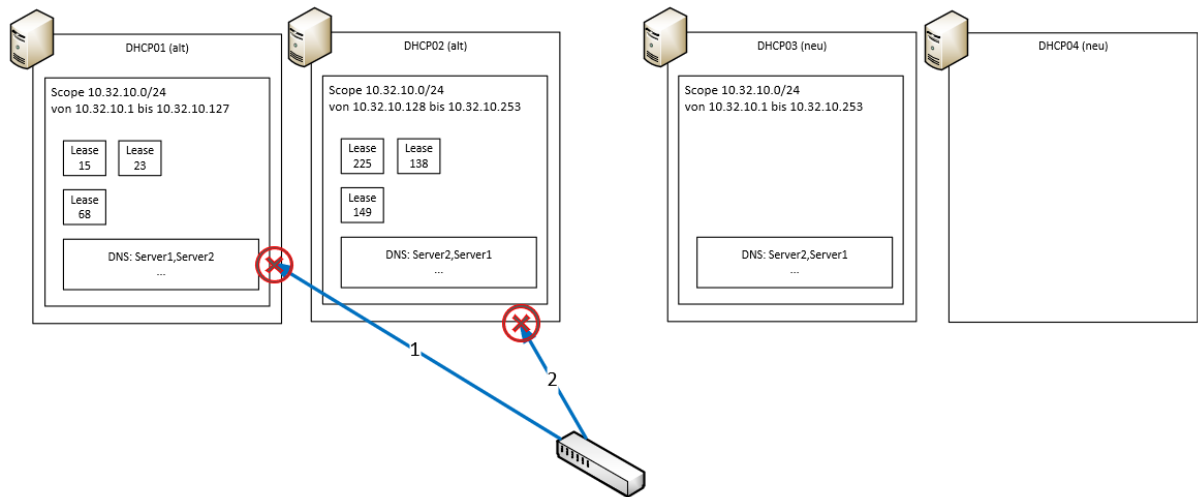
- DHCP1 (alt) vergibt aktuell von **10.32.10.1** bis **10.32.10.127**
- DHCP2 (alt) vergibt aktuell von **10.32.10.128** bis **10.32.10.253**
- der neue DHCP vergibt nach der Migration die IP-Adressen **10.32.10.1** bis **10.32.10.253**

Der andere neue DHCP-Server bleibt von Scope-frei.

Auch hier gibt es keine Service-Unterbrechung.

### Phase 3 – Deaktivierung der alten Scopes

Schema:



Jetzt wird die Vergabe der IP-Adressen auf den alten Servern ausgesetzt. Dies kann je Scope vorgenommen werden, indem man diese deaktiviert. Die bereits ausgeliehenen IPv4-Adressen bleiben dabei innerhalb ihrer Leasetime gültig. Clients ohne IPv4-Adresse werden aber nicht mehr bedient. Daher sollte diese Phase in einer aus DHCP-Sicht ruhigen Zeit stattfinden.

Das ist die Anweisung in der PowerShell. Sie führt die Phasen 3 bis 5 je Scope in einem Arbeitsschritt durch.

```
PS C:\> $ScopeID = '10.32.2.0'
$DHCPalt = 'x-dhcp1'
$DHCPneu = 'x-dhcp2'

Set-DhcpServerv4Scope -ComputerName $DHCPalt -ScopeId $ScopeID -State InActive

Get-DhcpServerv4Lease -ComputerName $DHCPalt -ScopeId $ScopeID |
  where-Object {$_.AddressState -eq 'Active' } |
  Add-DhcpServerv4Lease -ScopeId $ScopeID -ComputerName $DHCPneu

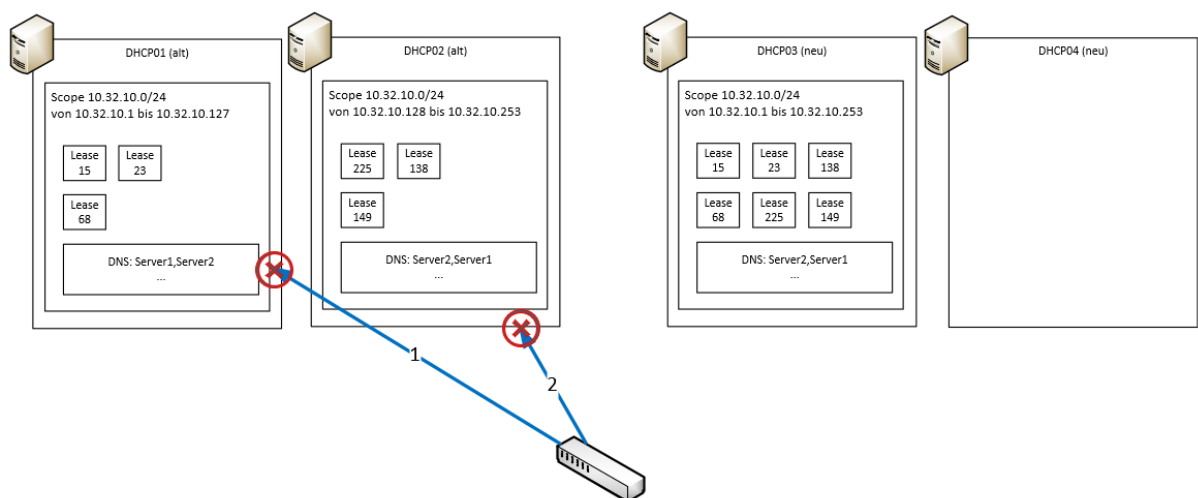
Set-DhcpServerv4Scope -ComputerName $DHCPneu -ScopeId $ScopeID -State Active

PS C:\>
```

Zeitlich ist diese Phase sehr kurz (weniger als eine Minute), wenn die Portierung zur nächsten Phase gescriptet vorgenommen wird.

#### Phase 4 – Portierung der Leases auf den neuen Server

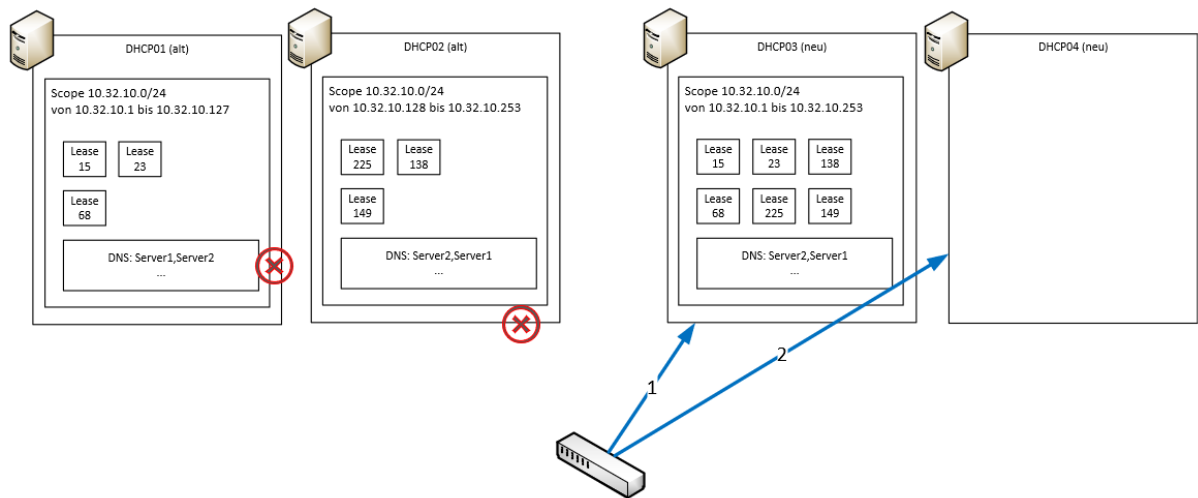
Schema:



Durch 2 PowerShell-Befehle werden nun die aktiven Leases und Reservierungen der beiden alten Server in den neuen Server integriert. Dieser kennt nun alle vergebenen Adressen. Der Vorgang dauert nur wenige Sekunden.

### Phase 5 – Aktivierung der neuen Scopes

Schema:

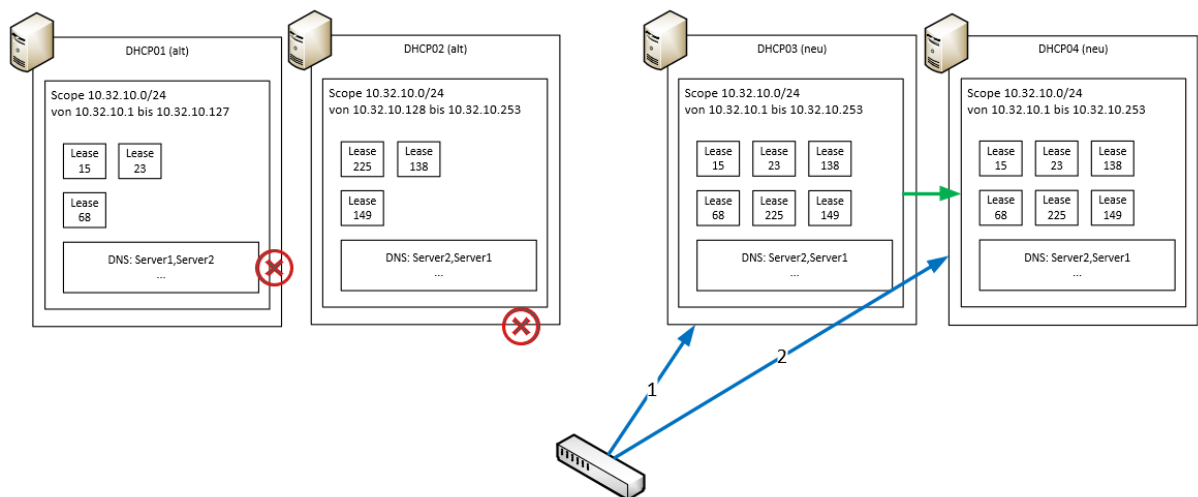


Jetzt werden die neuen Scopes auf dem neuen Server aktiviert. Zusätzlich können jetzt die DHCP-Relayagents (iphelper) auf den Routern auf die neuen DHCP-Server angepasst werden. Ab diesem Moment werden Clients wieder mit IPv4-Adressen versorgt. Der neue Server wird dabei nur nicht-verwendete Adressen vergeben, da er ja die aktiven Leases der beiden alten Server kennt.

Nach der Aktivierung des ersten neuen Servers steht der Service DHCP eingeschränkt zur Verfügung: Es fehlt die Verfügbarkeit – der Ausfall des neuen Servers unterbricht die Versorgung mit IPv4-Adressen.

### Phase 6 – Aktivierung des DHCP-Failovers

Schema:



Damit der Service DHCP wieder höher verfügbar wird, kann jetzt der fertige Scope durch die Einrichtung eines DHCP-Failovers auf den zweiten neuen DHCP-Server gespiegelt werden.

Die beiden alten Server werden nach dem Umzug aller alten Scopes nicht länger benötigt und können zurückgebaut werden.

## Ablauf der Migration aus der Sicht eines Clients

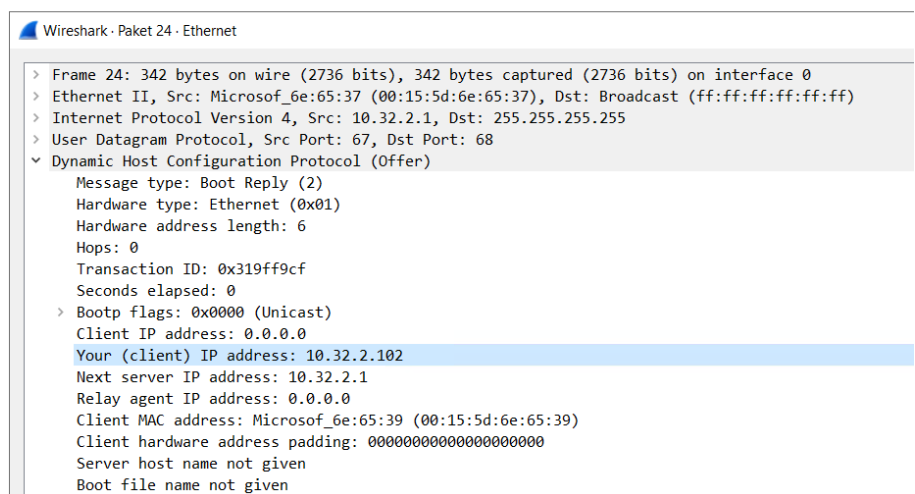
Serverseitig ist der Migrationsprozess recht einfach. Dennoch wird es auf der Seite der Clients eine kurze Unterbrechung der Netzwerk-Konnektivität geben. Um diesem Umstand zu verstehen, möchte ich das Verhalten der Clients in 3 Schritten aufzeigen.

### Address-Lease vom alten DHCP

Ein Client hat auf dem alten DHCP-Server eine IPv4-Adresse angefragt. Das Verfahren beruht auf den 4 DORA-Paketen (Discover, Offer, Request, Ack), die er via **Broadcast** mit dem DHCP-Server übermittelt.

Ihm wurde die 10.32.2.102 zugewiesen:

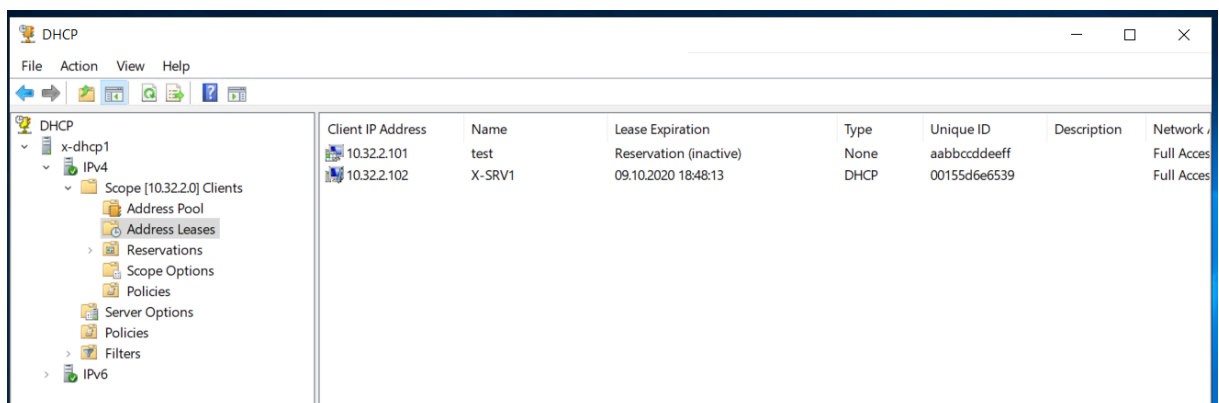
No.	Time	Source	Destination	Protocol	Length	Info
23	18:44:13,018638	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x319ff9cf
24	18:44:13,019703	10.32.2.1	255.255.255.255	DHCP	342	DHCP Offer - Transaction ID 0x319ff9cf
25	18:44:13,020122	0.0.0.0	255.255.255.255	DHCP	352	DHCP Request - Transaction ID 0x319ff9cf
26	18:44:13,021026	10.32.2.1	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0x319ff9cf



Wireshark · Paket 24 · Ethernet

- > Frame 24: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
- > Ethernet II, Src: Microsof\_6e:65:37 (00:15:5d:6e:65:37), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
- > Internet Protocol Version 4, Src: 10.32.2.1, Dst: 255.255.255.255
- > User Datagram Protocol, Src Port: 67, Dst Port: 68
- > Dynamic Host Configuration Protocol (Offer)
  - Message type: Boot Reply (2)
  - Hardware type: Ethernet (0x01)
  - Hardware address length: 6
  - Hops: 0
  - Transaction ID: 0x319ff9cf
  - Seconds elapsed: 0
  - Bootp flags: 0x0000 (Unicast)
  - Client IP address: 0.0.0.0
  - Your (client) IP address: 10.32.2.102**
  - Next server IP address: 10.32.2.1
  - Relay agent IP address: 0.0.0.0
  - Client MAC address: Microsof\_6e:65:39 (00:15:5d:6e:65:39)
  - Client hardware address padding: 00000000000000000000
  - Server host name not given
  - Boot file name not given

Die IPv4-Adresse wurde in der Datenbank des alten DHCP-Servers eingetragen:



DHCP console screenshot showing a reservation for IP 10.32.2.102.

Client IP Address	Name	Lease Expiration	Type	Unique ID	Description	Network
10.32.2.101	test	Reservation (inactive)	None	aabbccddeeff		Full Access
10.32.2.102	X-SRV1	09.10.2020 18:48:13	DHCP	00155d6e6539		Full Access

Damit ist der Vorgang abgeschlossen und der Client kann die Adresse innerhalb der Leasetime verwenden.

### Lease-Renew zum alten DHCP

Nach Ablauf der halben Lease-Time wird der Client ein **Unicast**-Packet zum DHCP-Server senden, von dem er die Adresse erhalten hat. Dieser bestätigt die Lease-Erneuerung ebenfalls mit einem **Unicast**:

No.	Time	Source	Destination	Protocol	Length	Info
23	18:44:13,018638	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x319ff9cf
24	18:44:13,019703	10.32.2.1	255.255.255.255	DHCP	342	DHCP Offer - Transaction ID 0x319ff9cf
25	18:44:13,020122	0.0.0.0	255.255.255.255	DHCP	352	DHCP Request - Transaction ID 0x319ff9cf
26	18:44:13,021026	10.32.2.1	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0x319ff9cf
185	18:46:13,279283	10.32.2.102	10.32.2.1	DHCP	342	DHCP Request - Transaction ID 0xb24526e9
186	18:46:13,280199	10.32.2.1	10.32.2.102	DHCP	342	DHCP ACK - Transaction ID 0xb24526e9

```

Wireshark - Paket 185 - Ethernet
> Frame 185: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
> Ethernet II, Src: Microsof_6e:65:39 (00:15:5d:6e:65:39), Dst: Microsof_6e:65:37 (00:15:5d:6e:65:37)
> Internet Protocol Version 4, Src: 10.32.2.102, Dst: 10.32.2.1
> User Datagram Protocol, Src Port: 68, Dst Port: 67
v Dynamic Host Configuration Protocol (Request)
  Message type: Boot Request (1)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 0
  Transaction ID: 0xb24526e9
  Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
  Client IP address: 10.32.2.102
  Your (client) IP address: 0.0.0.0
  Next server IP address: 0.0.0.0
  Relay agent IP address: 0.0.0.0
  Client MAC address: Microsof_6e:65:39 (00:15:5d:6e:65:39)
  Client hardware address padding: 00000000000000000000
  Server boot name not defined
  
```

Und hier liegt das Problem: Der Client kennt die IPv4-Adresse des DHCP-Servers, von dem er seine eigene Adresse erhalten hat. Daher spricht er ihn direkt an. Sollte der Server zu diesem Zeitpunkt (Ablauf halbe Leasetime) nicht erreichbar sein, dann wird er es nach Ablauf von 87,5% der Leasetime erneut mit einem Unicast versuchen. Schlägt auch dieser fehl, dann wird der Client nach Ablauf von 100% Leasetime die IPv4-Adresse aufgeben und via Broadcast eine neue im Netzwerk anfragen. Dabei werden bestehende Netzwerkverbindungen unterbrochen.

### Lease-Renew nach der Migration

Der Scope mit der IPv4-Adresse des Clients wurde jetzt vom alten DHCP-Server auf den neuen Server umgezogen.

Der Client versucht wieder nach Ablauf der halben Lease-Time, den ursprünglichen DHCP-Server via **Unicast** zu kontaktieren, um eine Verlängerung zu beantragen:

No.	Time	Source	Destination	Protocol	Length	Info
23	18:44:13,018638	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x319ff9cf
24	18:44:13,019703	10.32.2.1	255.255.255.255	DHCP	342	DHCP Offer - Transaction ID 0x319ff9cf
25	18:44:13,020122	0.0.0.0	255.255.255.255	DHCP	352	DHCP Request - Transaction ID 0x319ff9cf
26	18:44:13,021026	10.32.2.1	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0x319ff9cf
185	18:46:13,279283	10.32.2.102	10.32.2.1	DHCP	342	DHCP Request - Transaction ID 0xb24526e9
186	18:46:13,280199	10.32.2.1	10.32.2.102	DHCP	342	DHCP ACK - Transaction ID 0xb24526e9
273	18:48:13,111087	10.32.2.102	10.32.2.1	DHCP	342	DHCP Request - Transaction ID 0x4118479a
274	18:48:13,112141	10.32.2.1	255.255.255.255	DHCP	342	DHCP NAK - Transaction ID 0x4118479a
277	18:48:13,121174	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xe2f8c1bc
278	18:48:13,124979	10.32.2.2	255.255.255.255	DHCP	342	DHCP Offer - Transaction ID 0xe2f8c1bc
280	18:48:13,125538	0.0.0.0	255.255.255.255	DHCP	352	DHCP Request - Transaction ID 0xe2f8c1bc
281	18:48:13,127584	10.32.2.2	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0xe2f8c1bc

```

Wireshark - Paket 273 - Ethernet
> Frame 273: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
> Ethernet II, Src: Microsof_6e:65:39 (00:15:5d:6e:65:39), Dst: Microsof_6e:65:37 (00:15:5d:6e:65:37)
> Internet Protocol Version 4, Src: 10.32.2.102, Dst: 10.32.2.1
> User Datagram Protocol, Src Port: 68, Dst Port: 67
v Dynamic Host Configuration Protocol (Request)
  Message type: Boot Request (1)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 0
  Transaction ID: 0x4118479a
  Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
  Client IP address: 10.32.2.102
  Your (client) IP address: 0.0.0.0
  Next server IP address: 0.0.0.0
  Relay agent IP address: 0.0.0.0
  Client MAC address: Microsof_6e:65:39 (00:15:5d:6e:65:39)
  
```

Aber durch die Deaktivierung des Scopes auf dem alten Server lehnt dieser die Lease-Verlängerung ab:

No.	Time	Source	Destination	Protocol	Length	Info
23	18:44:13,018638	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x319ff9cf
24	18:44:13,019703	10.32.2.1	255.255.255.255	DHCP	342	DHCP Offer - Transaction ID 0x319ff9cf
25	18:44:13,020122	0.0.0.0	255.255.255.255	DHCP	352	DHCP Request - Transaction ID 0x319ff9cf
26	18:44:13,021026	10.32.2.1	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0x319ff9cf
185	18:46:13,279283	10.32.2.102	10.32.2.1	DHCP	342	DHCP Request - Transaction ID 0xb24526e9
186	18:46:13,280199	10.32.2.1	10.32.2.102	DHCP	342	DHCP ACK - Transaction ID 0xb24526e9
273	18:48:13,111087	10.32.2.102	10.32.2.1	DHCP	342	DHCP Request - Transaction ID 0x4118479a
274	18:48:13,112141	10.32.2.1	255.255.255.255	DHCP	342	DHCP NAK - Transaction ID 0x4118479a
277	18:48:13,121174	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xe2f8c1bc
278	18:48:13,124979	10.32.2.2	255.255.255.255	DHCP	342	DHCP Offer - Transaction ID 0xe2f8c1bc
280	18:48:13,125538	0.0.0.0	255.255.255.255	DHCP	352	DHCP Request - Transaction ID 0xe2f8c1bc
281	18:48:13,127584	10.32.2.2	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0xe2f8c1bc

### Wireshark - Paket 274 - Ethernet

```

> Frame 274: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
> Ethernet II, Src: Microsof_6e:65:37 (00:15:5d:6e:65:37), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 10.32.2.1, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 67, Dst Port: 68
v Dynamic Host Configuration Protocol (NAK)
  Message type: Boot Reply (2)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 0
  Transaction ID: 0x4118479a
  Seconds elapsed: 0
  > Bootp flags: 0x8000, Broadcast flag (Broadcast)
  Client IP address: 0.0.0.0
  Your (client) IP address: 0.0.0.0
  
```

Danach muss der Client die IPv4-Adresse direkt angeben und eine neue Adresse via Broadcast anfragen:

No.	Time	Source	Destination	Protocol	Length	Info
23	18:44:13,018638	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x319ff9cf
24	18:44:13,019703	10.32.2.1	255.255.255.255	DHCP	342	DHCP Offer - Transaction ID 0x319ff9cf
25	18:44:13,020122	0.0.0.0	255.255.255.255	DHCP	352	DHCP Request - Transaction ID 0x319ff9cf
26	18:44:13,021026	10.32.2.1	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0x319ff9cf
185	18:46:13,279283	10.32.2.102	10.32.2.1	DHCP	342	DHCP Request - Transaction ID 0xb24526e9
186	18:46:13,280199	10.32.2.1	10.32.2.102	DHCP	342	DHCP ACK - Transaction ID 0xb24526e9
273	18:48:13,111087	10.32.2.102	10.32.2.1	DHCP	342	DHCP Request - Transaction ID 0x4118479a
274	18:48:13,112141	10.32.2.1	255.255.255.255	DHCP	342	DHCP NAK - Transaction ID 0x4118479a
277	18:48:13,121174	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xe2f8c1bc
278	18:48:13,124979	10.32.2.2	255.255.255.255	DHCP	342	DHCP Offer - Transaction ID 0xe2f8c1bc
280	18:48:13,125538	0.0.0.0	255.255.255.255	DHCP	352	DHCP Request - Transaction ID 0xe2f8c1bc
281	18:48:13,127584	10.32.2.2	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0xe2f8c1bc

### Wireshark - Paket 277 - Ethernet

```

> Frame 277: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
> Ethernet II, Src: Microsof_6e:65:39 (00:15:5d:6e:65:39), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 68, Dst Port: 67
v Dynamic Host Configuration Protocol (Discover)
  Message type: Boot Request (1)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 0
  Transaction ID: 0xe2f8c1bc
  Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
  Client IP address: 0.0.0.0
  Your (client) IP address: 0.0.0.0
  Next server IP address: 0.0.0.0
  
```

Jetzt antwortet der neue DHCP-Server. Dieser kennt dank der importierten und immer noch gültigen Lease (diese ist ja erst zu 50% abgelaufen) die MAC-Adresse des Clients und bietet ihm daher seine „alte“ IPv4-Adresse wieder an:



No.	Time	Source	Destination	Protocol	Length	Info
23	18:44:13,018638	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x319ff9cf
24	18:44:13,019703	10.32.2.1	255.255.255.255	DHCP	342	DHCP Offer - Transaction ID 0x319ff9cf
25	18:44:13,020122	0.0.0.0	255.255.255.255	DHCP	352	DHCP Request - Transaction ID 0x319ff9cf
26	18:44:13,021026	10.32.2.1	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0x319ff9cf
185	18:46:13,279283	10.32.2.102	10.32.2.1	DHCP	342	DHCP Request - Transaction ID 0xb24526e9
186	18:46:13,280199	10.32.2.1	10.32.2.102	DHCP	342	DHCP ACK - Transaction ID 0xb24526e9
273	18:48:13,111087	10.32.2.102	10.32.2.1	DHCP	342	DHCP Request - Transaction ID 0x4118479a
274	18:48:13,112141	10.32.2.1	255.255.255.255	DHCP	342	DHCP NAK - Transaction ID 0x4118479a
277	18:48:13,121174	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xe2f8c1bc
278	18:48:13,124979	10.32.2.2	255.255.255.255	DHCP	342	DHCP Offer - Transaction ID 0xe2f8c1bc
280	18:48:13,125538	0.0.0.0	255.255.255.255	DHCP	352	DHCP Request - Transaction ID 0xe2f8c1bc
281	18:48:13,127584	10.32.2.2	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0xe2f8c1bc

Wireshark - Paket 278 - Ethernet

- > Frame 278: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
- > Ethernet II, Src: Microsof\_6e:65:38 (00:15:5d:6e:65:38), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
- > Internet Protocol Version 4, Src: 10.32.2.2, Dst: 255.255.255.255
- > User Datagram Protocol, Src Port: 67, Dst Port: 68
- > Dynamic Host Configuration Protocol (Offer)
  - Message type: Boot Reply (2)
  - Hardware type: Ethernet (0x01)
  - Hardware address length: 6
  - Hops: 0
  - Transaction ID: 0xe2f8c1bc
  - Seconds elapsed: 0
  - > Bootp flags: 0x0000 (Unicast)
    - Client IP address: 0.0.0.0
    - Your (client) IP address: 10.32.2.102

Der Client wird dieses Angebot akzeptieren. Seine IPv4-Adresse wird also durch die Migration nicht verändert. Er wird aber für einen kurzen Zeitraum keine Netzwerkverbindung haben. In dem Beispiel betrug die Unterbrechung 0,015443 Sekunden.