

# DHCP implementieren

Die Serverrolle *Dynamic Host Configuration Protocol* (DHCP) vereinfacht die Konfiguration Ihrer Netzwerkklients, da diesen hiermit automatisch eine Internet Protocol Version 4-Konfiguration (IPv4) oder eine Internet Protocol Version 6-Konfiguration (IPv6) zugewiesen werden kann. Die DHCP-Serverrolle ist ein unverzichtbarer Dienst; ohne ihn können die Netzwerkklients und Geräte keine IPv4- oder IPv6-Konfiguration erhalten. Darum ist es wichtig, dass Sie wissen, wie Sie die DHCP-Serverrolle verwalten und warten. Daher umfasst die Prüfung 70-741 »Netzwerkinfrastruktur in Windows Server 2016 implementieren« die Installation, Konfiguration, Verwaltung und Wartung der DHCP-Serverrolle.

## Prüfungsziele in diesem Kapitel

- DHCP installieren und konfigurieren
- DHCP verwalten und warten

## Prüfungsziel 2.1: DHCP installieren und konfigurieren

---

Es ist relativ einfach, für ein Gerät manuell eine IPv4- oder IPv6-Adresse festzulegen. Falls Sie jedoch zahlreiche Geräte konfigurieren müssen und Ihr Netzwerk mehrere Subnetze oder Standorte umfasst, kann es sehr zeitaufwendig und fehleranfällig sein, dies manuell zu tun.

## DHCP im Überblick

Mit DHCP können Sie Geräten einfach und schnell die erforderlichen IPv4- oder IPv6-Einstellungen zuweisen. DHCP bietet Administratoren die folgenden Vorteile:

- Weist IP-Adressen automatisch zu
- Stellt die korrekte IP-Konfiguration sicher
- Unterstützt die Neukonfiguration von Geräten
- Ermöglicht die effiziente Nutzung des verfügbaren IP-Adresspools
- Zentralisiert die IP-Konfiguration

Um DHCP in Ihrem Unternehmen zu nutzen, müssen Sie einen oder mehrere DHCP-Server bereitstellen. Jeder DHCP-Server ist für einen oder mehrere DHCP-Bereiche zuständig. Ein DHCP-Bereich enthält den verfügbaren IP-Adressbereich sowie weitere Optionen, die zur Konfiguration eines Clientcomputers benötigt werden.

Nachdem Sie den DHCP-Server installiert und konfiguriert haben, hört er die konfigurierte Netzwerkschnittstelle nach DHCP-Clientanforderungen ab. Diese Clientanforderungen stammen von Clientgeräten, die eine IP-Konfiguration erhalten wollen. Diese Anforderungen werden über eine Broadcast-Adresse gesendet, da den Clients noch keine IP-Adresse zugewiesen wurde, die für die direkte Kommunikation mit einem DHCP-Server erforderlich wäre. Der Server antwortet mit dem Angebot einer geeigneten IP-Konfiguration, das der Client normalerweise akzeptiert. Der Server schließt den Vorgang ab, indem er die Zuweisung der Adresse bestätigt.

Der Prozess der Adresszuweisung umfasst die folgenden vier Kommunikationsphasen:

1. Der DHCP-Client sendet ein DHCPDISCOVER-Paket in Form einer Broadcast-Anfrage.
2. Ein DHCP-Server antwortet mit einem DHCPOFFER-Paket, das die vorgeschlagene IP-Adresse enthält.
3. Der Client empfängt den Vorschlag und broadcastet ein DHCPREQUEST-Paket, das einen Serverbezeichner enthält. Dieses Paket gibt an, dass der Client die angebotene Konfiguration nutzen möchte. Falls mehrere DHCP-Server vorhanden sind, erhalten alle die DHCPREQUEST-Nachricht. Anhand des Serverbezeichners können die DHCP-Server erkennen, dass ein anderer Server die Clientanforderung bedient.
4. Der angesprochene Server verwendet eine DHCPACK-Nachricht, um den Client zu informieren, dass die Konfiguration live ist und dass die IP-Adresse nun an den Client geleast wurde.

Der Clientcomputer verwendet die zugewiesene IP-Konfiguration so lange, bis die Leasedauer abgelaufen ist. Um beim Ablauf der Lease nicht die Verbindung zu verlieren, versuchen die Clients eine Neuzuweisung, wenn 50 Prozent der Leasedauer abgelaufen ist. Auch beim Neustart des Computers versuchen die Clients, die Lease zu erneuern. Falls der DHCP-Server online ist und auf ihn zugegriffen werden kann, wird die Lease erneuert. Hierbei werden lediglich zwei Nachrichten versendet: eine DHCPREQUEST-Nachricht vom Client und eine DHCPACK-Nachricht vom Server.



#### **PRÜFUNGSTIPP**

**Die Erneuerungsnachrichten sind keine Broadcast-Anfragen, da der Clients bereits eine gültige IP-Konfiguration besitzt und er Unicast-Verkehr verwenden kann.**

---

Falls der Client bei der 50-Prozent-Schwelle der Leasedauer nicht mit dem DHCP-Server kommunizieren kann, versucht er es erneut, nachdem 87,5 Prozent der Leasedauer abgelaufen sind. Ab diesem Punkt sendet der Client wieder Broadcast-Abfragen. Falls der Client bei 100 Prozent Leasedauer keine Bestätigung der Erneuerung erhält, wechselt er in den DHCP-Discovery-Modus, der weiter oben beschrieben ist.

Falls der Client beim Neustart die Zuweisung nicht erneuern kann, sind die Dinge ein wenig anders. Eine der Gründe, warum der Client nicht mit dem DHCP-Server kommunizieren kann, liegt darin, dass sich der Client nicht mehr im gleichen Subnetz befindet. Falls der Client beim Neustart vom konfigurierten DHCP-Server keine Adresserneuerung erhält, sendet er eine

Nachricht an das Standardgateway. Falls der Client keine Antwort empfängt, geht er davon aus, dass er sich nicht mehr im ursprünglichen Subnetz befindet und er verwendet die DHCP-Discovery-Phase, um für das aktuelle Subnetz eine neue, gültige Konfiguration zu erhalten.

Falls ein Windows-basierter Client seine DHCP-Lease nicht erneuern kann, beendet er die Verwendung der geleasten Konfiguration und verwendet normalerweise eine APIPA-Adresse (Automatic Private IP Addressing). APIPA-Adressen ermöglichen einen einfachen Netzbetrieb, wobei lediglich die lokale Kommunikation innerhalb des eigenen Subnetzes möglich ist. Eine APIPA-Adresse befindet sich im Bereich 169.254.0.0/16. Dies bedeutet in der Regel, dass der Client nicht in der Lage ist, mit den meisten, wenn nicht sogar allen, vernetzten Ressourcen zu kommunizieren.

#### **WEITERE INFORMATIONEN** Wie DHCP funktioniert

Weitere Informationen über die Funktionsweise von DHCP finden auf der Microsoft TechNet-Website unter:

[https://technet.microsoft.com/library/dd183692\(v=ws.10\).aspx](https://technet.microsoft.com/library/dd183692(v=ws.10).aspx)

## DHCP installieren

Sie können die DHCP-Serverrolle mit dem Server-Manager oder mit Windows PowerShell installieren. Nach der Installation der DHCP-Serverrolle müssen Sie diese in den Active Directory-Domänendiensten autorisieren.



#### **PRÜFUNGSTIPP**

Sie können die DHCP-Serverrolle nicht auf einem Nano Server installieren.

---

## DHCP-Server installieren und konfigurieren

Bevor Sie die DHCP-Serverrolle installieren, müssen verschiedene Voraussetzungen erfüllt sein:

- Melden Sie sich mit einem lokalen Administratorenkonto an; in einer Domäne melden Sie sich als Mitglied der globalen Sicherheitsgruppe Domain Admins an.
- Prüfen Sie, ob Sie die Installation entweder auf einem Windows Server 2016 oder einem Windows Server 2016 Core durchführen.
- Konfigurieren Sie den Zielserver mit einer statischen IPv4- und/oder IPv6-Adresse.
- Achten Sie darauf, dass alle Datenträger mit NTFS formatiert sind. Das FAT-Dateisystem ist nicht sicher.



#### **PRÜFUNGSTIPP**

Vermeiden Sie es, die DHCP-Serverrolle auf Servern zu installieren, die spezielle Funktionen bereitstellen, wie das Hosten von Web-Apps, von Exchange Server oder von Microsoft SQL Server.

---

Führen Sie folgende Schritte durch, um die DHCP-Serverrolle zu installieren:

1. Klicken Sie im Server Manager auf *Verwalten* und dann auf *Rollen und Features hinzufügen*.
2. Klicken Sie auf der Seite *Vorbemerkungen des Assistenten zum Hinzufügen von Rollen und Features* auf *Weiter*.
3. Klicken Sie auf den Seiten *Installationstyp* und *Serverauswahl* auf *Weiter*.
4. Schalten Sie auf der Seite *Serverrollen auswählen* das Kontrollkästchen *DHCP-Server* ein.
5. Klicken Sie auf der Seite *Sollen für DHCP-Server erforderliche Features hinzugefügt werden* auf *Features hinzufügen* und klicken Sie dann auf *Weiter*.
6. Klicken Sie auf der Seite *Features* auf *Weiter*.
7. Klicken Sie auf der Seite *DHCP-Server* auf *Weiter*.
8. Klicken Sie auf der Seite *Installationsauswahl bestätigen* auf *Installieren*. Klicken Sie auf *Schließen*, nachdem die Rolle installiert ist.

Zur Installation der DHCP-Serverrolle können Sie auch das Windows PowerShell-Cmdlet `Add-WindowsFeature` verwenden. Um beispielsweise den DHCP-Server mit allen Verwaltungstools zu installieren, verwenden Sie den folgenden Befehl:

```
Add-WindowsFeature DHCP -IncludeManagementTools
```

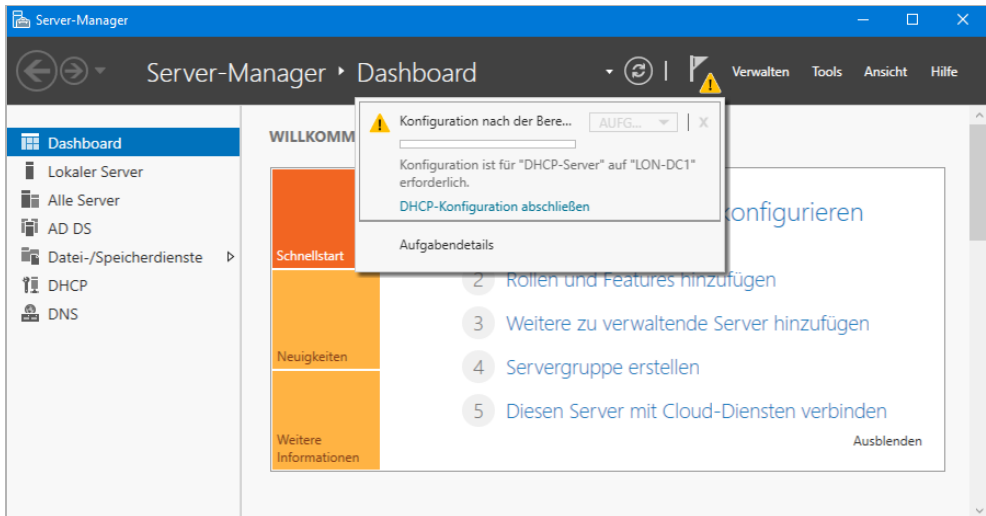
## Installation abschließen und DHCP-Server autorisieren

Nachdem Sie die Rolle installiert haben, müssen Sie die Konfiguration abschließen. Hierzu gehören das Erstellen der erforderlichen Sicherheitsgruppen und die Autorisierung des DHCP-Servers. Sie können für beide Schritte den *DHCP-Konfigurations-Assistent nach der Installation* verwenden. Der Assistent führt die folgenden Aufgaben durch:

- Er erstellt die erforderlichen Active Directory-Sicherheitsgruppen, die die Delegation der DHCP-Serververwaltung ermöglichen:
  - DHCP-Administratoren
  - DHCP-Benutzer
- Autorisiert die DHCP-Serverrolle, falls der Computer einer Domäne beigetreten ist

Sie können den *DHCP-Konfigurations-Assistenten nach der Installation* vom Server-Manager aus öffnen (siehe Abb. 2–1), indem Sie die folgenden Schritte verwenden.

1. Klicken Sie auf *Benachrichtigungen* und klicken Sie dann auf *DHCP-Konfiguration abschließen*.
2. Klicken Sie auf der Seite *Beschreibung des DHCP-Konfigurations-Assistenten nach der Installation* auf *Weiter*.
3. Geben Sie auf der Seite *Autorisierung* die Anmeldedaten ein, die für die Autorisierung des Servers in den Active Directory-Domänendiensten erforderlich ist. Das Konto, das Sie hier verwenden, sollte ein Mitglied der globalen Sicherheitsgruppe Domänen-Admins sein. Klicken Sie auf *Commit ausführen*, um die Autorisierung abzuschließen und die erforderlichen Sicherheitsgruppen zu erstellen.



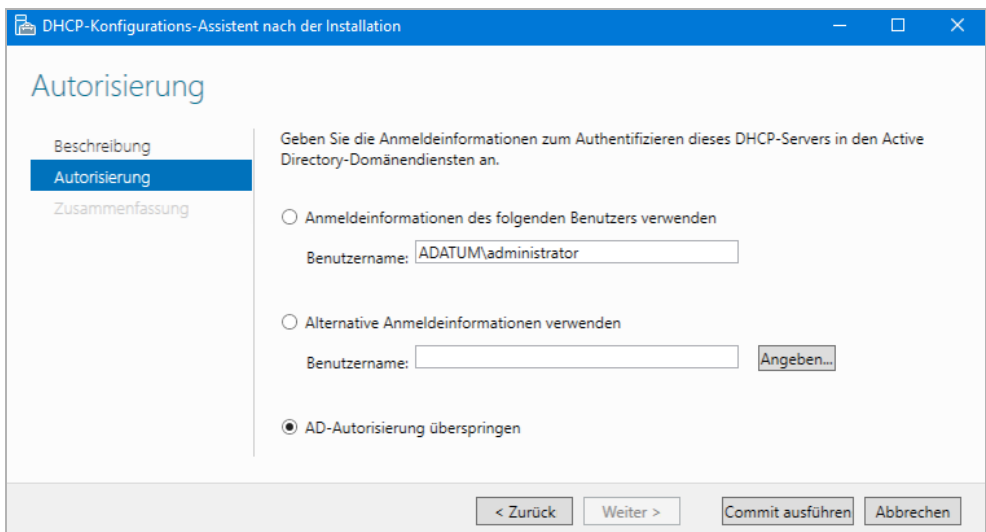
**Abb. 2-1** Die Installation der DHCP-Serverrolle abschließen



**PRÜFUNGSTIPP**

Sie müssen den DHCP-Server nur dann autorisieren, wenn er Mitglied einer Domäne ist.

Falls Sie die Autorisierung des Servers in einem separaten Schritt durchführen wollen, schalten Sie das Optionsfeld *AD-Autorisierung überspringen* ein (siehe Abb. 2-2) und klicken Sie dann auf *Commit ausführen*. Hierdurch werden lediglich die erforderlichen Sicherheitsgruppen erstellt und Sie müssen den DHCP-Server immer noch autorisieren.



**Abb. 2-2** AD-Autorisierung überspringen

Falls Sie sich entscheiden, den DHCP-Server nicht mit dem *DHCP-Konfigurations-Assistenten nach der Installation* zu autorisieren, müssen Sie dies tun, bevor Sie ihn aktivieren. Zur Autorisierung des DHCP-Servers nach der Installation können Sie die Konsole *DHCP* verwenden. Führen Sie dazu folgende Schritte durch:

1. Klicken Sie im Server-Manager auf *Tools* und dann auf *DHCP*.
2. Klicken Sie in der Konsole *DHCP* den Zielserver mit der rechten Maustaste an und wählen Sie *Autorisieren*.

Um diesen Vorgang abzuschließen, können Sie auch das Windows PowerShell-Cmdlet `Add-DhcpServerInDC` verwenden. Verwenden Sie beispielsweise den folgenden Befehl, um den Server `lon-svr2` in der Domäne `contoso.com` zu autorisieren.

```
Add-DhcpServerInDC -DnsName lon-svr2.contoso.com
```

### **WEITERE INFORMATIONEN** DHCP-Server-Cmdlets der Windows PowerShell

Weitere Informationen über die Verwendung von Windows PowerShell zur Konfiguration von DHCP finden Sie auf der Microsoft TechNet-Website unter:

[https://technet.microsoft.com/library/jj590751\(v=wps.630\).aspx](https://technet.microsoft.com/library/jj590751(v=wps.630).aspx)

## DHCP-Adressbereiche erstellen und verwalten

Nachdem Sie Ihren DHCP-Server installiert und autorisiert haben, können Sie mit dem Erstellen von DHCP-Bereichen beginnen. Bereiche enthalten den IPv4- oder IPv6-Adressbereich, der zugewiesen werden kann, sowie weitere Optionen, mit denen Sie Ihre Netzwerk-Clients konfigurieren können.

### Bereiche erstellen und konfigurieren

Ein DHCP-Bereich ist eine fundamentale Komponente der DHCP-Architektur. Ein Bereich enthält einen Pool von IPv4- oder IPv6-Adressen sowie weitere Konfigurationsoptionen, wie die Standardgateways, Domain Name System-Suffixes und DNS-Server.

Sie können Ihre DHCP-Bereiche mit der Konsole *DHCP* oder mit Windows PowerShell erstellen. Um einen DHCP-IPv4-Bereich mit der Konsole *DHCP* zu erstellen, führen Sie folgende Schritte durch:

1. Erweitern Sie in der Konsole *DHCP* den DHCP-Server, klicken Sie den Knoten *IPv4* mit der rechten Maustaste an und wählen Sie *Neuer Bereich*.
2. Klicken Sie auf der Seite *Willkommen* des Bereichserstellungs-Assistenten auf *Weiter*.
3. Geben Sie auf der Seite *Bereichsname* einen Namen und eine Beschreibung für Ihren Bereich ein. Diese Angaben sollten aussagekräftig sein. Klicken Sie auf *Weiter*.
4. Geben Sie auf der Seite *IP-Adressbereich* in das Feld *Start-IP-Adresse* die erste gültige IP-Adresse des Bereichs ein. Geben Sie in das Feld *End-IP-Adresse* die letzte gültige IP-Adresse des Bereichs ein. Wählen Sie im Drehfeld *Länge* die Anzahl der Bits in der Subnetzmaske aus. Wählen Sie beispielsweise 24 aus. Das Feld *Subnetzmaske* wird dann automatisch ausgefüllt (siehe Abb. 2–3). Klicken Sie auf *Weiter*.

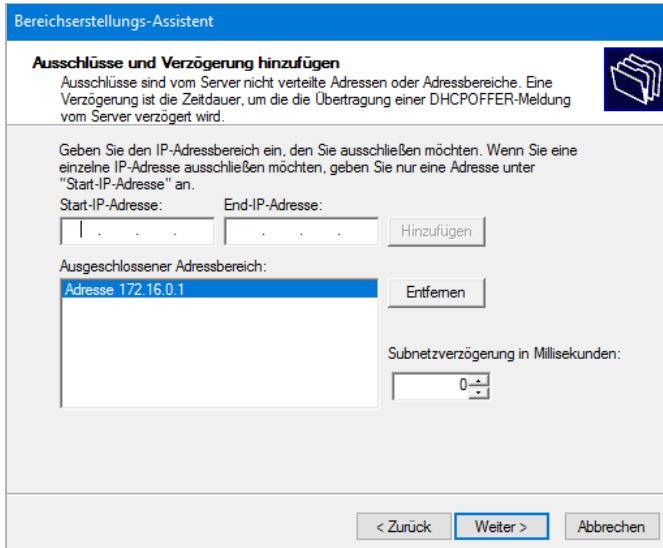
**Abb. 2–3** Legen Sie den IP-Adressbereich und die Subnetzmaske des Bereichs fest.

5. Geben Sie auf der Seite *Ausschlüsse und Verzögerung hinzufügen* in die Felder *Start-IP-Adresse* und *End-IP-Adresse* den Bereich der IP-Adressen ein, den Sie aus dem Pool ausschließen möchten, und klicken Sie auf *Hinzufügen*. Wenn Sie möchten, können Sie auch, wie in Abbildung 2–4 zu sehen, eine einzelne IP-Adresse ausschließen.



### **PRÜFUNGSTIPP**

Sie können den IP-Adressbereich und DHCP-Ausschlüsse ändern, nachdem Sie den Bereich erstellt haben.



**Abb. 2-4** Dem Bereich Ausschlüsse hinzufügen

6. Geben Sie in das Feld *Subnetzverzögerung* einen Wert ein, der festlegt, um wie viel Millisekunden der Versand des DHCP-OFFER-Pakets an die Clientcomputer verzögert werden soll. Normalerweise wird dieser Wert nicht verwendet.
7. Legen Sie auf der Seite *Leasedauer* die Leasedauer fest. Dies ist der Zeitraum, für den DHCP-Clients die zugewiesene IP-Adresse verwenden, bevor sie die Adresse erneuern oder freigeben müssen. Der Standardwert ist acht Tage. Verwenden Sie für Bereiche mit einem kleinen IP-Adresspool oder wenn sich die Clients häufig zwischen Subnetzen und Bereichen bewegen, eine kürzere Leasedauer.
8. Schalten Sie auf der Seite *DHCP-Optionen konfigurieren* das Optionsfeld *Ja, diese Optionen jetzt konfigurieren* ein und klicken Sie dann auf *Weiter*. Sie können die Konfiguration der Optionen später in der DHCP-Konsole ändern.
9. Geben Sie auf der Seite *Router (Standardgateway)* in das Feld *IP-Adresse* die IP-Adresse des Standardgateways ein, das die Clients in diesem Bereich bedient, und klicken Sie auf *Hinzufügen*. Sie können mehrere Gateways konfigurieren und die Reihenfolge der Liste ändern.
10. Geben Sie auf der Seite *Domänenname und DNS-Server* in das Feld *Servername* den vollqualifizierten Domännennamen (FQDN) oder die IP-Adresse des primären DNS-Servers für Clients in diesem Bereich ein und klicken Sie auf *Hinzufügen* (siehe Abb. 2-5). Klicken Sie dann auf *Weiter*.



**Abb. 2-5** Konfiguration der DNS-Bereichsoptionen



### **PRÜFUNGSTIPP**

Der Wert *Übergeordnete Domäne* wird automatisch anhand der Domänenmitgliedschaft des DHCP-Computers oder anhand des primären DNS-Suffixes eingetragen. Sie können diesen Wert ändern, falls er nicht mit dem Domännennamen der Clients übereinstimmt, die diesen Bereich verwenden.

11. Falls Sie NetBIOS-Apps verwenden und für die Namensauflösung von einfachen Bezeichnungen keine GlobalNames-Zone eingerichtet haben (siehe hierzu Kap. 1), geben Sie auf der Seite *WINS-Server* die IP-Adresse von einem oder mehreren WINS-Servern ein, und klicken Sie dann auf *Weiter*.
12. Falls Sie den Clients erlauben wollen, eine IP-Konfiguration aus dem Bereich abzurufen, schalten Sie abschließend auf der Seite *Bereich aktivieren* das Optionsfeld *Ja, diesen Bereich jetzt aktivieren* ein und klicken Sie auf *Weiter*. Sie können den Bereich auch später in der DHCP-Konsole aktivieren. Klicken Sie auf *Fertig stellen*.

Um mit Windows PowerShell einen DHCP-IPv4-Bereich zu erstellen, verwenden Sie das Cmdlet `Add-DhcpServerv4Scope`. So fügt beispielsweise der folgende Befehl dem auf dem lokalen Computer ausgeführten DHCP-Serverdienst einen neuen Bereich mit dem Namen **London** für das Subnetz 172.16.0.0/24 hinzu:

```
Add-DhcpServerv4Scope -Name "London" -StartRange 172.16.0.1 -EndRange 172.16.0.254
-SubnetMask 255.255.255.0
```

Nachdem Sie Ihre DHCP-Bereiche erstellt haben, können Sie sie mit der DHCP-Konsole oder mit Windows PowerShell konfigurieren. Nun wollen wir uns den konfigurierbaren Optionen zuwenden.

## Bereichsgruppierungen und Multicastbereiche erstellen und konfigurieren

Der DHCP-Server stellt zwei Optionen für komplexere Bereichsszenarien zur Verfügung. Dies sind Bereichsgruppierungen (Superscopes) und Multicastbereiche.

- **Bereichsgruppierungen** Sie können DHCP-Bereichsgruppierungen verwenden, um Mehrfachnetze zu unterstützen. Ein Mehrfachnetz ist eine Netzwerkumgebung, in der sich auf einem physischen Netzwerk, wie einem Ethernet-Segment, mehrere logische Netzwerke oder Subnetze befinden. Bereichsgruppierungen sind in Mehrfachnetzen und hier in den folgenden Situationen hilfreich:
  - **Adresspool aufgebraucht** Im Adresspool steht eine unzureichende Anzahl von IP-Adressen zur Verfügung. Da Sie den Adressraum nicht erweitern können, müssen Sie einen weiteren Bereich mit einem eigenen Adresspool hinzufügen.
  - **Clientmigration** Sie migrieren die Clientgeräte in einen neuen DHCP-Bereich, vielleicht weil Sie ein neues Adressierungsschema implementieren.
  - **Mehrere DHCP-Server** Sie möchten zwei oder mehr DHCP-Server verwenden, die die Clients im selben physischen Netzwerksegment bedienen, um so separate logische IP-Netzwerke verwalten zu können.
- **Multicastbereiche** Ein Multicastbereich, der auch MADCAP-Bereich (Multicast Address Dynamic Client Allocation-Protokoll) genannt wird, unterstützt Apps, die zur Kommunikation Multicastdatenverkehr verwenden. Die Adressen eines Multicastbereichs verwenden Klasse-D-IP-Adressen und befinden sich im Bereich zwischen 224.0.0.0 bis 239.255.255.255 (224.0.0.0/3). Sie verwenden Multicastbereiche, damit Apps für ihre Kommunikation eine Multicast-Adresse reservieren können.



### **PRÜFUNGSTIPP**

Der Multicastdatenverkehr erlaubt es einem Server, ohne die Verwendung von Broadcasts effizient mit mehreren Clients zu kommunizieren. Multicastdatenverkehr wird häufig von Bereitstellungssoftware, wie den Windows-Bereitstellungsdiensten, verwendet.

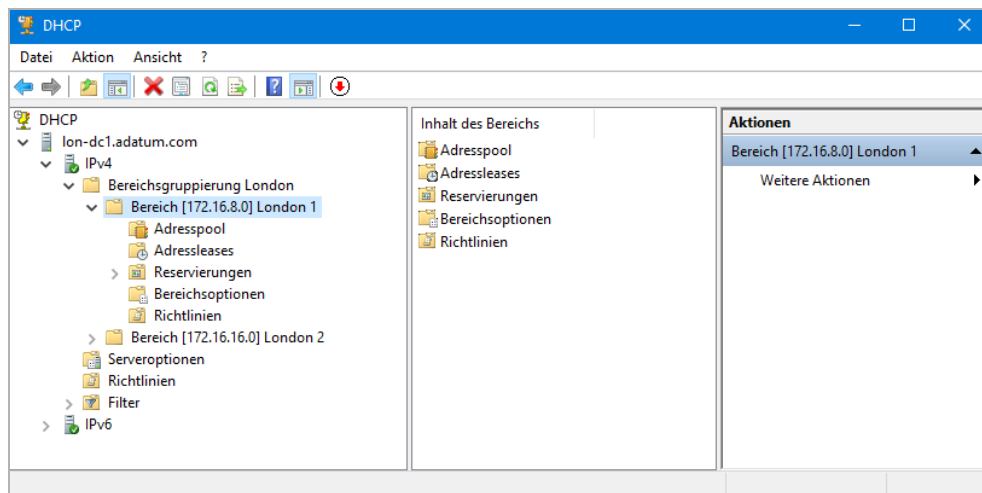
---

### **BEREICHSGRUPPIERUNG ERSTELLEN**

Um eine Bereichsgruppierung zu erstellen, muss auf Ihrem DHCP-Server mindestens ein Bereich eingerichtet sein. Dann klicken Sie in der DHCP-Konsole den Knoten *IPv4* mit der rechten Maustaste an und wählen im Kontextmenü den Befehl *Neue Bereichsgruppierung*. Hierdurch wird der *Assistent zum Erstellen von Bereichsgruppierungen* gestartet. Sie müssen die folgenden Eigenschaften festlegen:

- **Name** Ein aussagekräftiger Name für die Bereichsgruppierung.
- **Bereiche auswählen** Sie müssen festlegen, welche Bereiche in der Bereichsgruppierung enthalten sein sollen.

Nachdem Sie die Bereichsgruppierung erstellt haben, werden die ausgewählten Bereiche in der DHCP-Konsole unterhalb eines neuen Knotens mit dem Namen *Bereichsgruppierung* angezeigt (siehe Abb. 2–6).



**Abb. 2–6** Der Knoten *Bereichsgruppierung*



### **PRÜFUNGSTIPP**

Um einen Bereich in eine Bereichsgruppierung einzufügen, klicken Sie ihn in der DHCP-Konsole mit der rechten Maustaste an und klicken im Kontextmenü auf *Zur Bereichsgruppierung hinzufügen*.

Sie können das Windows PowerShell-Cmdlet `Add-DhcpServerv4Superscope` verwenden. Nutzen Sie beispielsweise den folgenden Befehl, um die Bereichsgruppierung London zu erstellen und um die zwei Bereiche im Adressbereich 172.16.0.0/248 zu kombinieren:

```
Add-DhcpServerv4Superscope -SuperscopeName "London" -ScopeId 172.16.8.0,
172.16.16.0
```

### **WEITERE INFORMATIONEN Eine DHCP-Bereichsgruppierung konfigurieren**

Weitere Details zu DHCP-Bereichsgruppierungen finden Sie auf der Microsoft TechNet-Website unter:

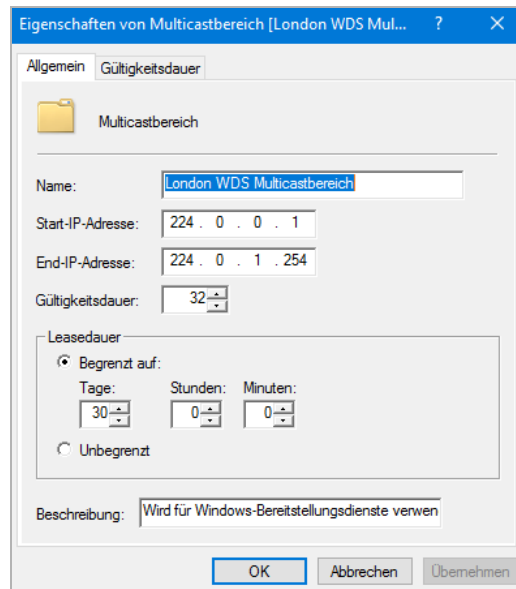
[https://technet.microsoft.com/library/dd759168\(v=ws.11\).aspx](https://technet.microsoft.com/library/dd759168(v=ws.11).aspx)

## MULTICASTBEREICH ERSTELLEN

Um einen Multicastbereich zu erstellen, müssen Sie zuerst prüfen, ob Ihre Anwendung via DHCP eine Multicast-Adresse anfordern kann. Anschließend öffnen Sie die DHCP-Konsole, klicken den Knoten *IPv4* mit der rechten Maustaste an und wählen im Kontextmenü den Befehl *Neuer Multicastbereich*. Der Assistent zum Erstellen von Multicastbereichen wird gestartet. Sie müssen die folgenden Eigenschaften definieren:

- **Name** Ein aussagekräftiger Name für den Multicastbereich.
- **Beschreibung** Eine optionale Beschreibung des Multicastbereichs.
- **IP-Adressbereich** Der Bereich von Klasse-D-IP-Adressen, die Sie dem Bereich zuweisen wollen. Geben Sie eine *Start-* und eine *End-IP-Adresse* an, die im Bereich zwischen 224.0.0.0 und 239.255.255.255 liegen muss. Der Bereich, den Sie hier angeben, muss mindestens 256 IP-Adressen enthalten.
- **Ausschlüsse** Wie bei einem Standardbereich können Sie eine oder mehrere IP-Adressen ausschließen.
- **Leasedauer** Der Standardwert ist 30 Tage.

Nachdem Sie Ihren Multicastbereich erstellt haben, können Sie, wie in Abbildung 2–7 zu sehen, dessen Eigenschaften konfigurieren.



**Abb. 2–7** Die Eigenschaften eines Multicastbereichs konfigurieren

Sie können auch das Windows PowerShell-Cmdlet `Add-DhcpServerv4MulticastScope` verwenden, um Multicastbereiche zu erstellen. Der folgende Befehl erzeugt beispielsweise den gleichen Multicastbereich, den Abbildung 2–7 zeigt:

```
Add-DhcpServerv4MulticastScope -ComputerName "lon-svr2.Contoso.com" -Name "Wird für Windows-Bereitstellungsdienste verwendet" -StartRange 224.0.0.1 -EndRange 224.0.1.254
```

## **WEITERE INFORMATIONEN** Einen DHCP-Multicastbereich konfigurieren

Weitere Informationen zu DHCP-Multicastbereichen finden Sie auf der Microsoft TechNet-Website unter:

[https://technet.microsoft.com/library/dd759152\(v=ws.11\).aspx](https://technet.microsoft.com/library/dd759152(v=ws.11).aspx)

## Eine DHCP-Reservierung konfigurieren

Angenommen, Sie wollen dem Server lon-svr3.contoso.com eine bestimmte IPv4-Adresse zuweisen. Sie können hierfür auf dem Server lon-svr3 manuell eine IPv4-Konfiguration erstellen; Sie müssen dann daran denken, die manuell festgelegte IP-Adresse in allen DHCP-Bereichen auszuschließen, die diese Adresse enthalten. Außerdem müssen Sie immer dann, wenn Sie die IP-Konfiguration von lon-svr3 ändern wollen, dies auf dem Computer selbst durchführen und anschließend in allen Bereichen die Ausschlüsse aktualisieren.

Die DHCP-Reservierung ist ein Verfahren, bei dem Sie eine bestimmte IPv4- oder IPv6-Adresse aus einem Adresspool einem bestimmten Clientgerät zuordnen können. Dies bietet die folgenden Vorteile:

- Sie müssen die reservierte Adresse nicht ausschließen, da sich die zugeordnete Adresse im Adresspool des Bereichs befindet.
- Sie brauchen den Computer bei einer Neukonfiguration nicht erneut zu besuchen, da Sie die reservierte Adresse von der DHCP-Konsole aus neu konfigurieren können.

Um innerhalb eines Bereichs eine Reservierung zu erstellen, müssen Sie die folgenden Informationen angeben:

- **Reservierungsname** Ein Name, der die Reservierung identifiziert. Meist wird hier der Computername verwendet.
- **IP-Adresse** Die IP-Adresse, die Sie dem Client aus dem IP-Adressbereich zuweisen wollen.
- **MAC-Adresse** Die MAC-Adresse (Media Access Control, MAC) der Netzwerkschnittstelle im Clientcomputer, an die Sie die IP-Adresse binden wollen. Diese Adresse ist eindeutig und identifiziert den Clientcomputer.
- **Beschreibung** Ein optionales Feld, das den Client beschreibt.

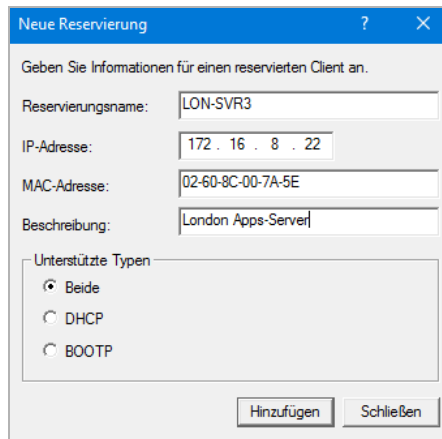


### **PRÜFUNGSTIPP**

Sie können die MAC-Adresse eines Geräts auf unterschiedliche Arten ermitteln. Wenn Sie beispielsweise den Befehl `ipconfig /a11` verwenden, wird die MAC-Adresse im Feld *Physikalische Adresse* angezeigt. Sie können auch den Befehl `arp -a` verwenden, um eine Liste der IP-Adressen und deren MAC-Adressen anzeigen zu lassen.

---

Um in der DHCP-Konsole eine Reservierung zu erstellen, wählen Sie den gewünschten Bereich aus, klicken Sie den Knoten *Reservierungen* mit der rechten Maustaste an und wählen Sie im Kontextmenü den Befehl *Neue Reservierung*. Füllen Sie dann das Dialogfeld *Neue Reservierung* aus, das Sie in Abbildung 2–8 sehen.



**Abb. 2–8** Eine Reservierung hinzufügen

Sie können auch das Windows PowerShell-Cmdlet `Add-DhcpServerv4Reservation` verwenden. So erzeugt beispielsweise der folgende Befehl eine Reservierung für den Client LON-SVR3 mit der Mac-Adresse 02-60-8C-00-7A-5E:

```
Add-DhcpServerv4Reservation -ScopeId 172.16.8.0 -IPAddress 172.16.8.22 -ClientId 02-60-8C-00-7A-5E -Description "LON-SVR3"
```



### **PRÜFUNGSTIPP**

Alle Reservierungen werden im Knoten *Adressleases* unterhalb des Bereichsknotens angezeigt. Je nachdem, ob das konfigurierte Gerät die Reservierung verwendet oder nicht, wird in der Spalte *Leaseablaufdatum* der Text *Reservierung (aktiv)* oder *Reservierung (inaktiv)* angezeigt.

## DHCP-Optionen konfigurieren

Beim Erstellen und Konfigurieren eines DHCP-Bereichs werden Sie gefragt, ob Sie Bereichsoptionen konfigurieren wollen. Mit diesen Optionen ist es möglich, Clientcomputern eine vollständige IP-Konfiguration zuzuweisen. Ohne diese Optionen erhält der DHCP-Client lediglich eine IP-Adresse und eine Subnetzmaske. Hierdurch ist weder die Namensauflösung noch Kommunikation außerhalb des lokalen Subnetzes möglich.

Mit den DHCP-Optionen können Sie neben der IP-Adresse und der Subnetzmaske weitere IP-Konfigurationseigenschaften zuweisen. Es stehen Ihnen zahlreiche Optionen zur Verfügung. In den meisten Fällen werden Sie mindestens ein Standardgateway (Router) sowie Optionen konfigurieren, mit denen die Namensauflösung möglich ist.

Optionscode	Name
003	Router
004	Zeitserver
005	Namensserver
006	DNS-Server
015	DNS-Domänenname
031	Routersuche ausführen
044	WINS/NBNN-Server
046	WINS/NBT-Knotentyp
047	NetBIOS-Bereichskennung
060	Pre-Boot Execution-Client (PXE)
066	Hostname des Startservers
067	Name der Startdatei

**Tab. 2-1** DHCP-Optionen

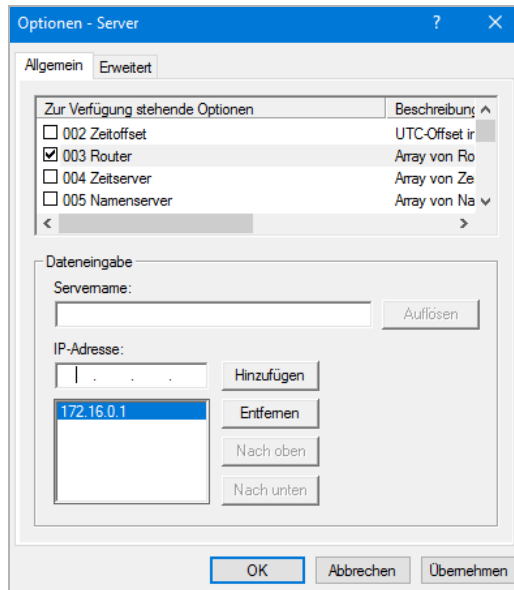
Sie können DHCP-Optionen auf vier unterschiedlichen Ebenen konfigurieren und zuweisen:

- **Server** Optionen gelten für alle DHCP-Clients dieses Servers.
- **Bereich** Optionen gelten für alle DHCP-Clients dieses Bereichs. Die Bereichsoptionen überschreiben die Serveroptionen.
- **Klassen** Optionen gelten für alle Clientgeräte, die sich als Mitglied einer konfigurierten Klasse zu erkennen geben.
- **Clientreservierung** Weist einer bestimmten DHCP-Reservierung Optionen zu. Optionen auf der Ebene einer Reservierung gelten nur für die Geräte, die eine DHCP-Reservierung besitzen, und überschreiben alle anderen konfigurierten Optionen.

Falls die gleiche Option auf unterschiedlichen Ebenen konfiguriert wurde, überschreiben die am meisten spezifischen Einstellungen alle anderen. Falls Sie beispielsweise das Standardgateway auf der Bereichsebene definiert und einem reservierten Client einen anderen Wert für das Standardgateway zugewiesen haben, wird die in der Reservierung festgelegte Einstellung verwendet.

### DHCP-SERVEROPTIONEN KONFIGURIEREN

Sie können die DHCP-Serveroptionen in der DHCP-Konsole konfigurieren. Klicken Sie unterhalb des Knotens *IPv4* oder *IPv6* mit der rechten Maustaste auf den Knoten *Serveroptionen* und klicken Sie im Kontextmenü auf *Optionen konfigurieren*. Im Dialogfeld *Optionen – Server*, das Sie in Abbildung 2-9 sehen, können Sie die betreffende Option konfigurieren, indem Sie ihr Kontrollkästchen einschalten und dann den/die erforderlichen Wert/e angeben.



**Abb. 2-9** Konfiguration von DHCP-Serveroptionen

Sie können die DHCP-Serveroptionen auch mit dem Windows PowerShell-Cmdlet `Set-DhcpServerv4optionValue` konfigurieren. Beispielsweise konfiguriert der folgende Befehl auf dem Server LON-SVR2 diese Serveroptionen: Standardgateway/Router (003), DNS-Server (006) und DNS-Domänenname (015):

```
Set-DhcpServerv4optionValue -ComputerName LON-SVR2.contoso.com -DnsServer
172.16.0.10 -DnsDomain contoso.com -Router 172.16.0.1
```

## DHCP-BEREICHSOPTIONEN KONFIGURIEREN

Um DHCP-Optionen auf der Bereichsebene zu konfigurieren, suchen Sie in der DHCP-Konsole nach dem gewünschten Bereich, klicken Sie den Knoten *Bereichsoptionen* mit der rechten Maustaste an und klicken Sie dann auf *Optionen konfigurieren*.

DHCP-Bereichsoptionen lassen sich auch mit dem Windows PowerShell-Cmdlet `Set-DhcpServerv4optionValue` konfigurieren, indem Sie den Parameter `-ScopeID` verwenden. Mit dem folgenden Befehl konfigurieren Sie für den Bereich mit der ID 172.16.8.0 die Bereichsoptionen Standardgateway/Router (003), DNS-Server (006) und DNS-Domänenname (015):

```
Set-DhcpServerv4optionValue -ComputerName LON-SVR2.contoso.com -ScopeId 172.16.8.0
-DnsServer 172.16.0.10 -DnsDomain contoso.com -Router 172.16.0.1
```

## KLASSENOPTIONEN KONFIGURIEREN

Neben den Optionen auf Server- und Bereichsebene können Sie Ihren DHCP-Clients außerdem Optionen auf Klassenebene zuweisen. Klassenoptionen werden zugewiesen, wenn ein Computer oder Gerät eine bestimmte Klassen-ID besitzt. Diese Klassen können von einem Hersteller, wie Microsoft, zugewiesen werden oder durch die DHCP-Administratoren; in diesem Fall spricht man von Benutzerklassenoptionen.



Bevor Sie Benutzerklassenoptionen implementieren können, müssen Sie zuerst die entsprechende Benutzerklasse erstellen. Hierzu führen Sie die folgenden Schritte durch:

1. Klicken Sie in der Konsole *DHCP* den Knoten *IPv4* mit der rechten Maustaste an und klicken Sie dann auf *Benutzerklassen definieren*. Erstellen Sie die gewünschte Benutzerklasse und weisen Sie ihr eine eindeutige ID zu. Sie können beispielsweise eine Benutzerklasse für Laptops erstellen und diese Klasse **LAPTOP** nennen.
2. Weisen Sie dem Gerät auf den Clientgeräten die gewünschte Benutzerklasse zu. Verwenden Sie hier das Befehlszeilenwerkzeug *IPConfig.exe*. Tippen Sie beispielsweise `IPConfig /setclassid "Ethernet" LAPTOP` ein, wobei Ethernet der Name der Netzwerkverbindung des Geräts ist.
3. Verwenden Sie DHCP-Richtlinien, um den von Ihnen definierten Benutzerklassen DHCP-Optionen zuzuweisen.



### **PRÜFUNGSTIPP**

**Benutzerklassen können nur für den gesamten IPv4-Knoten definiert werden und nicht für einzelne Server oder Bereiche. Für IPv6 stehen Benutzerklassen nicht zur Verfügung.**

---

Sie verwenden Herstellerklassen, um Clientoptionen auf Basis eines Herstellertyps zu definieren. Die Clients müssen sich zuerst als zu einer bestimmten Herstellerklasse zugehörig zu erkennen geben. Hierzu geben Sie bei der Anforderung einer Lease in der DHCPREQUEST-Nachricht in das Feld mit der Herstellerklassen-ID einen Wert an. Herstellerklassen werden durch einen Gerätehersteller festgelegt. Wie bei den Benutzerklassen verwenden Sie hier ebenfalls DHCP-Richtlinien, um sie zuzuweisen. Im Abschnitt »Prüfungsziel 2.2: DHCP verwalten und warten« (S. 87) erfahren Sie mehr über DHCP-Richtlinien.

### **DNS-OPTIONEN IN DHCP KONFIGURIEREN**

Sie haben bereits gesehen, dass Sie mit den DHCP-Optionen den/die Namensserver (Option 006) und den DNS-Domänennamen (Option 015) zuweisen können. Sie können auch die Integration von DHCP und DNS konfigurieren. Microsoft DNS unterstützt dynamische Updates, wodurch ein DNS-Client seinen Hosteintrag und andere Datensätze in der DNS-Zonendatenbank aktualisieren kann. Sie können auch den DHCP-Server so konfigurieren, dass er auf dem DNS-Server eines Clients automatisch den Host- (A) und den Zeigereintrag (PTR) des Clients aktualisieren kann.

Sie können die folgenden Optionen konfigurieren, die Sie in Abbildung 2–10 sehen:

- Dynamische DNS-Aktualisierungen nur nach Anforderung durch den Client vornehmen (dies ist die Standardeinstellung)
- DNS-Aktualisierungen immer automatisch vornehmen
- A- und PTR-Einträge beim Löschen der Lease verwerfen (standardmäßig aktiviert)

- Dynamische Aktualisierung für DHCP-Clients aktivieren, die keine Aktualisierungen anfordern (beispielsweise Clients unter Windows NT 4.0)
- Dynamische Aktualisierungen für DNS-PTR-Einträge deaktivieren

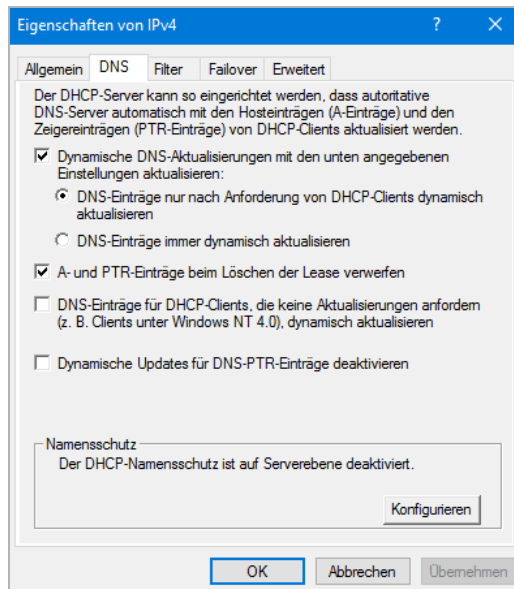
Mit den Standardeinstellungen können die meisten Clients ihre DNS-Einträge selbst aktualisieren. Jedoch löscht der DHCP-Server den Host- und Zeigereintrag aus der DNS-Zone immer dann, wenn eine Adresslease abläuft.

Sie können die Option Namensschutz verwenden, um die DNS-Zone vor inkorrekten oder unsicheren Aktualisierungen zu schützen. Wenn der DHCP-Server versucht, einen DNS-Namen zu aktualisieren, und er dabei entdeckt, dass ein anderer Client den Namen bereits aktualisiert hat, schlägt die Aktualisierung fehl.



**PRÜFUNGSTIPP**

Damit die Einstellung Namensschutz funktioniert, müssen Ihre DNS-Zonen für sichere dynamische Updates konfiguriert sein.



**Abb. 2-10** DNS-Optionen für IPv4 konfigurieren



**PRÜFUNGSTIPP**

Sie können die gleichen Einstellungen im Knoten *IPv6* vornehmen, um die DNS-Integrationsoptionen Ihrer IPv6-Clients zu konfigurieren.

## DHCP-Richtlinien konfigurieren

Sie können DHCP-Richtlinien verwenden, um Ihren DHCP-Clients bestimmte IPv4-Optionen zuzuweisen. Die Optionen werden von DHCP anhand der Bedingungen in Ihrer Richtlinie zugewiesen, einschließlich der Benutzer- und der Herstellerklassen, der MAC-Adressen sowie anderer Faktoren. So können Sie beispielsweise eine Richtlinie erstellen, die dafür sorgt, dass den Laptopcomputern Adressen aus einem bestimmten Adressbereich zugewiesen werden, oder die für Desktopcomputer eine längere Leasedauer verwendet.



### **PRÜFUNGSTIPP**

Sie können Richtlinien auf der Serverebene erstellen, die für alle DHCP-Bereiche gelten, oder Richtlinien auf Bereichsebene, die nur auf einen bestimmten Bereich angewendet werden.

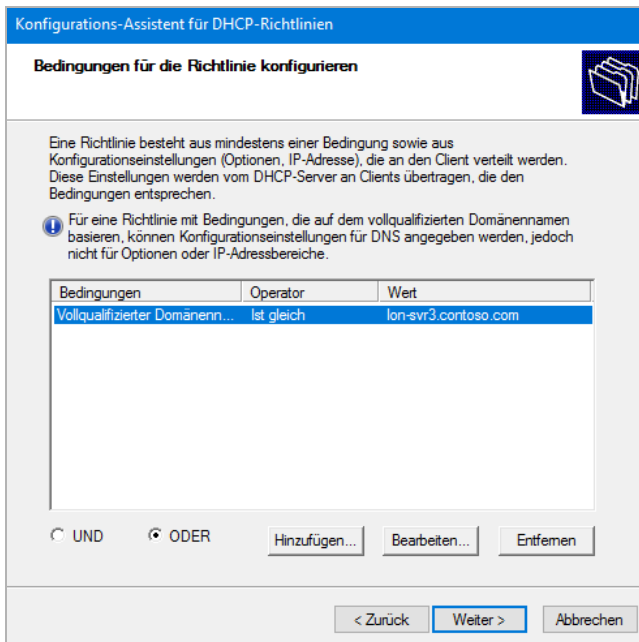
---

Zum Erstellen einer DHCP-Richtlinie verwenden Sie die DHCP-Konsole oder das Windows PowerShell-Cmdlet `Add-DhcpServerv4Policy`. Um in der DHCP-Konsole eine neue Richtlinie auf Serverebene zu erstellen, klicken Sie unterhalb des Knotens *IPv4* den Knoten *Richtlinien* mit der rechten Maustaste an und wählen dann im Kontextmenü den Befehl *Neue Richtlinie*. Um eine Richtlinie für einen Bereich zu erstellen, verwenden Sie den Knoten *Richtlinien* unterhalb des gewünschten Bereichs.

Beim Erstellen einer Richtlinie geben Sie die folgenden Informationen an:

- **Richtliniename und Beschreibung** Verwenden Sie aussagekräftige Namen und Beschreibungen, damit der Zweck der Richtlinie einfach zu erkennen ist.
- **Bedingungen** Eine Bedingung besteht aus einem Kriterium und einem Operator wie *Ist gleich* oder *Ist ungleich* (siehe Abb. 2–11). Legen Sie eine oder mehrere Bedingungen fest, die erfüllt sein müssen, damit die Richtlinie angewendet wird. Mit den Operatoren *UND* und *ODER* legen Sie fest, ob mehrere Bedingungen erfüllt sein müssen oder ob es ausreicht, wenn eine der Bedingungen zutrifft. Sie können zwischen den folgenden Kriterien wählen:
  - Herstellerklasse
  - Benutzerklasse
  - MAC-Adresse
  - Clientkennung
  - Vollqualifizierter Domänenname
  - Informationen zum Relay-Agent
- **IP-Adressbereich** Bei Richtlinien auf Bereichsebene können Sie aus dem Adresspool, der dem Bereich zugewiesen ist, einen IP-Adressbereich festlegen, aus dem den Clients eine Adresse zugewiesen wird, falls sie die Bedingung/en erfüllen.

- **Optionen** Nur bei Bereichsrichtlinien können Sie DHCP-Optionen konfigurieren, die den Clients zugewiesen werden, die bestimmte Bedingungen erfüllen: 003 Router, 006 DNS-Server und 015 DNS-Domänenname. Bei Richtlinien auf Serverebene weisen Sie diese Optionen zu, nachdem Sie die Richtlinie erstellt haben.



**Abb. 2-11** Richtlinienbedingungen erstellen

Nachdem Sie die Richtlinie erstellt haben, können Sie allgemeine DHCP-Optionen, wie Router und DNS-Server und DNS-spezifische Einstellungen, konfigurieren. Klicken Sie hierzu die Richtlinie im Knoten *Richtlinien* mit der rechten Maustaste an und wählen Sie den Befehl *Eigenschaften*. Sie können dann die folgenden Registerkarten verwenden:

- **Allgemein** Hier können Sie die Leasedauer für die Richtlinie festlegen. Schalten Sie das Kontrollkästchen *Leasedauer der Richtlinie festlegen* ein und konfigurieren Sie dann die Dauer.
- **Bedingungen** Hier können Sie die Konfiguration der Bedingungen für die Richtlinie anpassen.
- **IP-Adressbereich** Bei Richtlinien auf Bereichsebene können Sie die Konfiguration des IP-Adressbereichs ändern.
- **Optionen** Hier finden Sie alle Standard-DHCP-Optionen wie 003 Router, 006 DNS-Server und 015 DNS-Domänenname.
- **DNS** Sie können die DNS-Integrationseinstellungen für Clients ändern, auf die sich diese Richtlinie auswirkt.

## **WEITERE INFORMATIONEN** Schritt-für-Schritt: Konfigurieren von DHCP mit richtlinienbasierter Zuweisung

Weitere Informationen über die Verwendung von DHCP-Richtlinien finden Sie auf der Microsoft TechNet-Website unter:

[https://technet.microsoft.com/library/hh831538\(v=ws.11\).aspx](https://technet.microsoft.com/library/hh831538(v=ws.11).aspx)

## IPv6-Adressierung mit DHCPv6 implementieren

Auch wenn IPv6 noch nicht sehr verbreitet ist, so wird es doch immer häufiger verwendet. Manchmal ist dies nötig, um Anwendungen zu unterstützen, die IPv6 benötigen. DHCP unterstützt IPv6 durch die Verwendung von IPv6-Bereichen. Sie können diese Bereiche so konfigurieren und verwalten, wie Sie es bei IPv4-Bereichen machen, und hierfür sowohl die DHCP-Konsole als auch Windows PowerShell-Cmdlets verwenden.

IPv6-Knoten können auf unterschiedliche Weise eine IPv6-Konfiguration erhalten. Diese sind:

- **Statusfrei (stateless)** Für die Adresskonfiguration wird lediglich das Router-Advertisement verwendet. Bei der statusfreien Autokonfiguration wird lediglich ein Routerpräfix verwendet. Diese Methode stellt keine Konfigurationsoptionen, wie DNS-Server, zur Verfügung.
- **Statusbehaftet (stateful)** Für die Zuweisung von Adressen und anderen Konfigurationsoptionen wird ein DHCPv6-Server verwendet.
- **Beide** Der IPv6-Client erhält seine Konfiguration anhand von Router-Advertisements und DHCPv6.



### **PRÜFUNGSTIPP**

Wenn ein IPV6-Gerät mit einem DHCPv6-Server kommuniziert, verwendet es IPv6-Multicast-Adressen. Hingegen benötigen IPv4-Geräte IPv4-Broadcast-Adressen.

---

Beim Erstellen eines IPv6-Bereichs geben Sie die folgenden Informationen an:

- **Name und Beschreibung** Diese sollten aussagefähig sein, damit Sie den Bereich einfach identifizieren können.
- **Präfix** IPv6 verwendet Präfixe, ähnlich wie IPv4 Subnetzmasken verwendet. Jede IPv6-Adresse besteht aus 128 Bits. Das IPv6-Präfix gibt an, wie viele Bits für Informationen wie IPv6-Subnetze, Routen und Adressbereiche verwendet werden.

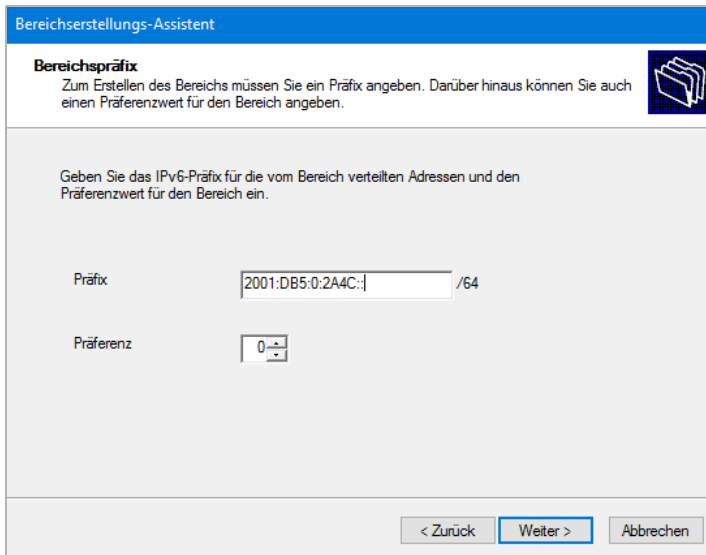


### **PRÜFUNGSTIPP**

IPv6-Präfixe verwenden folgende Notation: *Adresse/Präfixlänge*. So ist beispielsweise 2001:DB5:0:2A4C::/64 eine IPv6-Adresspräfix für ein Subnetz.

---

- **Präferenz** Falls mehrere DHCPv6-Server einem Client eine IPv6-Konfiguration anbieten, verwendet der Client den Server mit dem höchsten Präferenzwert. Falls mehrere Server den gleichen Präferenzwert besitzen, wählt der Client das Angebot aus, in dem die meisten Optionen konfiguriert sind. Diese Einstellung wird nicht verwendet, wenn Sie, wie in Abbildung 2–12 zu sehen, für *Präferenz* den Wert 0 (den Standardwert) verwenden.



**Abb. 2–12** Das Präfix und die Präferenz für einen DHCPv6-Bereich konfigurieren

- **Ausschlüsse** Geben Sie, je nachdem, was Sie aus dem Bereich ausschließen wollen, eine Adresse, mehrere Adressen oder einen Adressbereich ein.
- **Leasedauer** Der Standardwert ist acht Tage.

Sie können auch das Windows PowerShell-Cmdlet `Add-DhcpServerv6Scope` verwenden, um einen IPv6-Bereich zu erstellen. Beispielsweise erzeugt der folgende Befehl einen IPv6-Bereich mit dem Präfix `2001:DB5:0:2A4C::` und dem Bereichsnamen `LondonScope`:

```
Add-DhcpServerv6Scope -Prefix 2001:DB5:0:2A4C:: -Name "LondonScope"
```

Die meisten der Konfigurationsoptionen, die für IPv4-Bereiche zur Verfügung stehen, können Sie auch in IPv6-Bereichen verwenden. Sie können beispielsweise IPv6-Serveroptionen konfigurieren oder die Optionen auf der Ebene des Bereichs, der Klasse oder einer einzelnen Reservierung festlegen. Die Optionen zur DNS-Integration stehen auf der Registerkarte *DNS* des *Eigenschaften*-Dialogfelds eines IPv6-Knotens zur Verfügung, so wie Sie es bereits von IPv4 kennen.

#### **HINWEIS**

Die IPv6-Adressierung wird ausführlicher in Kapitel 5 und dort im Abschnitt »Prüfungsziel 5.1: IPv4- und IPv6-Adressierung implementieren« (S. 253) beschrieben.

## DHCP-Relay-Agent und PXE-Boot konfigurieren

Um auch DHCP-Clients in Subnetzen, in denen sich kein lokaler DHCP-Server befindet, zu unterstützen, können Sie in Ihrem Netzwerk einen DHCP-Relay-Agent aktivieren und konfigurieren. Damit auch Clientcomputer booten können, auf denen lokal kein Betriebssystem installiert ist, können Sie die PXE-Boot-Umgebung aktivieren und konfigurieren.

### DHCP-Relay-Agent konfigurieren

Ein großer Teil des DHCP-Netzwerkverkehrs ist Broadcast-basiert. Dies bedeutet, dass die Netzwerkkommunikation zwischen einem DHCP-Server und einem DHCP-Client nicht über Router übertragen wird. (In der Regel leiten Router keine Broadcast-Pakete weiter.) Falls sich ein Client, der eine IP-Konfiguration benötigt, in einem Subnetz ohne lokalen DHCP-Server befindet, kann er daher keine IP-Konfiguration erhalten.

Mit dem DHCP-Relay-Agent können Sie dieses Problem lösen. Der DHCP-Relay-Agent empfängt den Broadcast-basierten DHCP-Datenverkehr auf den konfigurierten Netzwerkschnittstellen. Die DHCP-Client-Pakete werden an einen konfigurierten DHCP-Server, der sich in einem anderen Subnetz befindet, weitergeleitet. So ist der DHCP-Client in der Lage, eine IP-Konfiguration zu erhalten.

Heutzutage ist diese Funktionalität bereits in vielen Netzwerkroutern integriert. Falls Ihre Router die in RFC 1542 definierte BOOTP-Weiterleitung nicht unterstützen, können Sie den DHCP-Relay-Agent auf einem Computer mit Windows Server 2016 installieren, und zwar in jedem Subnetz, in dem sich kein DHCP-Server befindet.

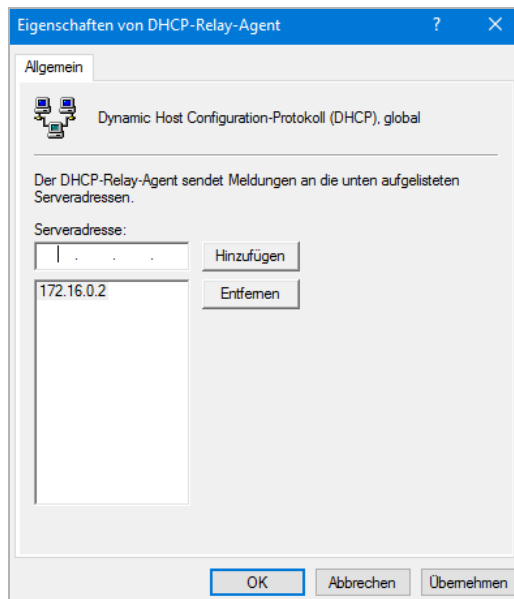
Der DHCP-Relay-Agent in Windows Server 2016 ist ein Feature des Routing-Rollendienstes in der Serverrolle Remotezugriff und nicht der DHCP-Serverrolle. Gehen Sie folgendermaßen vor, um den DHCP-Relay-Agent zu installieren und zu konfigurieren:

1. Installieren Sie mit Server-Manager die Serverrolle *Remotezugriff*.
2. Wenn Sie vom *Assistenten zum Hinzufügen von Rollen und Features* aufgefordert werden, die Rollendienste auszuwählen, schalten Sie das Kontrollkästchen *Routing* ein.
3. Klicken Sie nach der Installation im Server-Manager auf *Tools* und dann auf *Routing und RAS*.
4. Klicken Sie in der Konsole *Routing und RAS* Ihren Server mit der rechten Maustaste an und wählen Sie *Routing und RAS konfigurieren und aktivieren*.
5. Verwenden Sie im *Setup-Assistenten für den Routing- und RAS-Server* die Option *Benutzerdefinierte Konfiguration* und wählen Sie dann *LAN-Routing*.
6. Beenden Sie den Assistenten und starten Sie den LAN-Routingdienst, wenn Sie dazu aufgefordert werden.

Nachdem Sie den Routing- und RAS-Dienst installiert haben, müssen Sie den DHCP-Relay-Agent aktivieren und konfigurieren:

1. Erweitern Sie in der Konsole *Routing und RAS* den Knoten *IPv4*, klicken Sie den Knoten *Allgemein* mit der rechten Maustaste an und wählen Sie *Neues Routingprotokoll*.
2. Markieren Sie die Option *DHCP Relay Agent* und klicken Sie auf *OK*.

3. Klicken Sie im Navigationsbereich den Eintrag *DHCP-Relay-Agent* mit der rechten Maustaste an und wählen Sie *Neue Schnittstelle*. Sie müssen alle Netzwerkschnittstellen hinzufügen, über die möglicherweise DHCP-Anforderungen empfangen werden. Hierzu gehören sowohl die Schnittstellen, die DHCP-Clients ohne einen lokalen DHCP-Server enthalten, als auch die Schnittstellen mit einem DHCP-Server. Nachdem Sie die Schnittstellen hinzugefügt haben, werden ihre Eigenschaften angezeigt. Sie können dann festlegen, ob auf dieser Schnittstelle DHCP-Pakete weitergeleitet werden oder nicht.
4. Klicken Sie im Navigationsbereich den Eintrag *DHCP-Relay-Agent* mit der rechten Maustaste an und wählen Sie *Eigenschaften*, um das entsprechende Dialogfeld zu öffnen (siehe Abb. 2–13). Geben Sie die IP-Adresse von einem oder mehreren DHCP-Servern ein, klicken Sie auf *Hinzufügen* und dann auf *OK*.



**Abb. 2–13** Konfiguration des DHCP-Relay-Agents

## PXE Boot konfigurieren

Die meisten Computer können über eine Netzwerkkarte gestartet werden, ohne dass lokal ein Betriebssystem installiert ist. Möglicherweise müssen Sie dieses Feature im BIOS oder der UEFI-Firmware Ihres Computers aktivieren. Um vom Netzwerk zu starten, muss der Computer in der Lage sein, mit einer Bereitstellungsplattform für Betriebssysteme, wie den Windows-Bereitstellungsdiensten (Windows Deployment Services, WDS), zu kommunizieren.

Wenn Sie einen Bereitstellungsdienst, wie die Windows-Bereitstellungsdienste, implementieren, verwendet er die gleichen Kommunikations-Ports wie DHCP. Die Nachrichten DHCP-DISCOVER und DHCP-OFFER verwenden die UDP-Ports 67 und 68 (User Datagram Protocol, UDP). Dies sind die gleichen Ports, wie sie vom PXE-Server der Windows-Bereitstellungsdienste verwendet werden.



Wenn Sie sowohl DHCP als auch die Windows-Bereitstellungsdienste auf demselben Computer installieren, führt dies zu einem Portkonflikt. Um dieses Problem zu beheben, müssen Sie die Konfiguration der verwendeten Ports anpassen. Sie können dies erledigen, indem Sie in DHCP die Clientoption 060 Pre-Boot Execution (PXE) konfigurieren. Außerdem müssen Sie die Optionen 066 Hostname des Startservers und 067 Name der Startdatei ändern.

Die Optionen 066 und 067 können Sie in der DHCP-Konsole ändern. Für die Option 060 ist dies nicht möglich und Sie müssen das Befehlszeilenwerkzeug Netsh.exe einsetzen:

1. Öffnen Sie auf Ihrem DHCP-Computer eine Eingabeaufforderung mit erhöhten Rechten.
2. Geben Sie **Netsh.exe** ein und drücken Sie .
3. Geben Sie an der Eingabeaufforderung `netsh> dhcp` ein und drücken Sie .
4. Geben Sie an der Eingabeaufforderung `netsh dhcp> server \\Servername` ein und drücken Sie , um sich mit dem DHCP-Server zu verbinden. Ersetzen Sie *Servername* durch den Namen Ihres Servers.
5. Geben Sie an der Eingabeaufforderung `netsh dhcp server>` folgenden Befehl ein und drücken Sie : **add optiondef 60 PXEClient String 0 comment=PXE-Support.**
6. Geben Sie an der Eingabeaufforderung `netsh dhcp server>` folgenden Befehl ein und drücken Sie : **set optionvalue 60 STRING PXEClient.**
7. Geben Sie an der Eingabeaufforderung `netsh dhcp server> exit` ein, drücken Sie  und beenden Sie die Eingabeaufforderung.



#### **PRÜFUNGSTIPP**

Nachdem Sie diese Änderung vorgenommen haben, sollten Sie den DHCP-Dienst neu starten.

---

Sie können Option 060 auch in der DHCP-Managementkonsole hinzufügen, indem Sie den Knoten *IPv4* mit der rechten Maustaste anklicken, den Befehl *Vordefinierte Optionen einstellen* wählen und dann im Dialogfeld *Vordefinierte Optionen und Werte* auf *Hinzufügen* klicken. Oder Sie verwenden hierfür Windows PowerShell:

```
Add-DhcpServerv4OptionDefinition -ComputerName MyDHCPserver -Name PXEClient  
-Description "PXE-Support" -OptionId 060 -Type String
```

So legen Sie den Wert der Option für einen Bereich fest:

```
Set-DhcpServerv4OptionValue -ComputerName MeinDHCPserver -ScopeId "MyScope"  
-OptionId 060 -Value "PXEClient"
```

## **DHCP-Server exportieren, importieren und migrieren**

Es kann ab und zu vorkommen, dass Sie die DHCP-Serverrolle von einem auf einen anderen Computer verschieben wollen. Um diese Migration der Serverrolle durchzuführen, müssen Sie wissen, wie Sie die DHCP-Serverrolle und die Daten exportieren und importieren.

## Export und Import eines DHCP-Servers vornehmen

Falls Sie die Daten eines DHCP-Servers exportieren wollen, können Sie das Windows PowerShell-Cmdlet `Export-DhcpServer` verwenden. Der folgende Befehl exportiert beispielsweise die DHCP-Daten in eine Datei mit dem Namen `lon-svr2_export`:

```
Export-DhcpServer -ComputerName lon-svr2 -Leases -File C:\lon-svr2_export.xml  
-verbose
```



### **PRÜFUNGSTIPP**

Sie können auch das Befehlszeilenwerkzeug `Netsh.exe` verwenden. Geben Sie an der Eingabeaufforderung `netsh dhcp server>` den Befehl **Export C:\lon-svr2\_export.txt** all ein.

---

Um die DHCP-Serverdaten eines Exportvorgangs zu importieren, verwenden Sie das Windows PowerShell-Cmdlet `Import-DhcpServer`. Beispielsweise importiert der folgende Befehl die DHCP-Daten in der Datei `c:\lon-svr2_export.xml` in den neuen DHCP-Server mit dem Namen `LON-SVR3`:

```
Import-DhcpServer -ComputerName LON-SVR3 -Leases -File C:\lon-svr2_export.xml  
-BackupPath C:\ -Verbose
```



### **PRÜFUNGSTIPP**

Sie können auch das Befehlszeilenwerkzeug `Netsh.exe` verwenden. Geben Sie an der Eingabeaufforderung `netsh dhcp server>` den Befehl **Import C:\lon-svr2\_export.txt** all ein.

---

## DHCP-Server-Migration durchführen

Falls Sie einen älteren Server ersetzen wollen, müssen Sie die Rollen migrieren, die auf dem Server ausgeführt werden, zu denen möglicherweise auch die DHCP-Serverrolle gehört. Die Migration der DHCP-Serverrolle ist nicht kompliziert, jedoch müssen Sie für den Export und den Import entweder das Befehlszeilenwerkzeug `Netsh.exe` oder die entsprechenden Windows PowerShell-Cmdlets verwenden.

Führen Sie zur Migration Ihres DHCP-Servers die folgenden Aktionen durch:

1. Stellen Sie auf dem neuen Windows Server 2016-Computer die DHCP-Serverrolle bereit.
2. Beenden Sie auf dem alten DHCP-Server den DHCP-Dienst.
3. Exportieren Sie auf dem alten Server die DHCP-Daten.
4. Kopieren Sie die DHCP-Daten auf den neuen Server.
5. Importieren Sie die DHCP-Daten auf dem neuen Server.

## Prüfungsziel 2.2: DHCP verwalten und warten

---

Nachdem Sie DHCP installiert und die erforderlichen DHCP-Bereiche erstellt und konfiguriert haben, ist es wichtig zu wissen, wie Sie die DHCP-Serverrolle verwalten. Hierzu gehören die Konfiguration der Hochverfügbarkeit für DHCP-Server, die Verwaltung der DHCP-Datenbank und das Beheben von Problemen der DHCP-Rolle.

### **HINWEIS**

Die Konfiguration der Leasedauer ist im Abschnitt »DHCP-Adressbereiche erstellen und verwalten« (S. 66) beschrieben.

## Hochverfügbarkeit mit DHCP-Failover konfigurieren

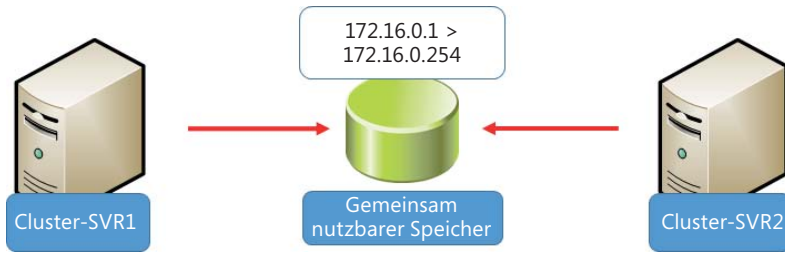
Wenn ein DHCP-Server offline ist, verwenden die Clients weiter die zugewiesene IP-Konfiguration. Neue Clients können jedoch keine Konfiguration erhalten; Clients, die ihre Lease erneuern wollen, sind dazu nicht mehr in der Lage. Aus diesen Gründen ist es wichtig, dass DHCP hochverfügbar ist, um ununterbrochen die Anforderungen nach einer IPv4- oder IPv6-Konfiguration bedienen zu können.

## Hochverfügbarkeitsoptionen für DHCP

Um Hochverfügbarkeit zu gewährleisten, scheint es naheliegend zu sein, mehrere DHCP-Server bereitzustellen und auf allen Servern die gleiche/n Zone/n zu konfigurieren. Aufgrund der Art und Weise, wie die Kommunikation zwischen DHCP-Client und -Server verläuft, gibt es kein einfaches Verfahren, mit einem DHCP-Server denselben Adressbereich zu verwenden, der sich auf einem anderen DHCP-Server befindet. Dies kann dazu führen, dass mehrere Clients von unterschiedlichen DHCP-Servern die gleiche IP-Konfiguration erhalten, ohne dass es möglich ist, den sich hieraus ergebenden Konflikt zu lösen.

Windows Server 2016 stellt für dieses Problem verschiedene Lösungen bereit. Diese sind:

- **DHCP in einem Windows-Failover-Cluster (Rechnerverbund)** Sie können ein Windows Server-Cluster einrichten, das aus zwei Mitgliedsservern besteht. Sie können die DHCP-Serverrolle auf beiden Clustermitgliedern installieren und dann auf beiden Servern identische Zonen, oder auch nur eine Zone, einrichten. Installieren Sie die DHCP-Daten auf einem gemeinsamen nutzbaren Speicher im Cluster. Falls einer der Clusterknoten ausfällt, kann der andere Knoten ohne Unterbrechung die Clientanforderungen bedienen (siehe Abb. 2–14).



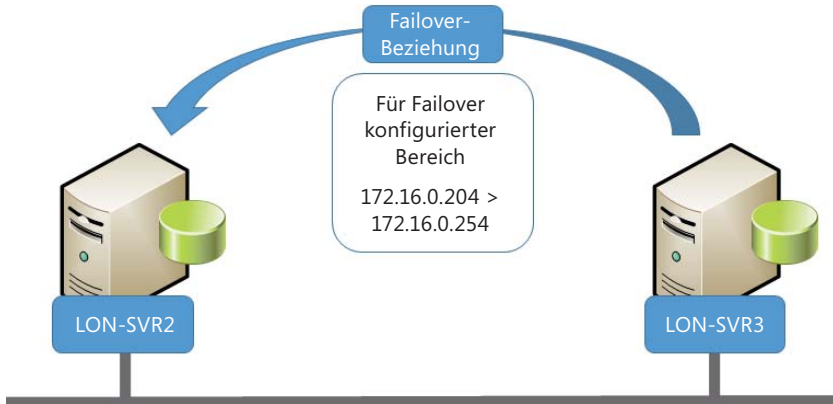
**Abb. 2-14** Server-Clustering mit DHCP

- DHCP-Bereichsaufteilung** Sie installieren die DHCP-Serverrolle auf zwei Servern. Auf jedem Server konfigurieren Sie eine Teilmenge der für Ihr Subnetz verfügbaren IP-Adressen und stellen sicher, dass es keine Überlappungen gibt (siehe Abb. 2-15). Anschließend verwenden Sie auf jedem Server die Verzögerungskonfiguration, um so einen primären Server festzulegen. Falls der primäre Server ausfällt, kann der sekundäre Server weiterhin die Clientanforderungen bedienen.



**Abb. 2-15** DHCP-Bereichsaufteilung verwenden

- DHCP-Failover** Mit DHCP-Failover können Sie zwei DHCP-Server so konfigurieren, dass sie denselben Subnetzen IP-Konfigurationen zuteilen. Die beiden DHCP-Server replizieren untereinander die Leaseinformationen, wie in Abbildung 2-16 zu sehen. Wenn einer der Server ausfällt, stellt der andere Server weiterhin für das/die konfigurierte Subnetz/e DHCP-Dienste bereit.



**Abb. 2-16** DHCP-Failover-Partner

## DHCP-Bereichsaufteilung konfigurieren

Für die Implementierung der DHCP-Bereichsaufteilung ist keine komplexe Konfiguration erforderlich, wie es beim Bereitstellen eines Windows-Failover-Clusters der Fall ist. Im Prinzip konfigurieren Sie auf jedem DHCP-Server einen ähnlichen DHCP-Bereich; Sie verwenden den gleichen Pool von IP-Adressen, lediglich die ausgeschlossenen Adressen unterscheiden sich.

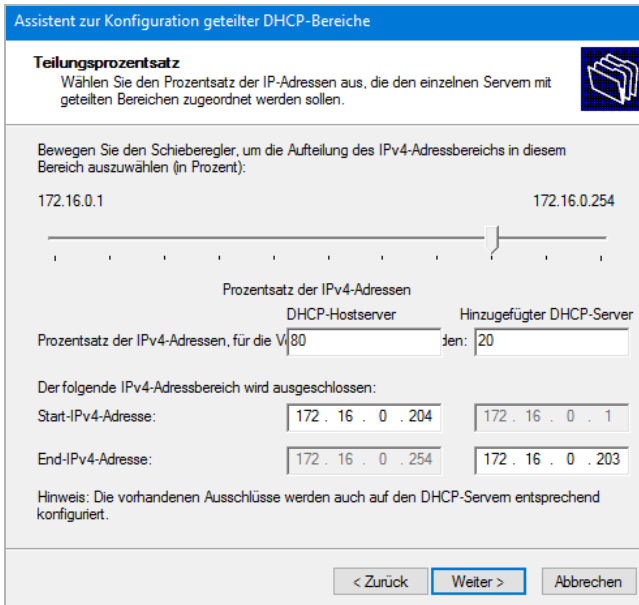
Angenommen, Sie haben zwei DHCP-Server, LON-SVR2 und LON-SVR3, Sie verwenden das Subnetz 172.16.0.0/24 und Ihnen steht ein Pool von 254 IPv4-Adressen zur Verfügung. Um für diese Konfiguration die DHCP-Bereichsaufteilung einzurichten, müssen Sie diese Aktionen durchführen:

1. Erstellen Sie auf einem Server einen Bereich mit dem IP-Adressbereich von 172.16.0.1 bis 172.16.0.254. Aktivieren Sie diesen Bereich nicht.
2. Starten Sie den Assistenten zur Konfiguration geteilter DHCP-Bereiche. Geben Sie im Assistenten folgende Informationen an:
  - Name des zusätzlichen DHCP-Servers
  - Aufteilung des IP-Adresspools des Bereichs zwischen den beiden DHCP-Servern
  - Konfigurieren Sie auf den beiden Servern unterschiedliche Verzögerungen beim DHCP-Angebot. Diese Werte bestimmen, welcher Server der primäre Server ist.
3. Aktivieren Sie beide Bereiche.

Nachdem Sie auf Ihrem primären DHCP-Server den Bereich erstellt haben, gehen Sie folgendermaßen vor, um einen geteilten Bereich zu erstellen:

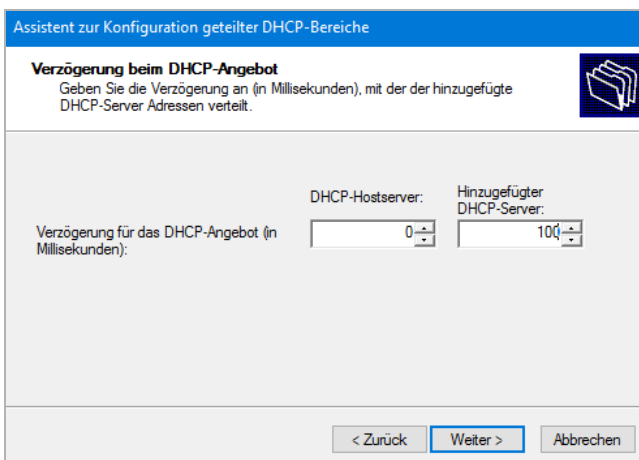
1. Klicken Sie in der Konsole *DHCP* den Bereich mit der rechten Maustaste an; klicken Sie auf *Erweitert* und dann auf *Geteilter Bereich*.
2. Klicken Sie auf der Einführungsseite des *Assistenten zur Konfiguration geteilter DHCP-Bereiche* auf *Weiter*.

3. Geben Sie auf der Seite *Zusätzlicher DHCP-Server* in das gleichnamige Textfeld den vollqualifizierten Domänennamen des sekundären DHCP-Servers ein und klicken Sie auf *Weiter*.
4. Verwenden Sie den Schieberegler auf der Seite *Teilungsprozentsatz*, die Abbildung 2–17 zeigt, um die Adressen zwischen den beiden DHCP-Servern zu verteilen. Klicken Sie dann auf *Weiter*.



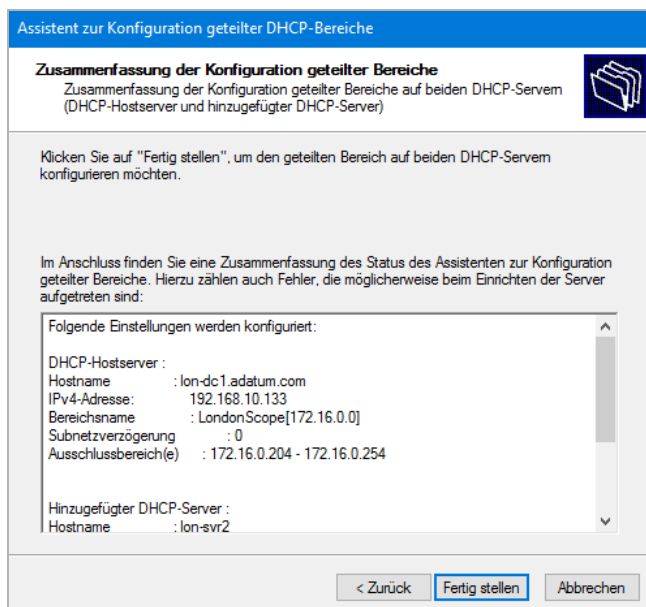
**Abb. 2–17** Die Verteilung der IP-Adressen für den geteilten Bereich festlegen

5. Legen Sie auf der Seite *Verzögerung beim DHCP-Angebot*, die Sie in Abbildung 2–18 sehen, die Verzögerung für jeden Server fest und klicken Sie dann auf *Weiter*. Der Server mit der geringsten Verzögerung wird der primäre Server.



**Abb. 2–18** Den Masterserver für eine Konfiguration mit einem geteilten DHCP-Bereich festlegen

6. Klicken Sie auf der Seite *Zusammenfassung der Konfiguration geteilter Bereiche* auf *Fertig stellen*. In Abbildung 2–19 können Sie erkennen, dass der *Assistent zur Konfiguration geteilter DHCP-Bereiche* auf dem sekundären Server den erforderlichen Bereich erstellt. Außerdem werden Ausschlüsse erstellt, damit jeder Server lediglich den vorher festgelegten Prozentsatz der Adressen aus dem Pool zuweisen kann. Klicken Sie auf *Schließen*.



**Abb. 2–19** Die Zusammenfassung der Konfiguration des geteilten DHCP-Bereichs

Sie können eine ähnliche Konfiguration manuell erstellen, indem Sie auf jedem Server übereinstimmende Bereiche erstellen und dann manuell die ausgeschlossenen IP-Adressen und die Subnetzverzögerung konfigurieren.

## DHCP-Failover konfigurieren

Mit geteilten DHCP-Bereichen wird zwar der primären Sorge Rechnung getragen, dass zur Beantwortung von DHCP-Anforderungen immer ein Server zur Verfügung steht. Der Nachteil besteht darin, dass der zur Verfügung stehende IP-Adressbereich zwischen zwei Servern aufgeteilt werden muss. Daher kann dies nur eine kurzfristige Lösung sein. In größeren Netzwerken, in denen der Adresspool knapp wird, kann dieser Ansatz während DHCP-Ausfällen möglicherweise nicht gut funktionieren. Als Alternative können Sie die Implementierung von DHCP-Failover in Erwägung ziehen.



### **PRÜFUNGSTIPP**

Bei DHCP-Failover können Sie lediglich zwei Server koppeln. Weiterhin können Sie nur IPv4-Bereiche und Subnetze verwenden. Für IPv6-Bereiche wird DHCP-Failover nicht unterstützt.

Bei der Konfiguration von DHCP-Failover können Sie zwischen zwei Modi wählen. Diese sind:

- **Lastenausgleich** Im Modus Lastenausgleich vergeben beide Server gleichzeitig IPv4-Konfigurationen. Die Gewichtung, die Sie den Servern zuweisen, bestimmt, wie die Arbeitslast verteilt und wie die Server auf IP-Konfigurationsanforderungen antworten.



**PRÜFUNGSTIPP**

Standardmäßig ist der Modus Lastenausgleich ausgewählt. Das Standardverhältnis ist 50/50, wodurch die Last gleichmäßig auf beide Server verteilt wird.

---

- **Hot Standby** Wenn Sie Hot Standby implementieren, legen Sie einen Server als primären und den anderen als sekundären Server fest. In diesem Modus vergibt nur der primäre Server IPv4-Konfigurationen an die Clients. Nur dann, wenn der primäre Server nicht verfügbar ist, nimmt der sekundäre Server dessen Aufgaben wahr.



**PRÜFUNGSTIPP**

Verwenden Sie den Modus Hot Standby in Bereitstellungen, in denen sich der Ersatzserver an einem anderen Standort befindet als der primäre Server. Damit die Failover-Nachrichten von Firewalls durchgelassen werden, müssen Sie darauf achten, den TCP-Port 647 freizugeben.

---

Führen Sie die folgenden Schritte durch, um DHCP-Failover zu konfigurieren.

1. Erstellen und konfigurieren Sie auf einem DHCP-Server den oder die Bereiche, die Sie benötigen.
2. Klicken Sie auf diesem Server in der DHCP-Konsole den Knoten *IPv4* mit der rechten Maustaste an und wählen Sie *Failover konfigurieren*.
3. Markieren Sie auf der Seite *Einführung* des Dialogfelds *Failover konfigurieren* alle DHCP-Bereiche, die Sie als Teil der Failoverbeziehung konfigurieren wollen. Klicken Sie auf *Weiter*.
4. Klicken Sie auf der Seite *Den Partnerserver angeben, der für Failover verwendet werden soll* auf *Server hinzufügen*. Wählen Sie den gewünschten anderen DHCP-Server aus und klicken Sie auf *Weiter*.
5. Konfigurieren Sie auf der Seite *Neue Failoverbeziehung erstellen* (siehe Abb. 2–20) die folgenden Parameter. Klicken Sie auf *Weiter* und dann auf *Fertig stellen*.
  - **Name der Beziehung** Verwenden Sie dieses Feld, um die Beziehung zu beschreiben.
  - **Maximale Clientvorlaufzeit** Dieser Wert wird im Hot-Standby-Modus verwendet. Er legt fest, wie lange der sekundäre Server warten muss, bevor er die Kontrolle über den DHCP-Bereich übernimmt. Der Standardwert ist eine Stunde, er kann nicht 0 betragen.



- **Modus** Wählen Sie zwischen *Lastenausgleich* und *Hot Standby*.
- **Lastenausgleich in Prozent** Wird verwendet, wenn Sie den Modus Lastenausgleich aktivieren. Hier können Sie festlegen, welchen Prozentsatz des Adresspools jeder Server verwaltet. Der Standardwert ist 50/50.
- **Rolle des Partnerservers** Verwenden Sie diese Einstellung im Modus Hot Standby. Sie können hier festlegen, welcher der Server der primäre und welcher der sekundäre ist. Wählen Sie zwischen *Aktiv* und *Standby*.



#### **PRÜFUNGSTIPP**

Sie können einen einzigen DHCP-Server so konfigurieren, dass er gleichzeitig als primärer DHCP-Server für einen und als sekundärer DHCP-Server für einen anderen Bereich fungiert.

---

- **Für Standbyserver reservierte Adressen** Verwenden Sie diesen Wert, um festzulegen, welchen Prozentsatz der Adressen im Bereich der sekundäre Server zuweisen kann, während er darauf wartet, dass die maximale Clientvorlaufzeit (Maximum Client Lead Time, MCLT) abläuft. Dies erlaubt es dem Standbyserver, einen kleinen Teil des IP-Adresspools zu verwenden, während er darauf wartet, ob der primäre Server wieder online ist. Der Standardwert ist fünf Prozent der im Bereich verfügbaren Adressen.
- **Intervall für Zustands-Switchover** Wenn ein Server die Verbindung mit seinem Replikationspartner verliert, kann er nicht ermitteln, warum dies passierte. Sie müssen den Status des Partners manuell auf »Partner down« setzen, um den verbleibenden Partner darüber zu informieren, dass der andere Server nicht verfügbar ist. Mit dem Intervall für Zustands-Switchover können Sie den Zustandswechsel automatisieren und festlegen, dass er nach einem bestimmten Intervall eintritt. Standardmäßig wird diese Einstellung nicht verwendet.
- **Nachrichtenauthentifizierung aktivieren** Sie können die Nachrichtenauthentifizierung konfigurieren und hierfür als Kennwort einen gemeinsamen geheimen Schlüssel verwenden. Hierdurch werden die Failovernachrichten zwischen den Replikationspartnern authentifiziert und sichergestellt, dass sie tatsächlich vom konfigurierten Failoverpartner stammen.
- **Gemeinsamer geheimer Schlüssel** Dieses Kennwort wird für die Nachrichtenauthentifizierung verwendet.

Failover konfigurieren

**Neue Failoverbeziehung erstellen**

Erstellen Sie eine neue Failoverbeziehung mit dem Partner "lon-svr2".

Name der Beziehung:

Maximale Clientvorlaufzeit:  Stunde  Minuten

Modus:

Lastenausgleich in Prozent

Lokaler Server: %

Partnerserver: %

Intervall für Zustands-Switchover:  Minuten

Nachrichtenthifizierung aktivieren

Gemeinsamer geheimer Schlüssel:

< Zurück Weiter > Abbrechen

**Abb. 2–20** DHCP-Failover konfigurieren

6. Klicken Sie im Dialogfeld *Status der Failoverkonfiguration* auf *Schließen*.

Sie können DHCP-Failover auch mit dem Windows PowerShell-Cmdlet `Add-DhcpServerv4Failover` konfigurieren. Um beispielsweise eine DHCP-Failoverbeziehung im Modus Lastenausgleich zwischen den Servern `lon-svr2.adatum.com` und `lon-svr3.adatum.com` mit dem Bereich `172.16.0.0`, der auf dem Partnercomputer `lon-svr3.adatum.com` erstellt werden soll, zu konfigurieren, geben Sie den folgenden Befehl ein:

```
Add-DhcpServerv4Failover -ComputerName lon-svr2.adatum.com -Name SF0-SIN-Failover
-PartnerServer lon-svr3.adatum.com -ScopeId 172.16.0.0 -SharedSecret "Pa$$w0rd"
```

#### **WEITERE INFORMATIONEN** DHCP-Server-Cmdlets in Windows PowerShell

Weitere Informationen über die Verwendung von Windows PowerShell zur Konfiguration in DHCP finden Sie auf der Microsoft TechNet-Website unter:

[https://technet.microsoft.com/library/jj590751\(v=wps.630\).aspx](https://technet.microsoft.com/library/jj590751(v=wps.630).aspx)

Nachdem Sie die Failoverbeziehung eingerichtet haben, können Sie folgende Wartungsaufgaben durchführen:

- **Einen Bereich replizieren** Ermöglicht Ihnen, zwischen den Partnern einer Failoverbeziehung alle Änderungen eines konfigurierten Bereich zu replizieren. Um einen Bereich zu replizieren, klicken Sie in der DHCP-Konsole unterhalb des Knotens *IPv4* den gewünschten Bereich mit der rechten Maustaste an und klicken auf *Bereich replizieren*.
- **Alle Bereiche replizieren** Ermöglicht Ihnen, zwischen den Partnern einer Failoverbeziehung alle Bereiche zu replizieren. Um diese Aufgabe durchzuführen, klicken Sie den Knoten *IPv4* mit der rechten Maustaste an und klicken auf *Failoverbereiche replizieren*.



#### **PRÜFUNGSTIPP**

Sie können diese Aufgaben auch mit dem Windows PowerShell-Cmdlet `Invoke-DhcpServerv4FailoverReplication` durchführen.

#### **WEITERE INFORMATIONEN Verstehen und Bereitstellen von DHCP-Failover**

Weitere Detailinformationen über DHCP-Failover finden Sie auf der Microsoft TechNet-Website unter:

[https://technet.microsoft.com/library/dn338978\(v=ws.11\).aspx](https://technet.microsoft.com/library/dn338978(v=ws.11).aspx)

## DHCP-Datenbank sichern und wiederherstellen

Die DHCP-Serverrolle speichert ihre Daten in einer Datenbank. Falls die Datenbank beschädigt wird, kann dies dazu führen, dass der Dienst nicht mehr verfügbar ist. Daher ist es wichtig zu wissen, wie Sie die DHCP-Datenbank sichern und wiederherstellen können.

### Die DHCP-Datenbank im Überblick

Die DHCP-Datenbank besteht aus zahlreichen Dateien, die sich im Ordner `%systemroot%\System32\dhcp` befinden. Die Dateien sind:

- **dhcp.mdb** Dies ist die Hauptdatenbankdatei des DHCP-Servers.
- **tmp.edb** Dies ist eine temporäre Arbeitsdatei, die verwendet wird, während an der Datenbankdatei Indizierungen und andere Wartungsarbeiten durchgeführt werden.
- **j50.log** Dies ist das Datenbanktransaktionsprotokoll. DHCP-Änderungen werden zuerst in das Transaktionsprotokoll eingetragen und vom Transaktionsprotokoll werden die Änderungen in die Datenbank überführt (commit). Nachdem die Datensätze erfolgreich übertragen wurden, wird ein Zeiger im Protokoll verschoben, um anzugeben, dass die Transaktion abgeschlossen ist. Dieser Prozess hilft dabei, während der Abarbeitung von Änderungen die Integrität der Datenbank nicht zu gefährden. Wenn das Transaktionsprotokoll voll ist, wird es umbenannt und eine neue Protokolldatei angelegt.

- **j5\*.log** Bei diesen fortlaufend nummerierten Dateien handelt es sich um die vorherigen Transaktionsprotokolle.
- **j50.chk** Dies ist die Prüfpunktdatei; sie wird verwendet, um festzustellen, welche Transaktionsprotokolle in die Datenbank committet wurden. Wenn der DHCP-Dienst startet, wird die Integrität der Datenbank gegen die aktuellen Transaktionen geprüft. Die Prüfpunktdatei beschleunigt diesen Vorgang.
- **j50res00001.jrs und j50res00002.jrs** Bei diesen beiden Dateien handelt es sich um reservierte Datenbankprotokolle, die zum Speichern noch nicht committeter Transaktionen der DHCP-Datenbank verwendet werden können. Diese Dateien werden dann verwendet, wenn der Speicherplatz auf dem Systemlaufwerk knapp wird. Wenn diese Dateien voll sind, beendet sich der DHCP-Dienst, um die Datenbankintegrität zu gewährleisten.

## Die DHCP-Datenbank sichern und wiederherstellen

Wenn Sie die DHCP-Datenbank sichern, werden im Backup die folgenden Informationen gespeichert:

- DHCP-Bereiche, konfigurierte Reservierungen und aktive Leases
- Serveroptionen, Bereichsoptionen, Klassen und Reservierungsoptionen
- Konfigurationseinstellungen, die Sie in den Eigenschaften des DHCP-Servers vorgenommen haben, und all diejenigen, die in der Registrierdatenbank gespeichert sind

### DIE DATENBANK SICHERN

Auch wenn die DHCP-Datenbank automatisch alle 60 Minuten gesichert wird, können Sie sie auch manuell sichern, wenn Sie beispielsweise umfangreiche Konfigurationsänderungen vorgenommen haben.

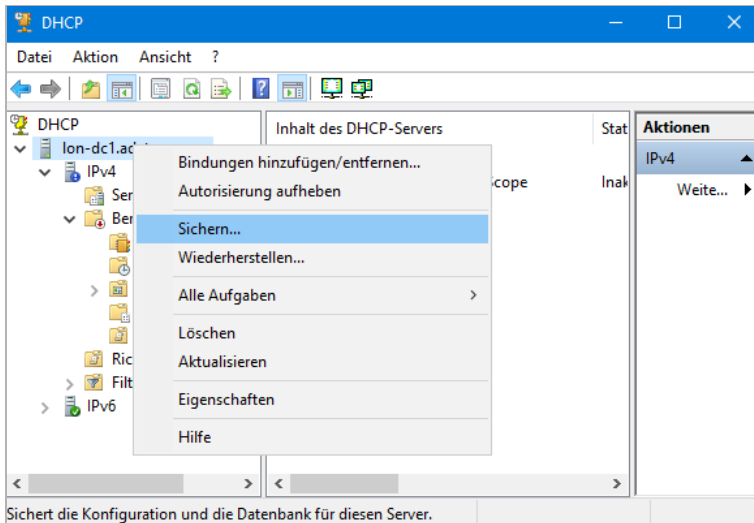


#### **PRÜFUNGSTIPP**

Sie können das Standardintervall für die automatische Sicherung der DHCP-Datenbank ändern, indem Sie den Wert *BackupInterval* im Schlüssel *HKLM\SYSTEM\CurrentControlSet\Services\DHCP\Parameters* der Registrierdatenbank bearbeiten.

---

Um die DHCP-Datenbank zu sichern, klicken Sie in der DHCP-Konsole den DHCP-Server mit der rechten Maustaste an und wählen den Befehl *Sichern* (siehe Abb. 2–21). Sie müssen dann den Ordner angeben, in dem die Sicherung gespeichert werden soll. Die Standardeinstellung ist %systemroot%\System32\dhcp\backup. Die Datenbank wird dann am angegebenen Ort gesichert.



**Abb. 2-21** Eine manuelle Sicherung der DHCP-Datenbank durchführen



**PRÜFUNGSTIPP**

Zur Sicherung der DHCP-Datenbank können Sie auch das Windows PowerShell-Cmdlet `Backup-DhcpServer` verwenden.

## Die Datenbank wiederherstellen

Falls Probleme mit DHCP auftauchen und eine Wiederherstellung der Daten das Problem lösen kann, können Sie die Datenbank folgendermaßen wiederherstellen. Klicken Sie in der DHCP-Konsole den DHCP-Server mit der rechten Maustaste an und wählen Sie den Befehl *Wiederherstellen*. Wechseln Sie zu dem Ordner, in dem Sie die Datensicherung gespeichert haben, und klicken Sie auf *OK*.

Der DHCP-Dienst muss angehalten werden, um ihn wiederherzustellen. Sie sehen daher ein Bestätigungsfeld mit dem Hinweis, dass der Dienst angehalten und neu gestartet werden muss. Klicken Sie auf *Ja*.



**PRÜFUNGSTIPP**

Zur Wiederherstellung der DHCP-Datenbank können Sie auch das Windows PowerShell-Cmdlet `Restore-DhcpServer` verwenden.

**HINWEIS**

Die Konfiguration des DHCP-Namenschutzes ist weiter vorne im Abschnitt »DHCP-Optionen konfigurieren« (S. 74) beschrieben.

# DHCP-Fehler beheben

DHCP versorgt Ihre Netzwerkgeräte, Clients und Server mit IP-Konfiguration. Wenn dieser Dienst nicht zur Verfügung steht, wirkt sich das schnell auf die Funktionalität des Netzwerks aus. Es ist daher wichtig, häufig vorkommende Symptome für Probleme bei der DHCP-Serverrolle erkennen und schnell geeignete Gegenmaßnahmen ergreifen zu können.

## Häufig auftretende DHCP-Probleme beschreiben

DHCP ist ein sehr zuverlässiger Dienst. Wenn er mit einer sorgfältig geplanten, ausfallsicheren und damit hoch verfügbaren Lösung implementiert ist, treten selten große Probleme auf. Dennoch kann es kleinere Störungen geben. In Tabelle 2–2 sind verschiedene Symptome beschrieben, die auf ein Problem mit der DHCP-Serverrolle hindeuten.

Symptom	Mögliche Ursache	Was Sie prüfen sollten
DHCP-Dienst wird nicht gestartet.	<ul style="list-style-type: none"> <li>Die Datenbank ist beschädigt.</li> </ul>	<ul style="list-style-type: none"> <li>Führen Sie eine Wiederherstellung der DHCP-Datenbank durch und versuchen Sie, den Dienst zu starten.</li> </ul>
DHCP-Dienst weist keine Adressleases zu.	<ul style="list-style-type: none"> <li>Möglicherweise wird der DHCP-Dienst nicht ausgeführt.</li> <li>Möglicherweise stehen im Adresspool unzureichend IP-Adressen zur Verfügung.</li> </ul>	<ul style="list-style-type: none"> <li>Prüfen Sie, ob der DHCP-Dienst läuft.</li> <li>Prüfen Sie, ob im Adresspool ausreichend IP-Adressen zur Verfügung stehen.</li> <li>Falls sich die Clients in einem anderen Subnetz befinden als der DHCP-Server, prüfen Sie, ob ein DHCP-Relay-Agent ausgeführt wird und ob er korrekt konfiguriert wurde.</li> </ul>
Client-Adresskonflikte	<ul style="list-style-type: none"> <li>Ein anderes Gerät oder ein anderer Dienst stellt DHCP-Funktionalität zur Verfügung.</li> <li>Zwei überlappende Bereiche bedienen im gleichen Subnetz IP-Konfigurationsanforderungen.</li> <li>Eine statisch zugewiesene Adresse kann im Konflikt mit einer dynamisch zugewiesenen Adresse stehen.</li> </ul>	<ul style="list-style-type: none"> <li>Stellen Sie fest, welche Geräte, wie WiFi Access Points oder Hubs, für die Zuteilung von IP-Adressen konfiguriert sind.</li> <li>Stellen Sie sicher, dass zwei benachbarte DHCP-Server keine überlappenden Adressbereiche aufweisen.</li> <li>Erwägen Sie, alle statisch zugewiesenen Adressen durch DHCP-Reservierungen zu ersetzen. Diese können Sie zentral verwalten und sie werden dem Adresspool entnommen.</li> </ul>
Der DHCP-Client ist nicht in der Lage, eine Adresse zu leasen, und fällt in den APIPA-Modus (Automatic Private IP Addressing) zurück.	<ul style="list-style-type: none"> <li>Es kann sein, dass der DHCP-Dienst nicht funktioniert.</li> <li>Möglicherweise stehen im Adresspool unzureichend IP-Adressen zur Verfügung.</li> <li>Möglicherweise befindet sich der DHCP-Client in einem Subnetz ohne DHCP-Server.</li> <li>Probleme bei der Netzwerkverkabelung</li> </ul>	<ul style="list-style-type: none"> <li>Prüfen Sie, ob der DHCP-Dienst läuft.</li> <li>Prüfen Sie, ob im Adresspool ausreichend IP-Adressen zur Verfügung stehen.</li> <li>Falls sich die Clients in einem anderen Subnetz befinden als der DHCP-Server, prüfen Sie, ob ein DHCP-Relay-Agent ausgeführt wird und ob er korrekt konfiguriert wurde.</li> <li>Stellen Sie sicher, dass alle per Kabel verbundenen Clients korrekt angeschlossen sind.</li> </ul>

**Tab. 2–2** Symptome häufig vorkommender DHCP-Probleme

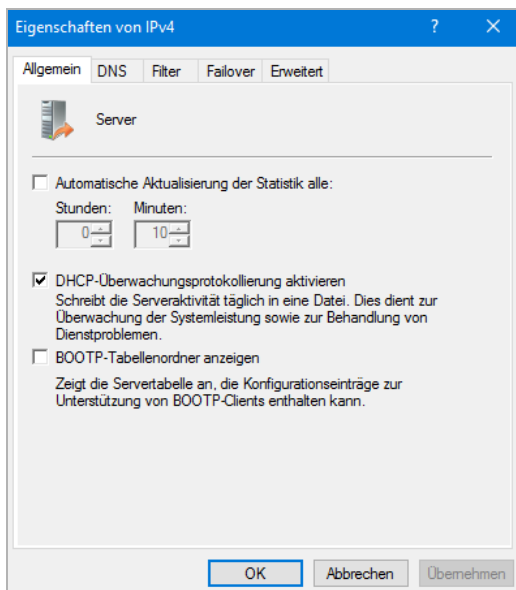
Tabelle 2–2 ist keine vollständige Liste, jedoch enthält sie einige der beim DHCP-Dienst am häufigsten auftretenden Symptome und deren Ursachen. Verwenden Sie für alle anderen Probleme die Standardverfahren für die Fehlersuche und die Fehlerbehebung in Netzwerken.

## Tools, mit denen sich häufig auftretende DHCP-Probleme lösen lassen

Es ist wichtig zu wissen, wie DHCP funktioniert. Nur so sind Sie in der Lage, auf effiziente Weise Probleme bei diesem Dienst in den Griff zu bekommen. Sie müssen sich gut mit den DHCP-Nachrichten auskennen, die bei der ersten Anforderung einer Adresslease und beim Erneuern versendet werden. Nur wenn Sie wissen, was zu erwarten ist, können Sie erkennen, wenn in diesem Prozess etwas schiefläuft.

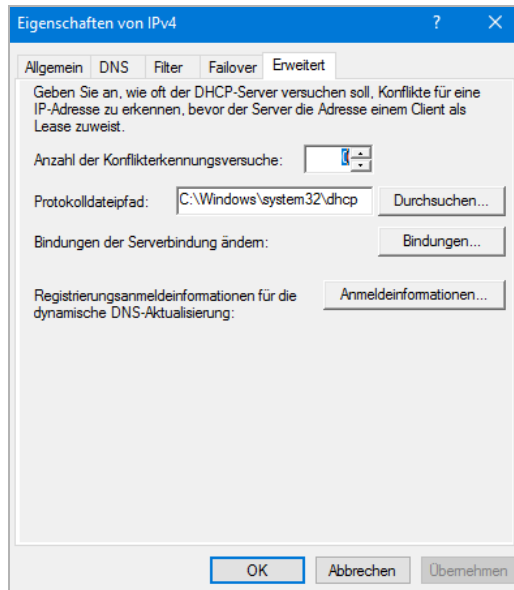
### DHCP-ÜBERWACHUNGSPROTOKOLLIERUNG VERWENDEN

Die DHCP-Überwachungsprotokollierung ist standardmäßig aktiviert. Sie können diese Einstellung überprüfen, indem Sie in der DHCP-Konsole auf den Knoten *IPv4* rechtsklicken und dann den Befehl *Eigenschaften* wählen (siehe Abb. 2–22). Auf der Registerkarte *Allgemein* sollte das Kontrollkästchen *DHCP-Überwachungsprotokollierung aktivieren* eingeschaltet sein.



**Abb. 2–22** Die DHCP-Überwachungsprotokollierung aktivieren

Nachdem Sie diese Option aktiviert haben, können Sie auf der Registerkarte *Erweitert* den *Protokolldateipfad* konfigurieren (siehe Abb. 2–23). Der Standardordner ist `%systemroot%\System32\dhcp`.



**Abb. 2-23** Den Protokolldateipfad für die DHCP-Überwachungsprotokollierung konfigurieren

Wenn diese Einstellung aktiviert ist, wird im angegebenen Ordner eine Protokolldatei mit dem Namen DhcpSrvLog – *Wochentag* erstellt, wobei *Wochentag* den Wochentag angibt, an dem die Protokolldatei erstellt wurde.



#### **PRÜFUNGSTIPP**

Die Protokolldatei mit dem Namensmuster DhcpV6SrvLog – *Wochentag* wird für IPv6-bezogene Ereignisse erstellt.

Sie können sich die Protokolldateien für DHCP-Ereignisse mit einem Texteditor, wie beispielsweise dem Editor (Notepad) von Windows, ansehen. Diese Datei enthält die Felder, die in Tabelle 2-3 aufgeführt sind.



Feld	Erklärung
ID	Die DHCP-Ereignis-ID
Datum	Datum, an dem das Ereignis protokolliert wurde
Zeit	Uhrzeit, zu der das Ereignis protokolliert wurde
Beschreibung	Eine kurze Beschreibung des Ereignisses
IP-Adresse	Die IP-Adresse des DHCP-Clients
Hostname	Der Hostname des DHCP-Clients
MAC-Adresse	Die MAC-Adresse (Media Access Control) des DHCP-Clients

**Tab. 2-3** Die Felder im DHCP-Aktivitätsprotokoll

Tabelle 2-4 enthält eine Liste der häufig auftretenden Ereignisse.

Ereignis-ID	Erläuterung
00	Das Protokoll wurde gestartet.
01	Das Protokoll wurde beendet.
02	Das Protokoll wurde aufgrund von unzureichendem Speicherplatz temporär angehalten.
10	Für einen Client wurde eine neue IP-Adresse geleast.
11	Eine Lease wurde von einem Client erneuert.
12	Eine Lease wurde von einem Client freigegeben.
13	Es wurde ermittelt, dass eine IP-Adresse im Netzwerk verwendet wird.
14	Eine Leaseanforderung konnte nicht erfüllt werden, da der Adresspool des Bereichs erschöpft war.
15	Eine Lease wurde verweigert.
20	Eine BOOTP-Adresse (Bootstrap Protocol) wurde einem Client geleast.
51	Ein DHCP-Server wurde erfolgreich in den Active Directory-Domänendiensten autorisiert.
54	Eine DHCP-Autorisierung war nicht erfolgreich.

**Tab. 2-4** Häufig auftretende Ereignisse, die in der Überwachungsprotokollierung protokolliert werden

Neben den Aktivitätsprotokollen können Sie auch die Ereignisanzeige verwenden, um sich das DHCP-Ereignisprotokoll anzusehen. Es befindet sich im Knoten *Anwendungs- und Dienstprotokolle/Microsoft/Windows/DHCP-Server/Microsoft-Windows-DHCP-Server/Betriebsbereit* (siehe Abb. 2-24).

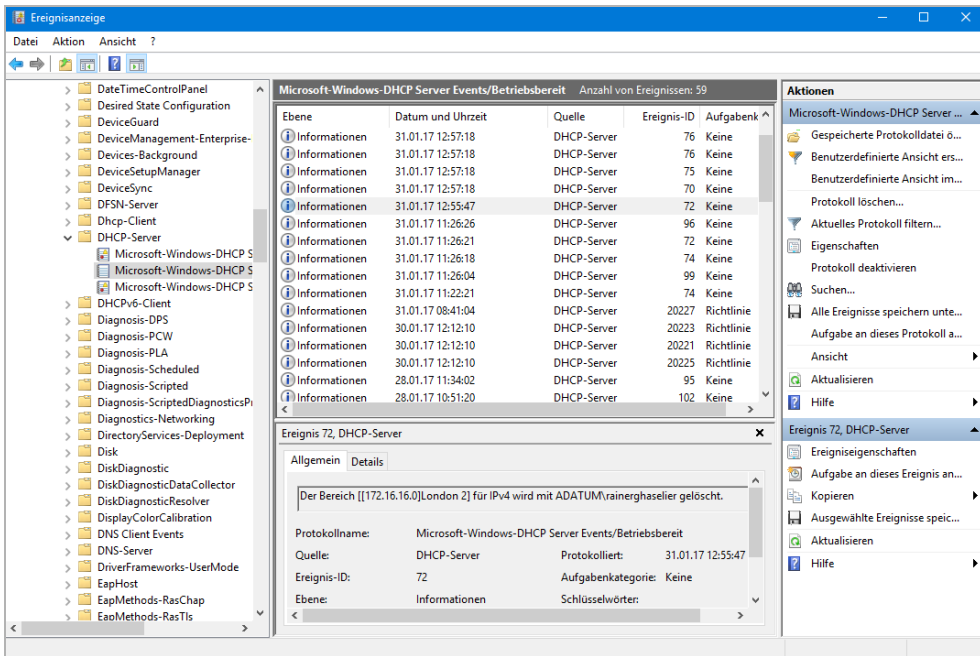


Abb. 2-24 DHCP-Ereignisse in der Ereignisanzeige

### **WEITERE INFORMATIONEN** DHCP-Überwachungsprotokollierung und -Ereignisprotokollierung

Weitere Informationen zur DHCP-Überwachungsprotokollierung und -Ereignisprotokollierung finden Sie auf der Microsoft TechNet-Website unter:

[https://technet.microsoft.com/library/dd759178\(v=ws.11\).aspx](https://technet.microsoft.com/library/dd759178(v=ws.11).aspx)

## BEFEHLSZEILENWERKZEUGE

Sie können das Befehlszeilenwerkzeug IPConfig.exe verwenden, um clientbezogene DHCP-Probleme zu diagnostizieren und zu lösen. Beispiele sehen Sie in Tabelle 2–5.

Befehl	Verwendung
ipconfig /all	<ul style="list-style-type: none"><li>■ Zeigt die vollständige IP-Konfiguration an.</li><li>■ Verwenden Sie den Befehl, um die aktuelle IP-Konfiguration zu überprüfen. An den angezeigten Informationen können Sie erkennen, ob die Client-Konfiguration von einem DHCP-Server zugewiesen wurde und, wenn ja, von welchem. Außerdem wird die Leasedauer angezeigt.</li></ul>
ipconfig /release	<ul style="list-style-type: none"><li>■ Gibt die aktuelle IP-Konfiguration frei.</li><li>■ Nachdem Sie eine IP-Konfiguration freigegeben haben, können Sie eine neue Lease anfordern und dann Tools für die Analyse des Netzwerkverkehrs, wie beispielsweise Microsoft Message Analyzer, verwenden, um sich den Vorgang anzusehen. Gleichzeitig können Sie sich in der DHCP-Konsole im betreffenden DHCP-Bereich den Knoten <i>Adressleases</i> ansehen.</li></ul>
ipconfig /renew	<ul style="list-style-type: none"><li>■ Erneuert die aktuell geleaste IP-Konfiguration.</li><li>■ Erlaubt Ihnen, den Erneuerungsvorgang einer Adresslease zu testen.</li></ul>

**Tab. 2–5** IPConfig.exe-Befehle, die bei der Fehlersuche bei DHCP helfen können

Die Ausgabe von `ipconfig /all` sehen Sie in Abbildung 2–25. In diesem Beispiel können Sie erkennen, dass der Client eine IP-Konfiguration mit den folgenden DHCP-Charakteristika erhalten hat:

- DHCP aktiviert ist Ja.
- Der DHCP-Server ist 172.16.0.10.
- Die Lease läuft ab am 31. Januar um 21:40.

Ein gebräuchliches Verfahren, um mit IPConfig.exe DHCP-Probleme zu untersuchen, besteht darin, eine DHCP-Lease anzufordern und wiederholt die Adresslease freizugeben und zu erneuern, während man in der DHCP-Konsole die geleaste Adressen untersucht. Wenn Sie hierbei gleichzeitig Microsoft Message Analyzer einsetzen, können Sie untersuchen, was auf dem physischen Netzwerk passiert, während Clients mit einem DHCP-Server kommunizieren.

```
Administrator: Eingabeaufforderung
windows-IP-Konfiguration

Hostname . . . . . : LON-SVR2
Primäres DNS-Suffix . . . . . : adatum.com
Knotentyp . . . . . : Hybrid
IP-Routing aktiviert . . . . . : Nein
WINS-Proxy aktiviert . . . . . : Nein
DNS-Suffixsuchliste . . . . . : adatum.com
                                local

Ethernet-Adapter Ethernet:

Verbindungsspezifisches DNS-Suffix: local
Beschreibung. . . . . : Intel(R) 82574L Gigabit Network Connection
Physische Adresse . . . . . : 00-1C-42-D3-76-EB
DHCP aktiviert. . . . . : Ja
Autokonfiguration aktiviert . . . : Ja
Verbindungslokale IPv6-Adresse . . : fe80::7cb9:3474:5b22:8643%7(Bevorzugt)
IPv4-Adresse . . . . . : 172.16.0.160(Bevorzugt)
Subnetzmaske . . . . . : 255.255.255.0
Lease erhalten. . . . . : 31. Januar 2017 20:40:53
Lease läuft ab. . . . . : 31. Januar 2017 21:40:52
Standardgateway . . . . . : 172.16.0.1
DHCP-Server . . . . . : 172.16.0.10
DHCPv6-IAID . . . . . : 50338882
DHCPv6-Client-DUID. . . . . : 00-01-00-01-20-0B-A1-02-00-1C-42-D3-76-EB
DNS-Server . . . . . : 172.16.0.10
NetBIOS über TCP/IP . . . . . : Aktiviert
```

Abb. 2–25 Die Ausgabe von `ipconfig.exe /all`

### MICROSOFT MESSAGE ANALYZER

Mit Microsoft Message Analyzer können Sie die Nachrichten untersuchen, die zwischen vernetzten Geräten ausgetauscht werden. Hierzu gehört auch die Kommunikation zwischen einem DHCP-Server und einem DHCP-Client. So können Sie überprüfen, ob der Nachrichtenverkehr wie erwartet ist. Dies ist insbesondere dann nützlich, wenn Sie komplexere DHCP-Infrastrukturen implementieren, die beispielsweise einen DHCP-Relay-Agent oder DHCP-Failover nutzen. Nachdem Sie dieses Werkzeug heruntergeladen und installiert haben, können Sie die Netzwerkpakete auf den lokalen Netzwerkschnittstellen, mit denen Ihr Computer verbunden ist, untersuchen.

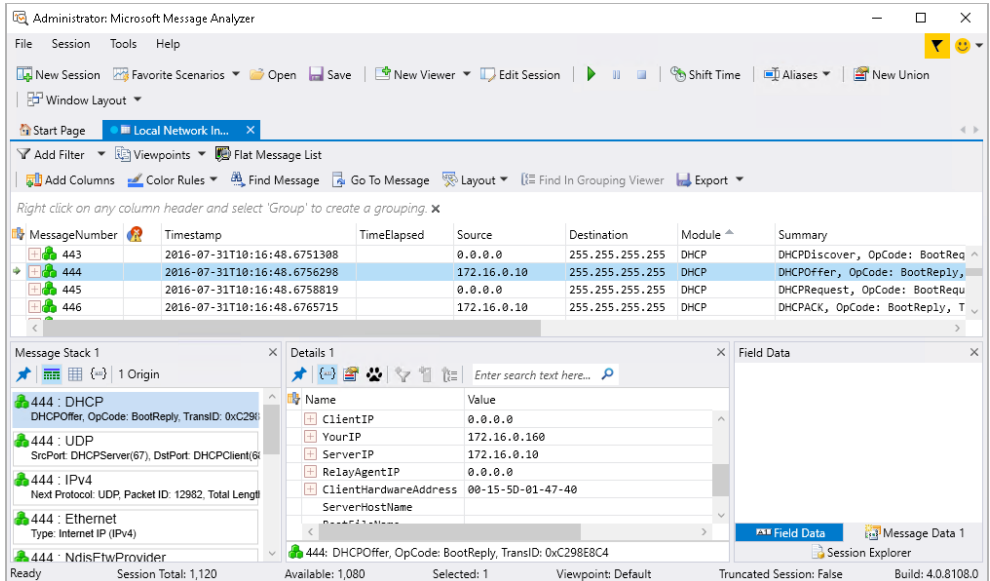
**HINWEIS**

Sie können Microsoft Message Analyzer von der Microsoft-Website herunterladen:

<https://www.microsoft.com/download/details.aspx?id=44226>

Nachdem Sie Microsoft Message Analyzer gestartet haben, können Sie eine lokale Ablaufverfolgung starten. Klicken Sie dazu auf der Startseite auf *Start Local Trace*. Der Analyzer beginnt auf den verbundenen Netzwerkschnittstellen mit dem Sammeln von Netzwerknachrichten. Sie können diese Nachrichten daraufhin analysieren, ob bei DHCP Probleme zu erkennen sind.

Um mit Microsoft Message Analyzer DHCP-Clientprobleme zu suchen, starten Sie die Ablaufverfolgung auf dem lokalen Computer und versuchen Sie dann, eine DHCP-Adresse anzufordern und zu erneuern. Sie können sich dann, wie in Abbildung 2–26 gezeigt, die aufgezeichneten Nachrichten ansehen.



**Abb. 2-26** Microsoft Message Analyzer

Wie Sie sehen können, wurden die bei der Anforderung einer DHCP-Lease zu erwartende Nachrichten aufgezeichnet.

### **HINWEIS**

Eine Beschreibung der Interaktion zwischen Client und Server finden Sie weiter vorne in diesem Kapitel im Abschnitt »DHCP im Überblick« (S. 61).

Aus der Ablaufverfolgung wurden vier Nachrichten isoliert. Diese sind mit 443 bis 446 nummeriert und entsprechen den Nachrichten DHCPDiscover, DHCPOffer, DHCPRequest sowie DHCPACK. Die DHCPOffer-Nachricht ist markiert; im Detailbereich können Sie sehen, dass der Client die IP-Adresse 0.0.0.0 besitzt. Dies ist normalerweise der Fall, wenn ein Client eine Adresslease anfragt, da er zu diesem Zeitpunkt noch keine gültige IPv4-Adresse besitzt. In der Liste mit den Nachrichten können Sie sehen, dass in der Spalte *Destination* die Adresse 255.255.255.255 verwendet wird. Dies ist eine IPv4-Broadcast-Adresse und auch dieses Verhalten ist zu erwarten, wenn ein Client erstmalig eine Lease anfordert.

Indem Sie sich die Ablaufverfolgung eines funktionierten DHCP-Dialogs ansehen, können Sie Inkonsistenzen erkennen, wenn der Nachrichtenverkehr nicht wie erwartet verläuft.

### **WEITERE INFORMATIONEN** Microsoft Message Analyzer-Bedienungsanleitung

Weitere Informationen über den Einsatz von Microsoft Message Analyzer finden Sie auf der Microsoft TechNet-Website unter:

<https://technet.microsoft.com/library/jj649776.aspx>

## Kapitelzusammenfassung

- DHCP vereinfacht die Administration des IPv4- und IPv6-Adressraums in Ihrem Unternehmen.
- In einer Umgebung mit Active Directory-Domänendiensten müssen Sie Ihre DHCP-Server in Active Directory autorisieren.
- Der DHCP-Bereich ist die zentrale Konfigurationseinheit in DHCP.
- Mit Bereichsgruppierungen können Sie Probleme lösen, die sich aus Mehrfachnetzwerk-Konfigurationen ergeben.
- Multicastbereiche unterstützen Anwendungen, die zur Kommunikation Multicastdatenverkehr verwenden.
- Sie können DHCP-Optionen auf Serverebene, Bereichsebene, Klassenebene und auf der Ebene einer Reservierung festlegen.
- DHCP-Richtlinien erlauben die Zuweisung von DHCP-Optionen anhand von konfigurierbaren Bedingungen.
- Um eine hochverfügbare DHCP-Infrastruktur bereitzustellen, können Sie Windows-Server-Clustering, geteilte DHCP-Bereiche oder DHCP-Failover verwenden.
- Bei der DHCP-Bereichsaufteilung wird der verfügbare Adresspool eines DHCP-Bereichs zwischen zwei Servern aufgeteilt. Bei DHCP-Failover wird der gesamte Bereich (oder auch mehrere Bereiche) zwischen den konfigurierten DHCP-Failoverpartnern repliziert.
- Die DHCP-Datenbank wird automatisch alle 60 Minuten gesichert.
- DHCP-Namensschutz hilft dabei, die vom DHCP-Dienst in DNS registrierten Namen zu schützen.
- Die Verwendung von Werkzeugen wie IPConfig.exe in Kombination mit Microsoft Message Analyzer ist ein wirksamer Weg, um die korrekte Funktionsweise der DHCP-Dienste zu überprüfen.

### **Gedankenexperiment**

In diesem Gedankenexperiment können Sie Ihre Fähigkeiten und Ihr Wissen über die in diesem Kapitel behandelten Themen testen. Die Antworten zu diesem Gedankenexperiment finden Sie im nächsten Abschnitt.

Sie arbeiten im Support von A.Datum. Beantworten Sie als Berater für A.Datum die folgenden Fragen über die Implementierung von DHCP in diesem Unternehmen:

1. Das Netzwerk von A.Datum besteht aus mehreren Subnetzen. Sie wollen nicht in jedem physischen Subnetz einen DHCP-Server bereitstellen, aber dennoch gewährleisten, dass alle Clientcomputer von einem DHCP-Server eine IP-Konfiguration erhalten können. Was müssen Sie tun, um dies zu erreichen?
2. Sie wollen die DHCP-Serverrolle bereitstellen und hierfür nicht die Konsole *Server-Manager* verwenden. Wie gehen Sie vor?

→

3. Sie wollen einen Bereich für ein IPv4-Subnetz mit der Adresse 172.16.16.0/255.255.240.0 erstellen. Wie viele Subnetzbits müssen Sie konfigurieren, wenn Sie diesen Bereich erstellen?
4. Sie wollen ein nicht von Microsoft stammendes Paket zur Softwarebereitstellung verwenden, um damit auf den Clientcomputern Anwendungen bereitzustellen. Die Anwendung verwendet Multicast-IP. Wie kann DHCP Sie in diesem Szenario unterstützen?
5. Sie wollen in der Lage sein, den Benutzern von Windows-Tablets eine kürzere Lease-dauer zuzuweisen. Wie erreichen Sie dies?
6. Ihr Manager bittet Sie, zu untersuchen, wie für eine Zweigniederlassung die fortlaufende Verfügbarkeit von DHCP gewährleistet werden kann. Derzeit erhalten alle Netzwerkclients ihre IP-Konfiguration von einem DHCP-Server, der sich in der regionalen Zentrale in London befindet. Immer dann, wenn dort Netzwerkverbindungsprobleme auftauchen, erhalten die Clients in der Zweigniederlassung keine IP-Konfiguration mehr. Mit welchen möglichen Lösungen können Sie diesem Problem begegnen? Welche würden Sie Ihrem Manager empfehlen?
7. Aufgrund eines vor Kurzem aufgetretenen Ausfalls eines DHCP-Servers konnten die Anwender in London auf ihren Laptop-Computern keine IP-Konfiguration mehr erhalten. Ihr Manager möchte, dass Sie gewährleisten, dass dies nie mehr passiert. Was können Sie tun?
8. Clientcomputer in einem Teil des Londoner Firmensitzes erhalten keine IP-Konfiguration. Diese Computer befinden sich in einem eigenen Gebäude auf der gegenüberliegenden Straßenseite der Londoner Zentrale. Sie untersuchen dieses Gebäude und stellen fest, dass es dort keinen lokalen DHCP-Server gibt. Was würden Sie als Nächstes tun, um mit der Behebung des Problems zu beginnen?

### **Antworten zum Gedankenexperiment**

In diesem Abschnitt finden Sie die Lösungen für das Gedankenexperiment. In jeder Antwort wird begründet, warum dies die richtige Antwort ist.

1. Falls Ihre Router BOOTP-Weiterleitungen unterstützen, wie sie in RFC 1452 definiert sind, müssen Sie nichts tun, da die DHCP-Nachrichten von den Routern zwischen den Subnetzen weitergeleitet werden. Falls Ihre Router dieses Feature nicht unterstützen, können Sie die Konsole *Routing und RAS* verwenden, um auf dem Windows Server 2016-Computer einen DHCP-Relay-Agent bereitzustellen.
2. Sie können den Windows PowerShell-Befehl `Add-WindowsFeature DHCP -IncludeManagementTools` verwenden, um die DHCP-Serverrolle und die erforderlichen Verwaltungstools bereitzustellen.
3. Für die Subnetzmaske 255.255.240.0 müssen Sie beim Erstellen des Bereichs 20 Bits verwenden.



4. DHCP erlaubt das Erstellen von Multicastbereichen, um Anwendungen und Clients zu unterstützen, die Multicastnachrichten verwenden.
5. Sie können in DHCP einen Bereich erstellen und dann eine Benutzerklasse für Tablets erstellen. Verwenden Sie das Werkzeug IPConfig.exe, um den Tablets diese Benutzerklasse zuzuweisen. Erstellen Sie abschließend eine DHCP-Richtlinie, die den Geräten mit der Benutzerklasse Tablets eine andere Leasedauer zuweist.
6. Es gibt hier verschiedene Ansätze. Eine Lösung besteht darin, allen Clients in der Zweigniederlassung manuell IP-Adressen zuzuweisen. Dies macht einen DHCP-Server zwar überflüssig, würde aber gleichzeitig die Verwaltung des IP-Adressraums im Unternehmen verkomplizieren. Beim Einsatz von DHCP wäre eine mögliche Lösung, in der Zweigniederlassung einen eigenen DHCP-Server zu platzieren und ihn mit dem für die Zweigniederlassung erforderlichen Bereich zu konfigurieren. Dies ist vermutlich die einfachste Lösung, die auch keine Failover-Konfiguration erfordert. Falls Sie es bevorzugen, dass die IPv4-Adressen aus dem Londoner Büro stammen, ist auch die Verwendung geteilter DHCP-Bereiche machbar. Legen Sie für den DHCP-Server in der Zweigniederlassung einen höheren Verzögerungswert für das DHCP-Angebot fest, damit er nur dann Adressen zuteilt, wenn der DHCP-Server in London nicht reagiert. Sie müssen darauf achten, diesen Wert korrekt einzustellen, da die Zuteilung einer IP-Konfiguration über ein Weitverkehrsnetz (Wide Area Network, WAN) langsamer ist als bei einer lokalen Netzwerkanbindung.
7. Dieses Szenario lässt sich wohl am besten mit DHCP-Failover lösen. Konfigurieren Sie den oder die DHCP-Bereiche für die Londoner Büros auf einem DHCP-Server, implementieren Sie dann DHCP-Failover im Modus Lastenausgleich und verteilen Sie den Bereich im Verhältnis 50/50. Hierdurch wird die Performance verbessert und Sie erreichen so eine hohe Verfügbarkeit.
8. Da die Clientcomputer keine IP-Konfiguration von den Servern erhalten, die in der Zentrale stehen, sollte die Verbindung zur Zentrale untersucht werden. Überprüfen Sie, ob irgendwelche Router offline sind. Vergewissern Sie sich, dass ein DHCP-Relay-Agent verwendet wird und dass er online sowie korrekt konfiguriert ist. Schließlich prüfen Sie noch, ob der normalerweise von den Clients verwendete DHCP-Server online ist. Schauen Sie auch nach, ob der Bereich, aus dem die Clients ihre Konfiguration beziehen, aktiviert ist.