

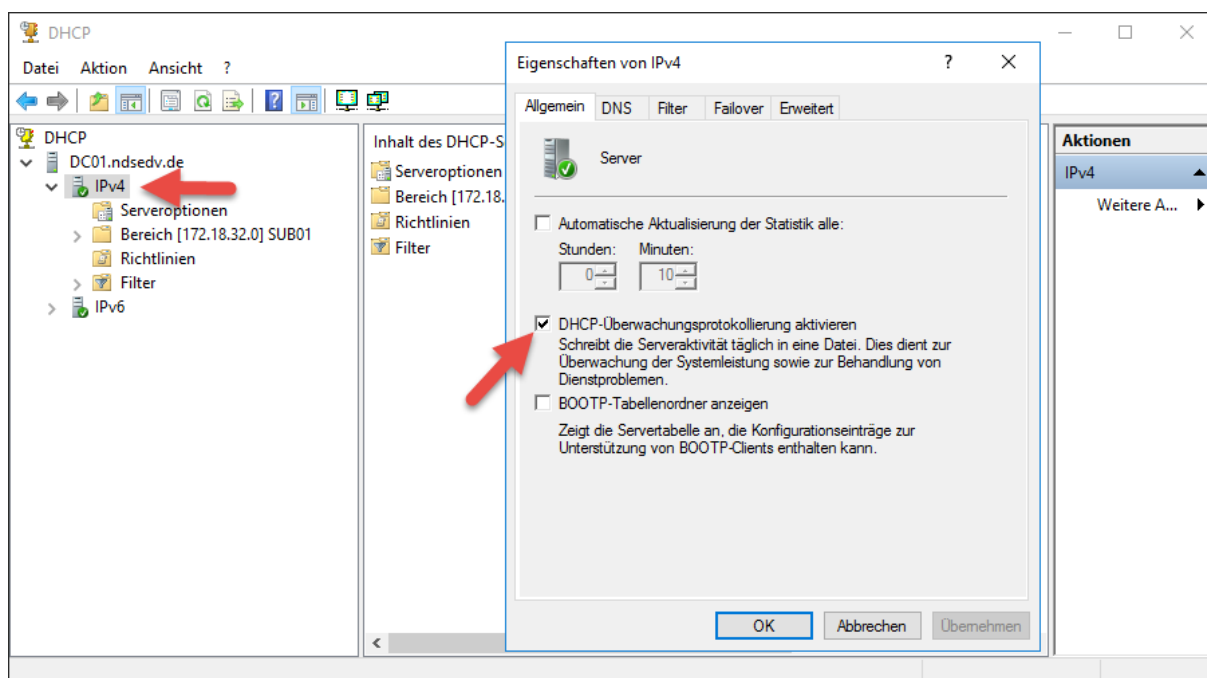


## DHCP Auditing und DHCP Service stoppt

DHCP steht für Dynamic Host Configuration Protocol. Der DHCP Dienst gibt in einem Netzwerk automatisch IP-Adressen an die Arbeitsstationen aus. Der zentrale Zweig von DHCP ist die Integration in DNS (Domain Name System). Das Ziel der Integration ist die automatische Registrierung von Hostnamen und IP-Adressen bei DNS-Servern durch den DHCP-Server.

Der Client sendet ein DHCP-Discover (Broadcast) ins Netzwerk und erwartet von einem vorhandenen DHCP-Server ein DHCP-Offer (eine IP Adresse angeboten). Der Client nimmt die ihm angebotene IP Adresse (DHCP-Offer) an und sendet dem DHCP-Server ein DHCP-Request (ich nehme dein Angebot an). Der DHCP-Server bestätigt mit einem DHCP-Acknowledge (damit sind wir im Geschäft). Wird kein DHCP-Server erreicht, bekommt der Client über APIPA (Automatic Private IP Addressing) eine vorläufige IP aus dem Bereich 169.254.0.1 – 255.254.

Zur Nachverfolgung solcher Aktionen ist es wichtig, dass die Auditing-Funktion aktiviert wird.



### Auditing aktivieren maximale Logging Größe und Pfad bestimmen:

```
Set-DhcpServerAuditLog -ComputerName "DC01.ndsedv.de" -Enable $True -Path "C:\Logs\DHCP\Auditing\dhcpauditlog\" -MaxMBFileSize 100
```

### Per Registry nur das Auditing aktivieren

```
reg add HKLM\System\CurrentControlSet\Services\DhcpServer\Parameters /v ActivityLogFlag /t REG_DWORD /d 1
```

### Maximale Logging Größe aller zu erstellenden Audit Logs anpassen:

```
Set-DhcpServerAuditLog -MaxMBFileSize 250  
Set-DhcpServerAuditLog -MaxMBFileSize 4096
```

### Dateipfade für die Logdateien anpassen:

```
netsh dhcp server set databasepath D:\Logs\DHCP  
netsh dhcp server set auditlog D:\Logs\DHCP\Auditing\dhcpauditlog
```



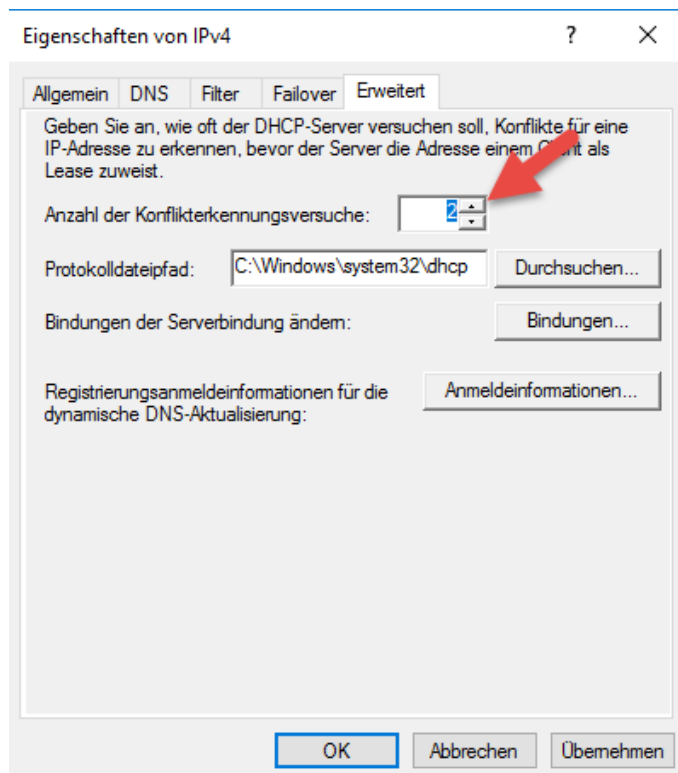
## DHCP Auditing und DHCP Service stoppt

### Hinweis:

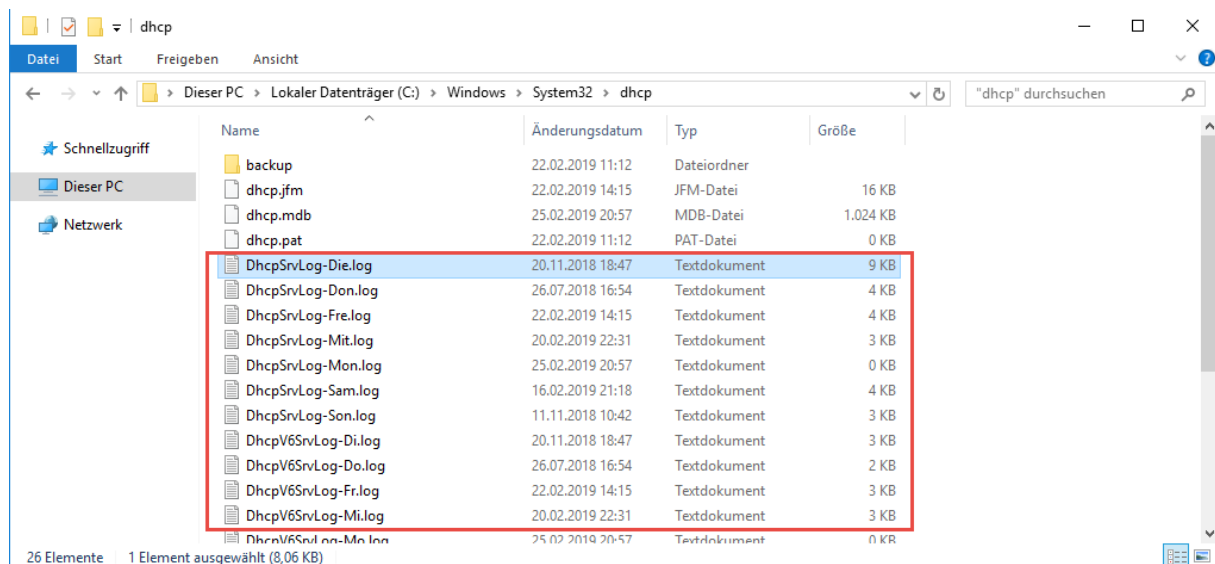
Bei dem Parameter MaxMBFileSize handelt es sich um die addierte Größe aller erstellen Log-Dateien. Wenn die maximale Größe aller addierten Log-Dateien den MaxMBFileSize übersteigt, wird das Logging eingestellt und es werden keine IP-Adressen mehr ausgegeben.

### DHCP Konflikterkennungsversuche aktivieren:

Wenn die Erkennung aktiviert ist, startet der DHCP Server einen Ping-Prozess, um die verfügbaren IP-Bereiche zu ermitteln. Erst danach wird der DHCP Lease einem Client angeboten. Der Wert sollte auf 2 stehen um die Netzwerklast nicht zu erhöhen.



Sobald das Auditing aktiviert ist, wird für jeden Tag eine neue Log-Datei angelegt:





## **DHCP Auditing und DHCP Service stoppt**

### **Ereignis-ID Bedeutung**

- 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.
- 16 Eine Lease wurde gelöscht.
- 17 Eine Lease war abgelaufen, und die DNS-Einträge für eine abgelaufene Lease wurden nicht gelöscht.
- 18 Eine Lease war abgelaufen, und die DNS-Einträge wurden gelöscht.
- 20 Eine BOOTP-Adresse wurde einem Client geleast.
- 21 Eine dynamische BOOTP-Adresse wurde einem Client geleast.
- 22 Eine BOOTP-Anforderung konnte nicht erfüllt werden, da der Adresspool für BOOTP des Bereichs erschöpft war.
- 23 Eine BOOTP-IP-Adresse wurde gelöscht, nachdem sichergestellt wurde, dass sie nicht verwendet wird.
- 24 Der Bereinigungsverfahren für die IP-Adresse wurde gestartet.
- 25 Statistik der IP-Adressenbereinigung.
- 30 DNS-Updateanforderung an den benannten DNS-Server.
- 31 Fehler beim DNS-Update.
- 32 Das DNS-Update war erfolgreich.
- 33 Das Paket wurde aufgrund der NAP-Richtlinie verworfen.
- 34 Fehler bei der DNS-Updateanforderung: Die maximale Anzahl von DNS-Updateanforderungen in der Warteschlange wurde überschritten.
- 35 Fehler bei der DNS-Updateanforderung.
- 36 Das Paket wurde verworfen, da sich der Server in der Failoverstandbyrolle befindet oder der Hash der Client-ID abweicht.
- 50+ Codes über 50 werden für Informationen über die Erkennung nicht autorisierter Server verwendet.



## DHCP Auditing und DHCP Service stoppt

Jeder Eintrag in dem Log steht in einer separaten Zeile:

Die Einträge enthalten Informationen zu

- ID = Event Code
- Date = Datum des Log Eintrags
- Time = Zeit des Log Eintrags
- Description = Beschreibung des Events
- IP Address = IP Adresse des DHCP Clients
- Host Name = Name des DHCP Servers
- Mac Address = MAC Adresse des Netzwerkadapters

```
DhcpSrvLog-Die.log - Editor
Datei Bearbeiten Format Ansicht ?
ID, Datum, Zeit, Beschreibung, IP-Adresse, Hostname, MAC-Adresse, Benutzername, Transaktions-ID, QErgebnis, Probezeit, Korrelations-ID, DHCID, Her.
00,11/20/18,17:18:06,Gestartet,,,,,0,6,,,,,,0
55,11/20/18,17:18:25,Autorisiert (Dienst gestartet),,ndsedv.de,,,0,6,,,,,,0
01,11/20/18,17:34:28,Angehalten,,,,,0,6,,,,,,0
00,11/20/18,17:35:27,Gestartet,,,,,0,6,,,,,,0
55,11/20/18,17:35:35,Autorisiert (Dienst gestartet),,ndsedv.de,,,0,6,,,,,,0
01,11/20/18,17:36:18,Angehalten,,,,,0,6,,,,,,0
00,11/20/18,17:47:40,Gestartet,,,,,0,6,,,,,,0
55,11/20/18,17:47:55,Autorisiert (Dienst gestartet),,ndsedv.de,,,0,6,,,,,,0
01,11/20/18,17:49:41,Angehalten,,,,,0,6,,,,,,0
00,11/20/18,17:53:07,Gestartet,,,,,0,6,,,,,,0
55,11/20/18,17:53:27,Autorisiert (Dienst gestartet),,ndsedv.de,,,0,6,,,,,,0
30,11/20/18,17:53:53,DNS-Aktualisierungsanforderung,172.18.32.101,DESKTOP-G4JPD7G.ndsedv.de,,,0,6,,,,,,0
10,11/20/18,17:53:53,Zuweisen,172.18.32.101,DESKTOP-G4JPD7G.ndsedv.de,000C2917B871,,2904633541,0,,,0x4D53465420352E30,MSFT 5.0,,,0
32,11/20/18,17:53:53,DNS-Aktualisierung erfolgreich,172.18.32.101,DESKTOP-G4JPD7G.ndsedv.de,,,0,6,,,,,,0
30,11/20/18,17:58:58,DNS-Aktualisierungsanforderung,172.18.32.101,DESKTOP-G4JPD7G.ndsedv.de,,,0,6,,,,,,0
11,11/20/18,17:58:58,Erneuern,172.18.32.101,DESKTOP-G4JPD7G.ndsedv.de,000C2917B871,,3271380025,0,,,0x4D53465420352E30,MSFT 5.0,,,0
32,11/20/18,17:58:58,DNS-Aktualisierung erfolgreich,172.18.32.101,DESKTOP-G4JPD7G.ndsedv.de,,,0,6,,,,,,0
30,11/20/18,18:03:42,DNS-Aktualisierungsanforderung,172.18.32.101,DESKTOP-G4JPD7G.ndsedv.de,,,0,6,,,,,,0
```

Nach einer Woche werden die gespeicherten Logdateien wieder überschrieben.

## Abfragen wie viele DHCP Servers es gibt:

`netsh dhcp show server`

```
Administrator: Eingabeaufforderung
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. Alle Rechte vorbehalten.

C:\Windows\system32>netsh dhcp show server

2 Server im Verzeichnisdienst gefunden:

    Server [dc01.ndsedv.de] Adresse [255.0.0.1] Verzeichnisdienststandort: cn=dc01.ndsedv.de
    Server [dc01.ndsedv.de] Adresse [172.18.32.31] Verzeichnisdienststandort: cn=dc01.ndsedv.de

Der Befehl wurde erfolgreich ausgeführt.

C:\Windows\system32>
```



## DHCP Auditing und DHCP Service stoppt

### DHCP Server autorisierend hinzufügen:

```
netsh dhcp add server DC02 172.18.32.32
```

```
Administrator: Eingabeaufforderung
C:\Windows\system32>netsh dhcp add server DC02 172.18.32.32
Server DC02, 172.18.32.32 wird hinzugefügt.
Der Befehl wurde erfolgreich ausgeführt.
C:\Windows\system32>
```

```
Administrator: Eingabeaufforderung
Der Befehl wurde erfolgreich ausgeführt.
C:\Windows\system32>netsh dhcp show server
3 Server im Verzeichnisdienst gefunden:
    Server [dc01.ndsedv.de] Adresse [255.0.0.1] Verzeichnisdienststandort: cn=dc01.ndsedv.de
    Server [dc01.ndsedv.de] Adresse [172.18.32.31] Verzeichnisdienststandort: cn=dc01.ndsedv.de
    Server [dc02] Adresse [172.18.32.32] Verzeichnisdienststandort: cn=dc02
Der Befehl wurde erfolgreich ausgeführt.
C:\Windows\system32>
```

### DHCP Server Autorisierung aufheben:

```
netsh dhcp delete server DC02 172.18.32.32
```

```
Administrator: Eingabeaufforderung
C:\Windows\system32>netsh dhcp delete server DC02 172.18.32.32
Server wird mit DC02, 172.18.32.32 gelöscht.
Der Befehl wurde erfolgreich ausgeführt.
C:\Windows\system32>
```

### Hinweis:

Sollte die Aufhebung der Autorisierung über die GUI oder CMD nicht zum Erfolg führen, so können die alten DHCP-Server über die MMC ADSIEdit gelöscht werden.



## DHCP Auditing und DHCP Service stoppt

Aufhebung der Autorisierung über die GUI

The screenshot shows the DHCP console window. On the left, a tree view shows 'DC01.ndsedv.de' selected. A dialog box titled 'Autorisierte Server verwalten' is open in the center. It contains a table with two columns: 'Name' and 'IP-Adresse'. The table lists two entries: 'dc01.ndsedv.de' with IP '172.18.32.31' and 'dc01.ndsedv.de' with IP '255.0.0.1'. A red arrow points to the 'Aufheben' button next to the second entry. Below the table, there is a text box with instructions: 'Wählen Sie einen Computer aus, und klicken Sie dann auf "OK", um einen Computer der DHCP-Konsole hinzuzufügen.' At the bottom of the dialog are 'OK' and 'Schließen' buttons.

DHCP Server - Ansicht über ADSIEdit:

The screenshot shows the ADSI-Editor window. On the left, a tree view shows the directory structure. A red arrow points to the 'CN=NetServices' folder. In the center, a table lists objects: 'CN=dc01.ndsedv.de' (class dHCPClass) and 'CN=DhcpRoot' (class dHCPClass). On the right, a dialog box titled 'Eigenschaften von CN=dc01.ndsedv.de' is open. It shows a list of attributes and their values. A red arrow points to the 'CN=NetServices' folder in the left tree view.

Attribut	Wert
cn	dc01.ndsedv.de
dhcpFlags	0
dhcpIdentification	DHCP Server object
dhcpServers	{255.0.0.1}{cn=dc01.ndsedv.de}{0x00000000}
dhcpType	1
dhcpUniqueKey	0
distinguishedName	CN=dc01.ndsedv.de,CN=NetServices,CN=...
dSCorePropagationD...	0x0 = ( )
instanceType	0x4 = ( WRITE )
name	dc01.ndsedv.de
objectCategory	CN=DHCP-Class,CN=Schema,CN=Configura...
objectClass	top; dHCPClass
objectGUID	1d0c865f-0698-4a4f-ba82-31ee87210658
realPropertyMetaData	AttID Ver Loc USN Org DSA



## DHCP Auditing und DHCP Service stoppt

Eingesetzte Softwareprodukte wie AD Audit von Manage Engine oder Arcsight, benötigen diese Logs für das Compliance Management.

Ebene	Datum und Uhrzeit	Quelle	Ereignis-ID	Aufgabenkategorie
Informationen	10.09.2017 18:56:40	DHCP-Server	107	Keine
Informationen	10.09.2017 18:56:40	DHCP-Server	107	Keine
Informationen	10.09.2017 18:56:40	DHCP-Server	107	Keine
Informationen	21.11.2016 12:11:57	DHCP-Server	108	Keine
Informationen	21.11.2016 12:11:57	DHCP-Server	106	Keine
Informationen	21.11.2016 12:11:57	DHCP-Server	107	Keine

**Ereignis 107, DHCP-Server**

Die Reservierung [(172.18.32.107)] für IPv4 wird unter dem Bereich [(172.18.32.0)SUB01] von NDSedv.NDS gelöscht.

Protokollname: Microsoft-Windows-DHCP Server Events/Betriebsbereit  
Quelle: DHCP-Server  
Ereignis-ID: 107  
Benutzer: NDSedv.NDS  
Vorgangscodename: Info  
Weitere Informationen: [Onlinehilfe](#)

### DHCP Test:

<https://files.thecybershadow.net/dhcptest/>  
<https://github.com/CyberShadow/dhcptest>

```
Administrator: Windows PowerShell
PS C:\Temp> .\dhcptest-0.7-win64.exe
dhcptest v0.7 - Created by Vladimir Panteleev
https://github.com/CyberShadow/dhcptest
Run with --help for a list of command-line options.

Listening for DHCP replies on port 68.
Type "d" to broadcast a DHCP discover packet, or "help" for details.
d
Sending packet:
op=BOOTREQUEST chaddr=04:CD:D5:8C:81:22 hops=0 xid=08052C87 secs=0 flags=8000
ciaddr=0.0.0.0 yiaddr=0.0.0.0 siaddr=0.0.0.0 giaddr=0.0.0.0 sname= file=
1 options:
 53 (DHCP Message Type): discover
Received packet from 10.42.150.105:67:
op=BOOTREPLY chaddr=04:CD:D5:8C:81:22 hops=0 xid=08052C87 secs=0 flags=0000
ciaddr=0.0.0.0 yiaddr=10.42.150.210 siaddr=10.42.150.105 giaddr=0.0.0.0 sname= file=
6 options:
 53 (DHCP Message Type): offer
 1 (Subnet Mask): 255.255.255.0
 58 (Renewal (T1) Time Value): 1800 (30 minutes)
 59 (Rebinding (T2) Time Value): 3150 (52 minutes and 30 secs)
 51 (IP Address Lease Time): 3600 (1 hour)
 54 (Server Identifier): 10.42.150.105

Enter a command.
_
```

### Weitere Ereignis-ID Bedeutungen ab ID 50:

50 - The DHCP server could not locate the necessary domain.

51 - Authorization was successful.

52 - The server was recently upgraded to Windows Server 2003 Standard Edition. During the upgrade process, the unauthorized DHCP server detection mechanism, which is used to determine whether or not the DHCP server has been authorized in the active directory, was disabled.



## **DHCP Auditing und DHCP Service stoppt**

53 - The Active Directory was inaccessible at the time that the DHCP services started. Because of this, cached information was used to authorize the DHCP services to start.

54 - This is an authorization failure code. When this event occurs, it is because the DHCP server does not authorized within the active directory. An event code and 54 should be followed by an event ID showing that the DHCP services have stopped.

55 - The DHCP services were authorized to start.

56 - Event number 56 was the event that showed up in our sample log file. This event indicates that the DHCP service was not authorized to start, and was consequently shut down. As you probably know, you must authorize a DHCP server in active directory prior to starting the DHCP services.

57 - Another DHCP server already exist within the specified domain.

58 - The DHCP server was unable to locate the necessary domain.

59 - A network connectivity issue prevent the server for determining whether or not it has been authorized.

60 - This error code needs a bit of explaining. The event ID means that no domain controller is Directory Service enabled. This event ID this only encountered in mixed mode environments in which Windows NT domain controllers are present. Because a DHCP server can only be authorized through the Active Directory, the DHCP server must be able to communicate with the Active Directory in order to determine whether it has been authorized or not. Therefore, if the DHCP server is only able to communicate with Windows NT based domain controllers, the log file will reflect an event ID of 60.

61 - This event ID means that another DHCP server that belongs to the same domain was found on the network. This event ID is different from number 57 in that the detected DHCP server does not necessarily have to be authorized. For example, the DHCP services might be running on an old Windows NT server.

62 - Event ID number 62 means that another DHCP server was detected on the network. The difference between event ID number 62 and event ID numbers 61 and 57 is that event ID number 62 is not domain specific. In fact, the DHCP server that is detected does not even have to be a Windows server. This is simply a generic event ID that is produced anytime another DHCP server is detected.

63 - Event ID number 63 is produced when the DHCP server is having trouble with the rogue detection mechanism. This event is generated when the rogue detection mechanism is restarted. Restarting the rogue detection mechanism implies that the server is going to try one more time to determine whether or not it is authorized.

64 - This event ID indicates that there are no DHCP enabled network interfaces. What this means is that none of the server's network interfaces are configured in a way that is acceptable to the DHCP services. Typically this means one of three things. One possibility is that there may not be in network cable plugged into the network adapter in question. A second possibility is that all of the DHCP server's network interfaces might be configured to use dynamic IP addresses. A DHCP server requires at least one static IP address. Finally, the third possibility is that all of the network adapters bound to static IP addresses have been disabled.