Fehlerbehebung beim Dynamic Host Configuration Protocol in Catalyst Switches oder Enterprise Networks

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie die häufigsten Probleme mit dem Dynamic Host Configuration Protocol (DHCP) in einem Cisco Catalyst Switch-Netzwerk beheben.

Voraussetzungen

Anforderungen

Es sind keine besonderen Voraussetzungen erforderlich, um den Inhalt dieses Dokuments nachzuvollziehen.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps von Cisco zu Konventionen).

> **Anmerkung:** Nur registrierte Cisco Kunden haben Zugriff auf interne Fehlerberichte.

Hintergrundinformationen

DHCP stellt einen Mechanismus bereit, über den Computer, die das Transmission Control Protocol/Internet Protocol (TCP/IP) verwenden, Protokollkonfigurationsparameter automatisch über das Netzwerk abrufen können. DHCP ist ein offener Standard, der von der Dynamic Host Configuration-Working Group (DHC-WG) der Internet Engineering Task Force (IETF) entwickelt wurde.

DHCP basiert auf einem Client-Server-Paradigma, bei dem der DHCP-Client, beispielsweise ein Desktop-Computer, einen DHCP-Server für Konfigurationsparameter kontaktiert. Der DHCP-Server wird in der Regel zentral vom Netzwerkadministrator bereitgestellt und betrieben. Da der Server von einem Netzwerkadministrator betrieben wird, können DHCP-Clients zuverlässig und dynamisch mit Parametern konfiguriert werden, die der aktuellen Netzwerkarchitektur entsprechen.

Die meisten Unternehmensnetzwerke bestehen aus mehreren Subnetzen, die in so genannte virtuelle LANs (Virtual LANs) unterteilt sind, in denen Router zwischen den Subnetzen routen. Da Router standardmäßig keine Broadcasts weiterleiten, ist in jedem Subnetz ein DHCP-Server erforderlich, es sei denn, die Router sind für die Weiterleitung der DHCP-Broadcasts mit der DHCP Relay Agent-Funktion konfiguriert.

Schlüsselkonzepte

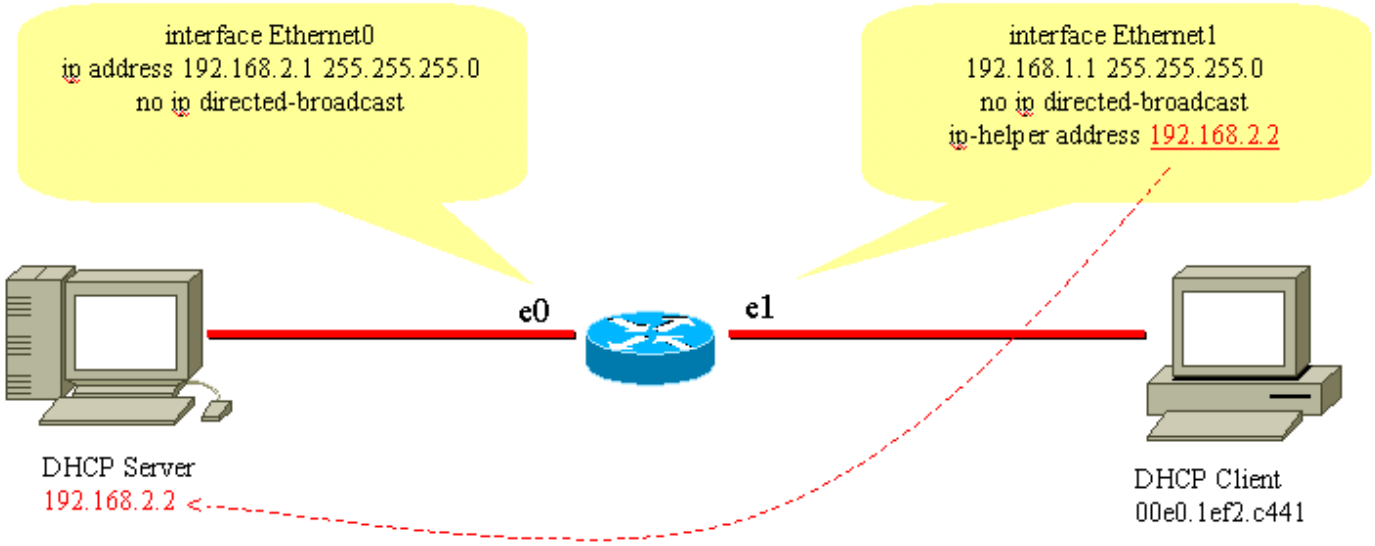
Es folgen einige wichtige DHCP-Konzepte:

- DHCP-Clients haben anfänglich keine konfigurierte IP-Adresse und müssen daher eine Broadcast-Anforderung senden, um eine IP-Adresse von einem DHCP-Server zu erhalten.
- Router leiten standardmäßig keine Broadcasts weiter. DHCP-Broadcast-Anfragen von Clients müssen berücksichtigt werden, wenn sich der DHCP-Server in einer anderen Broadcast-Domäne (Layer-3-L3-Netzwerk) befindet. Dies erfolgt mithilfe eines DHCP Relay Agents.
- Die Implementierung von DHCP Relay auf dem Cisco Router wird über **IP Helper-**Befehle auf Schnittstellenebene bereitgestellt.

Beispielszenarien

Szenario 1: Cisco Router-Routing zwischen DHCP-Client- und Server-Netzwerken

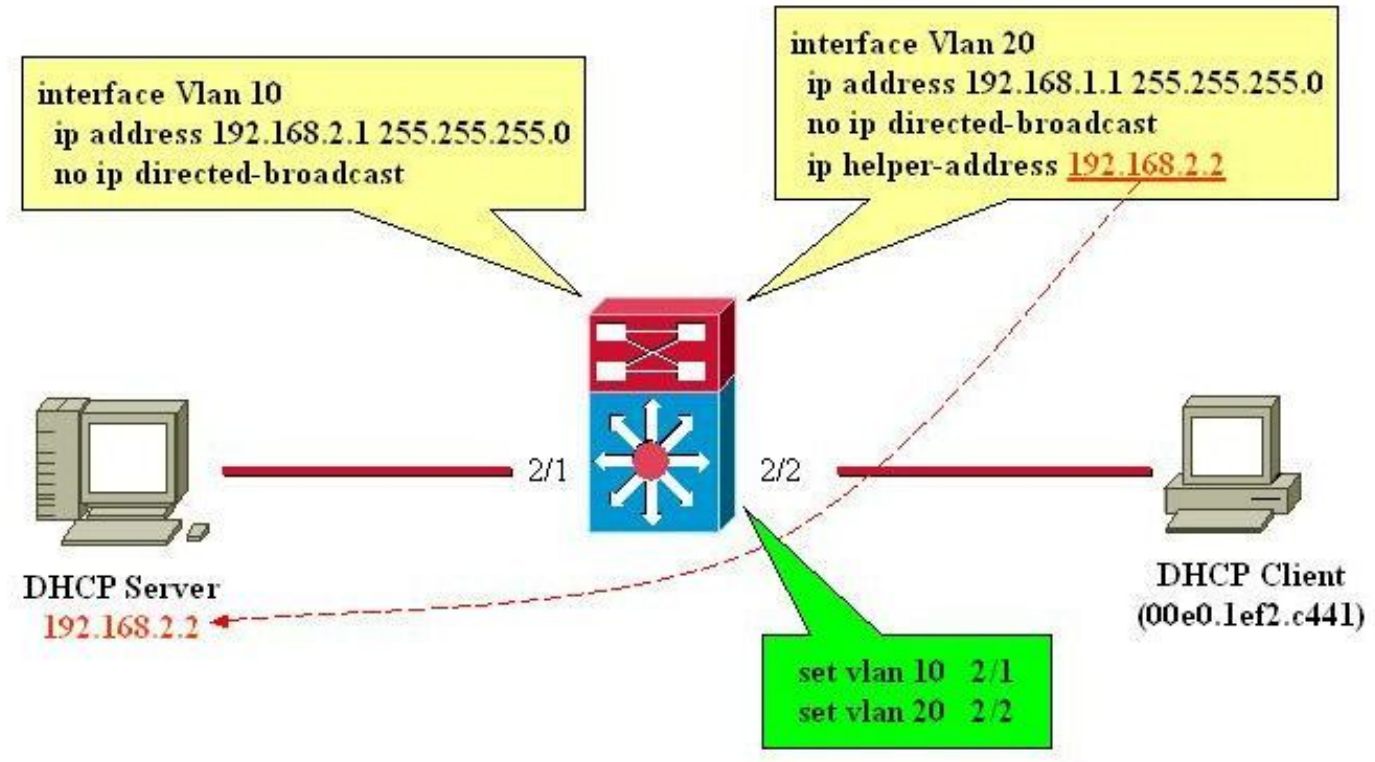
Wie in diesem Diagramm konfiguriert, leitet die Schnittstelle Ethernet1 den Client-Broadcast-DHCPDISCOVER über die Schnittstelle Ethernet1 an 192.168.2.2 weiter. Der DHCP-Server erfüllt die Anforderung über Unicast. In diesem Beispiel ist keine weitere Konfiguration für den Router erforderlich.



Routing zwischen DHCP-Client- und -Servernetzwerken

Szenario 2: Cisco Catalyst Switch mit L3-Modul-Routing zwischen DHCP-Client- und Server-Netzwerken

Wie im Diagramm konfiguriert, leitet die Schnittstelle VLAN20 den Client-Broadcast-DHCPDISCOVER über die Schnittstelle VLAN10 an 192.168.2.2 weiter. Der DHCP-Server erfüllt die Anforderung über Unicast. In diesem Beispiel ist keine weitere Konfiguration für den Router erforderlich. Die Switch-Ports müssen als Host-Ports konfiguriert sein und STP-Portfast (Spanning Tree Protocol) aktiviert sowie Trunking und Channeling deaktiviert.



L3-Modul-Route zwischen DHCP-Client- und Server-Netzwerken

DHCP verstehen

DHCP wurde ursprünglich in Requests for Comments (RFCs) 1531 definiert und ist seitdem durch

RFC 2131 veraltet. DHCP basiert auf dem Bootstrap Protocol (BootP), das in RFC 951 definiert ist.

DHCP wird von Workstations (Hosts) verwendet, um Informationen zur Erstkonfiguration wie eine IP-Adresse, eine Subnetzmaske und ein Standard-Gateway beim Start abzurufen. Mit DHCP müssen Sie nicht jeden Host manuell mit einer IP-Adresse konfigurieren. Wenn ein Host zu einem anderen IP-Subnetz wechselt, muss er außerdem eine andere IP-Adresse als die zuvor verwendete verwenden. DHCP übernimmt dies automatisch. Er ermöglicht es dem Host, eine IP-Adresse im richtigen IP-Subnetz auszuwählen.

Aktuelle DHCP-RFC-Referenzen

- RFC 2131 - DHCP
- RFC 2132 - DHCP-Optionen und BootP-Anbietererweiterungen
- RFC 1534 - Interoperation zwischen DHCP und BootP
- RFC 1542 - Clarifications and Extensions for the BootP
- RFC 2241 - DHCP-Optionen für Novell Directory Services
- RFC 2242 - Netware/IP-Domänenname und -Informationen
- RFC 2489 - Verfahren zum Definieren neuer DHCP-Optionen

DHCP verwendet ein Client-Server-Modell, bei dem ein oder mehrere Server (DHCP-Server) Clients (Hosts) beim Start des Clients IP-Adressen und andere optionale Konfigurationsparameter zuweisen. Diese Konfigurationsparameter werden vom Server für einen bestimmten Zeitraum an den Client geleast. Beim Hochfahren eines Hosts sendet der TCP/IP-Stack auf dem Host eine Broadcast-Nachricht (DHCPDISCOVER), um neben anderen Konfigurationsparametern eine IP-Adresse und eine Subnetzmaske zu erhalten. Dadurch wird ein Austausch zwischen dem DHCP-Server und dem Host initiiert. Während dieses Austauschs durchläuft der Client die folgenden klar definierten Zustände:

1. Initialisierung
2. Auswählen
3. Anfordern
4. Gebunden
5. Verlängerung
6. Wiederherstellung

Um zwischen diesen Zuständen zu wechseln, können der Client und der Server die in der DHCP-Nachrichtentabelle aufgelisteten Nachrichtentypen austauschen.

DHCP-Nachrichtentabelle

Referenz	Nachricht	Beschreibung
0 x 01	DHCPDISCOVER	Der Client sucht nach verfügbaren DHCP-Servern.
0 x 02	DHCPOFFER	Die Serverantwort auf den DHCPDISCOVER-Client.
0 x 03	DHCPREQUEST	Der Client sendet an den Server, Anfragen boten Parameter von einem Server speziell an, wie im Paket definiert.
0 x 04	DHCPDECLINE	Die Kommunikation zwischen Client und Server zeigt an, dass die Netzwerkadre bereits verwendet wird.
0 x 05	DHCPACK	Die Server-zu-Client-Kommunikation mit Konfigurationsparametern sowie der

		zugesicherten Netzwerkadresse.
0 x 06	DHCPNAK	Die Server-zu-Client-Kommunikation lehnt die Anforderung des Konfigurationsparameters ab.
0 x 07	DHCPRELEASE	Die Client-zu-Server-Kommunikation gibt die Netzwerkadresse ab und bricht der verbleibenden Lease-Zeitraum ab.
0 x 08	DHCPINFORM	Bei der Client-Server-Kommunikation werden nur lokale Konfigurationsparamete angefordert, die der Client bereits extern als Adresse konfiguriert hat.

DHCPDISCOVER

Wenn ein Client zum ersten Mal gestartet wird, befindet er sich im Initialisierungszustand und überträgt eine DHCPDISCOVER-Nachricht auf seinem lokalen physischen Subnetz über den UDP-Port 67 (BootP-Server). Da der Client das Subnetz, zu dem er gehört, nicht kennen kann, ist DHCPDISCOVER eine Übertragung aller Subnetze (Ziel-IP-Adresse 255.255.255.255) mit der Quell-IP-Adresse 0.0.0.0. Die Quell-IP-Adresse ist 0.0.0.0, da der Client keine konfigurierte IP-Adresse hat. Wenn ein DHCP-Server in diesem lokalen Subnetz vorhanden und konfiguriert ist und ordnungsgemäß funktioniert, hört der DHCP-Server den Broadcast und antwortet mit einer DHCPOFFER-Nachricht. Wenn kein DHCP-Server im lokalen Subnetz vorhanden ist, muss ein DHCP/BootP Relay Agent in diesem lokalen Subnetz vorhanden sein, um die DHCPDISCOVER-Nachricht an ein Subnetz weiterzuleiten, das einen DHCP-Server enthält.

Dieser Relay-Agent kann entweder ein dedizierter Host (z. B. Microsoft Windows Server) oder ein Router (z. B. ein Cisco Router, der mit IP-Helper-Anweisungen auf Schnittstellenebene konfiguriert ist) sein.

DHCPOFFER

Ein DHCP-Server, der eine DHCPDISCOVER-Nachricht empfängt, kann mit einer DHCPOFFER-Nachricht auf UDP-Port 68 (BootP-Client) antworten. Der Client empfängt den DHCPOFFER und wechselt in den Auswahlzustand. Diese DHCPOFFER-Nachricht enthält Informationen zur Erstkonfiguration des Clients. Der DHCP-Server füllt beispielsweise das Feld yiaddr der DHCPOFFER-Nachricht mit der angeforderten IP-Adresse aus. Die Subnetzmaske und das Standard-Gateway werden jeweils im Optionsfeld, in der Subnetzmaske und in den Routeroptionen angegeben. Weitere gängige Optionen in der DHCPOFFER-Nachricht sind die Leasedauer der IP-Adresse, die Verlängerungszeit, der Domänennamenserver und der NetBIOS-Namensserver (WINS). Der DHCP-Server sendet den DHCPOFFER an die Broadcast-Adresse, schließt jedoch die Client-Hardware-Adresse in das Chadr-Feld des Angebots ein, sodass der Client weiß, dass es sich um das beabsichtigte Ziel handelt. Falls sich der DHCP-Server nicht im lokalen Subnetz befindet, sendet der DHCP-Server den DHCPOFFER als Unicast-Paket auf UDP-Port 67 zurück an den DHCP/BootP Relay Agent, von dem der DHCPDISCOVER stammt. Der DHCP/BootP-Relay-Agent sendet bzw. deinstalliert den DHCPOFFER dann entweder über das lokale Subnetz auf dem UDP-Port 68, was vom vom Bootp-Client festgelegten Broadcast-Flag abhängt.

DHCPREQUEST

Nachdem der Client eine DHCPOFFER-Nachricht empfangen hat, antwortet er mit einer DHCPREQUEST-Nachricht und gibt seine Absicht an, die Parameter in DHCPOFFER zu

akzeptieren, und wechselt in den Anforderungszustand. Der Client kann mehrere DHCPOFFER-Nachrichten empfangen, eine von jedem DHCP-Server, der die ursprüngliche DHCPDISCOVER-Nachricht empfangen hat. Der Client wählt einen DHCPOFFER aus und antwortet nur auf diesen DHCP-Server und lehnt implizit alle anderen DHCPOFFER-Nachrichten ab. Der Client identifiziert den ausgewählten Server, nachdem er die IP-Adresse des DHCP-Servers in das Optionsfeld "Server Identifier" eingegeben hat. DHCPREQUEST ist auch ein Broadcast, sodass alle DHCP-Server, die einen DHCPREQUEST gesendet haben, den DHCPREQUEST sehen und jeder weiß, ob der DHCPPOFFER akzeptiert oder abgelehnt wurde. Alle zusätzlichen Konfigurationsoptionen, die der Client benötigt, sind im Optionsfeld der DHCPREQUEST-Nachricht enthalten. Obwohl dem Client eine IP-Adresse angeboten wurde, sendet er die DHCPREQUEST-Nachricht mit der Quell-IP-Adresse 0.0.0.0. Zu diesem Zeitpunkt hat der Client noch keine Bestätigung erhalten, dass die Verwendung der IP-Adresse eindeutig ist.

DHCPACK

Nachdem der DHCP-Server DHCPREQUEST empfangen hat, wird die Anforderung mit einer DHCPACK-Nachricht bestätigt, und der Initialisierungsprozess wird abgeschlossen. Die DHCPACK-Nachricht hat eine Quell-IP-Adresse des DHCP-Servers, und die Zieladresse ist wiederum ein Broadcast und enthält alle Parameter, die der Client in der DHCPREQUEST-Nachricht angefordert hat. Wenn der Client das DHCPACK empfängt, wechselt er in den Status "Bound" (Gebunden) und kann nun die IP-Adresse für die Kommunikation im Netzwerk verwenden. Währenddessen speichert der DHCP-Server das Lease in seiner Datenbank und identifiziert es eindeutig mit der Client-ID oder dem chaddr und der zugehörigen IP-Adresse. Sowohl der Client als auch der Server verwenden diese Kombination von Bezeichnern, um auf die Lease zu verweisen. Die Client-Kennung ist die MAC-Adresse des Geräts plus Medientyp.

Bevor der DHCP-Client die neue Adresse verwendet, muss er die einer geleasten Adresse zugeordneten Zeitparameter berechnen, d. h. Lease Time (LT), Renewal Time (T1) und Rebind Time (T2). Die Standardeinstellung für LT ist 72 Stunden. Sie können bei Bedarf kürzere Leasedauer nutzen, um Adressen zu sparen.

DHCPNAK

Wenn der ausgewählte Server die DHCPREQUEST-Nachricht nicht erfüllen kann, antwortet der DHCP-Server mit einer DHCPNAK-Nachricht. Wenn der Client eine DHCPNAK-Nachricht empfängt oder keine Antwort auf eine DHCPREQUEST-Nachricht erhält, startet der Client den Konfigurationsprozess neu, wenn er in den Anforderungsstatus wechselt. Der Client sendet DHCPREQUEST innerhalb von 60 Sekunden mindestens viermal neu, bevor der Initialisierungszustand neu gestartet wird.

DHCPDECLINE

Der Client erhält das DHCPACK und führt optional eine abschließende Überprüfung der Parameter durch. Der Client führt dieses Verfahren aus, wenn er ARP-Anforderungen (Address Resolution Protocol) für die im DHCPACK angegebene IP-Adresse sendet. Wenn der Client beim Empfang einer Antwort auf die ARP-Anforderung feststellt, dass die Adresse bereits verwendet wird, sendet er eine DHCPDECLINE-Nachricht an den Server und startet den Konfigurationsprozess im Status "Requesting" neu.

DHCPINFORM

Wenn ein Client eine Netzwerkadresse auf andere Weise erhalten hat oder über eine manuell konfigurierte IP-Adresse verfügt, kann eine Client-Workstation eine DHCPINFORM-Anforderungsnachricht verwenden, um andere lokale Konfigurationsparameter wie den Domänennamen und die Domänennamenserver (DNS) abzurufen. Wenn DHCP-Server eine DHCPINFORM-Nachricht empfangen, erstellen Sie eine DHCPACK-Nachricht mit allen lokalen Konfigurationsparametern, die für den Client geeignet sind, ohne eine neue IP-Adresse. Dieses DHCPACK wird als Unicast an den Client gesendet.

DHCPRELEASE

Ein DHCP-Client kann die Lease für eine Netzwerkadresse aufgeben, wenn er eine DHCPRELEASE-Nachricht an den DHCP-Server sendet. Der Client identifiziert den Lease, der durch die Verwendung des`Client-`Identifizierungsfelds und der Netzwerkadresse in der DHCPRELEASE-Nachricht freigegeben werden soll. Wenn Sie den aktuellen DHCP-Pool-Bereich erweitern müssen, entfernen Sie den aktuellen Pool von Adressen, und geben Sie den neuen IP-Adressbereich unter dem DHCP-Pool an. Um bestimmte IP-Adressen oder einen Adressbereich aus dem DHCP-Pool zu entfernen, verwenden Sie den Befehl **ip dhcp excluded-address**.

> **Anmerkung:** Wenn Geräte BOOTP verwenden, werden Leases mit unbegrenzter Länge in den DHCP-Bindungen der Router angezeigt.

Leasingverlängerung

Da die IP-Adresse nur vom Server geleast wird, muss die Lease von Zeit zu Zeit erneuert werden. Wenn eine Hälfte der Leasedauer abgelaufen ist (T1=0,5 x LT), versucht der Client, die Lease zu verlängern. Der Client wechselt in den Status "Renewing" (Erneuern) und sendet eine DHCPREQUEST-Nachricht an den Server, der den aktuellen Leasing-Zeitraum innehat. Der Server antwortet auf die Verlängerungsanfrage mit einer DHCPACK-Nachricht, wenn er der Verlängerung des Leasingvertrags zustimmt. Die DHCPACK-Nachricht enthält den neuen Lease-Vertrag und alle neuen Konfigurationsparameter für den Fall, dass während des vorherigen Lease-Vertrags Änderungen am Server vorgenommen werden. Wenn der Client den Server nicht erreichen kann, wenn er aus irgendeinem Grund die Lease hält, versucht er, die Adresse von einem DHCP-Server zu erneuern, nachdem der ursprüngliche DHCP-Server innerhalb einer Zeit T2 nicht auf die Verlängerungsanforderungen reagiert hat. Der Standardwert von T2 ist (7/8 x LT). Dies bedeutet T1 < T2< LT.

Wenn dem Client zuvor eine DHCP-zugewiesene IP-Adresse zugewiesen wurde und er neu gestartet wird, fordert der Client die zuvor geleaste IP-Adresse in einem DHCPREQUEST-Paket an. Diese DHCPREQUEST-Nachricht enthält weiterhin die Quell-IP-Adresse 0.0.0.0 und das Ziel die IP-Broadcast-Adresse 255.255.255.255.

Wenn ein Client im Zuge eines Neustarts ein DHCPREQUEST sendet, darf er nicht das Serverkennungsfeld ausfüllen, sondern muss das angeforderte IP-Adressoptionenfeld ausfüllen. Nur RFC-kompatible Clients füllen das Feld ciaddr mit der angeforderten Adresse anstatt des Felds für die DHCP-Option aus. Der DHCP-Server akzeptiert beide Methoden. Das Verhalten des DHCP-Servers hängt von einer Reihe von Faktoren ab, z. B. bei Windows NT DHCP-Servern von der verwendeten Version des Systems sowie von anderen Faktoren, z. B. der Überschneidung. Wenn der DHCP-Server feststellt, dass der Client die angeforderte IP-Adresse weiterhin verwenden kann, bleibt er stumm oder sendet ein DHCPACK für DHCPREQUEST. Wenn der Server feststellt, dass der Client die angeforderte IP-Adresse nicht verwenden kann, sendet er eine DHCPNACK zurück an den Client. Der Client wechselt dann in den Initialisierungszustand

und sendet eine DHCPDISCOVER-Nachricht.

> **Anmerkung:** Der DHCP-Server weist den DHCP-Clients die untere IP-Adresse aus einem Pool von IP-Adressen zu. Wenn das Leasing der unteren Adresse abläuft, wird sie einem anderen Client zugewiesen, falls dieser angefordert wird. Sie können die Reihenfolge, in der DHCP-Adressen zugewiesen werden, nicht ändern.

DHCP-Pakettabelle

Die Länge der DHCP-Nachricht ist variabel und besteht aus den Feldern in der DHCP-Pakettabelle.

> **Anmerkung:** Dieses Paket ist eine modifizierte Version des ursprünglichen BootP-Pakets.

Feld	Byte	Name	Beschreibung
Op	1	Betriebscode	Identifiziert das Paket als Anforderung oder Antwort: 1=BOOTREQUEST, 2=BOOTREPLY
htype	1	Hardwaretyp	Gibt den Adresstyp der Netzwerkhardware an.
abfallen	1	Hardware-Länge	Gibt die Länge der Hardwareadresse an.
Hopfen	1	Hopfen	Der Client setzt den Wert auf Null, und der Wert wird erhöht, wenn die Anforderung über einen Router weitergeleitet wird.
xid	4	Transaktions-ID	Eine Zufallszahl, die vom Client ausgewählt wird. Alle DHCP-Nachrichten, die für eine bestimmte DHCP-Transaktion ausgetauscht werden, verwenden die ID (xid).
s	2	Sekunden	Gibt die Anzahl der Sekunden seit dem Start des DHCP-Prozesses an.
Markierungen	2	Markierungen	Gibt an, ob es sich bei der Nachricht um Broadcast oder Unicast handelt.
Ziadr	4	Client-IP-Adresse	Wird nur verwendet, wenn der Client seine IP-Adresse kennt, wie im Fall der Status Gebunden, Erneuern oder Erneuern.
Yiadr	4	Ihre IP-Adresse	Wenn die Client-IP-Adresse 0.0.0.0 lautet, fügt der DHCP-Server die angebotene Client-IP-Adresse in dieses Feld ein.
Siadr	4	Server-IP-Adresse	Wenn der Client die IP-Adresse des DHCP-Servers kennt, wird dieses Feld mit der DHCP-Serveradresse ausgefüllt. Andernfalls wird es in DHCPOFFER und DHCPACK vom DHCP-Server verwendet.
Giadr	4	Router-IP-Adresse (GI ADDR)	Die Gateway-IP-Adresse, die vom DHCP/BootP Relay Agent eingegeben wird.
Anzieher	16	Client-MAC-Adresse	Die MAC-Adresse des DHCP-Clients
Name	64	Servername	Der optionale Hostname des Servers.
Datei	128	Name der Startdatei	Der Name der Startdatei.
Optionen	variabel	Optionsparameter	Die optionalen Parameter, die vom DHCP-Server bereitgeste werden können. RFC 2132 bietet alle möglichen Optionen.

Client-Server-Kommunikation für Client, der die DHCP-Adresse bezieht, wenn sich Client und DHCP-Server im gleichen Subnetz befinden

Paketbeschreibung	Quell-MAC-Adresse	Ziel-MAC-Adresse	Quell-IP-Adresse	Ziel-IP-Adresse
DHCPDISCOVER	Kunde	Senden	0.0.0.0	255.255.255.255
DHCPOFFER	DHCPServer	Senden	DHCPServer	255.255.255.255

DHCPREQUEST	Kunde	Senden	0.0.0.0	255.255.255.255
DHCPACK	DHCPServer	Senden	DHCPServer	255.255.255.255

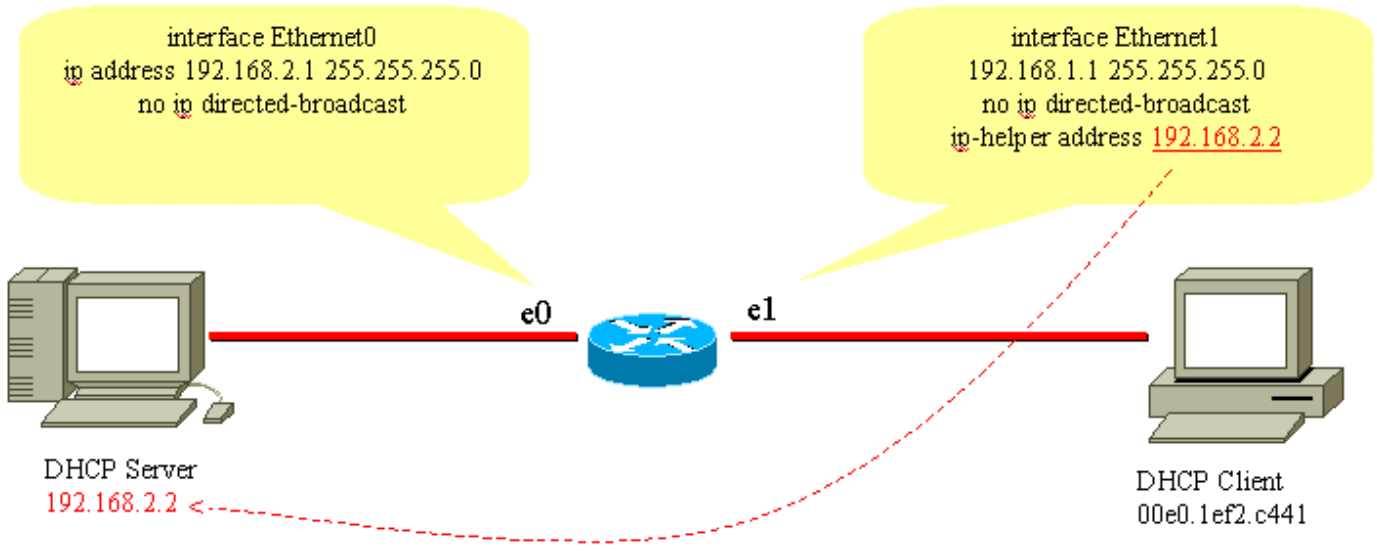
Rolle des DHCP/BootP-Relay-Agents

Router leiten standardmäßig keine Broadcast-Pakete weiter. Da DHCP-Client-Nachrichten die Ziel-IP-Adresse 255.255.255.255 (alle Netzwerk-Broadcasts) verwenden, können DHCP-Clients nur dann Anfragen an einen DHCP-Server in einem anderen Subnetz senden, wenn der DHCP/BootP Relay Agent auf dem Router konfiguriert ist. Der DHCP/BootP Relay Agent leitet DHCP-Anfragen im Auftrag eines DHCP-Clients an den DHCP-Server weiter. Der DHCP/BootP Relay Agent hängt seine eigene IP-Adresse an die Quell-IP-Adresse der DHCP-Frames an, die an den DHCP-Server gesendet werden. Dadurch kann der DHCP-Server per Unicast auf den DHCP/BootP Relay Agent reagieren. Der DHCP/BootP Relay Agent füllt das Gateway-IP-Adressfeld auch mit der IP-Adresse der Schnittstelle auf, über die die DHCP-Nachricht vom Client empfangen wird. Der DHCP-Server verwendet das IP-Adressfeld des Gateways, um das Subnetz zu ermitteln, von dem die DHCPDISCOVER-, DHCPREQUEST- oder DHCPINFORM-Nachricht stammt.

Konfigurieren der DHCP/BootP Relay Agent-Funktion auf dem Cisco IOS®-Router

Die Konfiguration eines Cisco Routers für die Weiterleitung von BootP- oder DHCP-Anfragen ist einfach. Sie müssen lediglich eine IP-Hilfsadresse konfigurieren, die auf den DHCP/BootP-Server oder die Subnetz-Broadcast-Adresse des Netzwerks verweist, in dem sich der Server befindet.

Netzwerkbeispiel:



DHCP/BootP-Relay-Agent

Zum Weiterleiten der BootP-/DHCP-Anfrage vom Client an den DHCP-Server wird der Befehl **eip helper-address** verwendet. Die IP-Hilfsadresse kann für die Weiterleitung von UDP-Broadcast basierend auf der UDP-Portnummer konfiguriert werden. Standardmäßig leitet die IP-Hilfsadresse folgende UDP-Broadcasts weiter:

- Trivial File Transfer Protocol (TFTP) (Port 69)

- DNS (Port 53), Zeitdienst (Port 37)
- NetBIOS-Namensserver (Port 137)
- NetBIOS Datagrammserver (Port 138)
- Boot Protocol (DHCP/BootP)-Client- und Server-Datagramme (Ports 67 und 68)
- Terminal Access Control Access Control System (TACACS)-Dienst (Port 49)
- IEN-116 Namensdienst (Port 42)

IP-Hilfsadressen können UDP-Broadcasts an eine Unicast- oder Broadcast-IP-Adresse weiterleiten. Verwenden Sie die IP-Hilfsadresse jedoch nicht, um UDP-Broadcasts von einem Subnetz an die Broadcast-Adresse eines anderen Subnetzes weiterzuleiten, da es zu umfangreichen Broadcast-Flooding kommen kann. Es werden auch mehrere IP-Hilfsadresseneinträge auf einer Schnittstelle unterstützt:

```
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname router
!
!
!
interface Ethernet0
ip address 192.168.2.1 255.255.255.0
no ip directed-broadcast
!
interface Ethernet1
ip address 192.168.1.1 255.255.255.0
ip helper-address 192.168.2.2
ip helper-address 192.168.2.3

!--- IP helper-address pointing to DHCP server

no ip directed-broadcast
!
!
!
line con 0
exec-timeout 0 0
transport input none
line aux 0
line vty 0 4
login
!
end
```

Cisco Router unterstützen kein Load Balancing von DHCP-Servern, die als DHCP Relay Agents konfiguriert sind. Cisco Router leiten die DHCPDISCOVER-Nachricht an alle für diese Schnittstelle genannten Hilfsadressen weiter. Wenn zwei oder mehr DHCP-Server für ein Subnetz verwendet werden, erhöht sich der DHCP-Datenverkehr nur, da die DHCPDISCOVER-, DHCPOFFER- und DHCPREQUEST/DHCPDECLINE-Nachrichten zwischen den Paaren von DHCP-Client und -Server ausgetauscht werden.

Manuelle Bindungen festlegen

Es gibt zwei Möglichkeiten, manuelle Bindungen einzurichten: einer für den Windows-Host und der andere für Nicht-Windows-Hosts. Für die Konfiguration werden zwei verschiedene Befehle

verwendet: Eine ist für Microsoft DHCP Clients, die andere für Nicht-Microsoft DHCP Clients: **DHCPclient-identifier (**manuelle Bindung - Microsoft DHCP Clients) **und DHCPhardware-address** (manuelle Bindung - Nicht-Microsoft DHCP Clients). Der Grund für zwei verschiedene Befehle besteht darin, dass ein PC, der mit Windows läuft, seine MACs ändert und am Anfang der Adresse eine **01** hinzugefügt wird. Dies sind die Beispielkonfigurationen:

- Dies ist eine Konfiguration für Microsoft DHCP-Clients:

```
configure terminal
ip dhcp pool new_pool
host ip_address subnet_mask
client-identifier 01XXXXXXXXXXXX

!--- xxxxxx represents 48 bit MAC address prepended with 01
```

- Dies ist eine Konfiguration für DHCP-Clients, die nicht von Microsoft stammen:

```
configure terminal
ip dhcp pool new_pool
host ip_address subnet_mask
hardware-address XXXXXXXXXXXX

!--- xxxxxx represents 48 bit MAC address
```

So aktivieren Sie DHCP für sekundäre IP-Segmente

DHCP hat standardmäßig die Einschränkung, dass Antwortpakete nur gesendet werden, wenn die Anforderung von der Schnittstelle empfangen wird, die mit der primären IP-Adresse konfiguriert wurde. Der DHCP-Datenverkehr verwendet die Broadcast-Adresse. Wenn die DHCP-Anfrage von der Router-Schnittstelle empfangen wird, leitet sie diese an den DHCP-Server (wenn die IP-Hilfsadresse konfiguriert ist) mit einer Quelladresse der primären IP-Adresse weiter, die auf der Schnittstelle konfiguriert ist, damit der DHCP-Server weiß, welchen IP-Pool (für den Client) er im DHCP-Antwortpaket verwenden muss.

Der Router kann nicht erfahren, ob die DHCP-Broadcast-Anforderung von einem Gerät stammt, das sich im sekundären, auf der Schnittstelle konfigurierten IP-Netzwerk befindet. Zur Problemumgehung kann die Subschnittstellenkonfiguration (vorausgesetzt, dass das mit dem Router verbundene Gerät das dot1q-Tagging unterstützt) zum Trennen der beiden Subnetze konfiguriert werden, sodass beide Subnetze die entsprechenden IP-Adressen erhalten.

Wenn die sekundäre Adresse die bevorzugte Methode ist, gibt es eine andere Problemumgehung, die darin besteht, den globalen Konfigurationsbefehl **dhcp smart-relay** zu aktivieren. Dies hat die Einschränkung, dass nur dann die sekundäre IP zum Weiterleiten der DHCP-Anfrage verwendet wird, wenn der DHCP-Server nach drei aufeinander folgenden Anfragen für den primären Adresspool keine Antwort erhält.

DHCP-Client-Server-Kommunikation mit DHCP-Relay-Funktion

In der nächsten Tabelle wird der Prozess veranschaulicht, mit dem ein DHCP-Client eine IP-Adresse von einem DHCP-Server bezieht. Diese Tabelle ist dem vorherigen Netzwerkdiagramm "DHCP/BootP Relay Agent-Funktion konfigurieren" nachgebildet. Jeder numerische Wert im Diagramm stellt ein Paket dar, das in dieser nächsten Tabelle beschrieben wird. Verwenden Sie diese Tabelle, um den Paketfluss der DHCP-Client-Server-Unterhaltung zu verstehen. Es hilft Ihnen auch, festzustellen, wo Probleme auftreten.

Prozess zum Abrufen einer IP-Adresse durch einen DHCP-Client

Paket	Client-IP-Adresse	Server-IP-Adresse	GI-Adresse	MAC-Adresse der Paketquelle	IP-Adr der Paketc
1. DHCPDISCOVER wird vom Client gesendet.	0.0.0.0	0.0.0.0	0.0.0.0	0005.DCC9.C640	0.0.0.0
2. Der Router empfängt den DHCPDISCOVER an der E1-Schnittstelle. Der Router erkennt, dass es sich um ein DHCP-UDP-Broadcast handelt. Der Router agiert jetzt als DHCP/BootP Relay Agent und füllt das IP-Adressfeld des Gateways mit der IP-Adresse der eingehenden Schnittstelle, ändert die IP-Quelladresse in eine IP-Adresse der eingehenden Schnittstelle und leitet die Anforderung direkt an den DHCP-Server weiter.	0.0.0.0	0.0.0.0	192.168.1.1	Schnittstelle E2 MAC-Adresse	192.16
3. Der DHCP-Server hat den DHCPDISCOVER empfangen und sendet einen DHCPOFFER an den DHCP Relay Agent.	192.168.1.2	192.168.2.2	192.168.1.1	MAC-Adresse des DHCP-Servers	192.16
4. Der DHCP Relay Agent empfängt eine DHCPOFFER-Nachricht und leitet diese an das lokale LAN weiter.	192.168.1.2	192.168.2.2	192.168.1.1	Schnittstelle E1 MAC-Adresse	192.16
5. DHCPREQUEST vom Client gesendet.	0.0.0.0	0.0.0.0	0.0.0.0	0005.DCC9.C640	0.0.0.0
6. Der Router empfängt den DHCPREQUEST über die E1-Schnittstelle. Der Router erkennt, dass es sich um ein DHCP-UDP-Broadcast-Paket handelt. Der Router agiert jetzt als DHCP Relay Agent und füllt das IP-Adressfeld des Gateways mit der gesendeten IP-Adresse der Schnittstelle aus, ändert die Quell-IP-Adresse in eine eingehende IP-Adresse der Schnittstelle und leitet die Anforderung direkt an den DHCP-Server weiter.	0.0.0.0	0.0.0.0	192.168.1.1	Schnittstelle E2 MAC-Adresse	192.16
7. Der DHCP-Server hat den	192.168.1.2	192.168.2.2	192.168.1.1	MAC-Adresse	192.16

DHCPREQUEST empfangen und sendet ein DHCPACK an den DHCP/BootP Relay Agent. 8. Der DHCP/BootP Relay Agent empfängt das DHCPACK und leitet den DHCPACK-Broadcast über das lokale LAN weiter. Der Client akzeptiert die ACK und verwendet die Client-IP-Adresse.	192.168.1.2	192.168.2.2	192.168.1.1	des DHCP-Servers Schnittstelle E1 MAC-Adresse	192.16

Überlegungen zum DHCP-Bootvorgang vor der Ausführung (PXE)

Pre-Execution Environment (PXE) ermöglicht es einer Workstation, von einem Server in einem Netzwerk zu starten, bevor das System auf der lokalen Festplatte gebootet wird. Ein Netzwerkadministrator muss nicht die jeweilige Workstation besuchen und manuell booten. Betriebssystem und andere Software wie Diagnoseprogramme können von einem Server über das Netzwerk auf das Gerät geladen werden. Die PXE-Umgebung verwendet DHCP zum Konfigurieren der IP-Adresse.

Die Konfiguration des DHCP/BootP-Relay-Agents muss auf dem Router vorgenommen werden, wenn sich der DHCP-Server in einem anderen gerouteten Netzwerksegment befindet. **Der Befehl "eip helper-address"** auf der lokalen Router-Schnittstelle muss konfiguriert werden. Konfigurationsinformationen finden Sie im Abschnitt Konfigurieren der DHCP/BootP Relay Agent-Funktion auf Cisco IOS Router dieses Dokuments.

Verstehen und Fehlerbehebung bei DHCP mit Sniffer-Traces

Dekodieren der Sniffer-Spur von DHCP-Client und -Server auf demselben LAN-Segment

Netzwerktopologie mit DHCP-Client und -Server im gleichen LAN-Segment

Das Sniffer-Trace-Beispiel besteht aus sechs Frames. Diese sechs Frames veranschaulichen ein Szenario, in dem sich der DHCP-Client und -Server im gleichen physischen oder logischen Segment befinden. Verwenden Sie das nächste Codebeispiel, um eine Fehlerbehebung für DHCP durchzuführen. Es ist wichtig, die Sniffer-Spur den Spuren in diesem Beispiel zuzuordnen. Es können einige Unterschiede zu den nächsten abgebildeten Spuren bestehen, aber der allgemeine Paketfluss muss genau derselbe sein. Die Paketverfolgung folgt früheren Diskussionen über die Funktionsweise von DHCP.

```
- - - - - - - - - - - - - - - - - - - - - Frame 1 - DHCPDISCOVER - - - - - - - - - - - - - - - - - -
- - -

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
1[0.0.0.0] [255.255.255.255] 618 0:01:26.810 0.575.244 05/07/2001 11:52:03 AM DHCP: Request,
 Message type: DHCP Discover
```

DLC: ----- DLC Header -----
DLC:
DLC: Frame 1arrived at 11:52:03.8106; frame size is 618 (026A hex) bytes.
DLC: **Destination = BROADCAST FFFFFFFFFFFF**, Broadcast
DLC: **Source = Station 0005DCC9C640**
DLC: Ethertype = 0800 (IP)
DLC:
IP: ----- IP Header -----
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP: 000. .... = routine
IP: ...0 .... = normal delay
IP: .... 0... = normal throughput
IP: .... .0.. = normal reliability
IP: .... ..0. = ECT bit - transport protocol will ignore the CE bit
IP: ....0 = CE bit - no congestion
IP: Total length = 604 bytes
IP: Identification = 9
IP: Flags = 0X
IP: .0.. .... = may fragment
IP: ..0. .... = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 255 seconds/hops
IP: Protocol = 17 (UDP)
IP: Header checksum = B988 (correct)
IP: **Source address = [0.0.0.0]**
IP: **Destination address = [255.255.255.255]**
IP: No options
IP:
UDP: ----- UDP Header -----
UDP:
UDP: **Source port = 68 (BootPc/DHCP)**
UDP: **Destination port = 67 (BootPs/DHCP)**
UDP: Length = 584
UDP: No checksum
UDP: [576 byte(s) of data]
UDP:
DHCP: ----- DHCP Header -----
DHCP:
DHCP: Boot record type = 1 (Request)
DHCP: Hardware address type = 1 (10Mb Ethernet)
DHCP: Hardware address length = 6 bytes
DHCP:
DHCP: Hops = 0
DHCP: **Transaction id = 00000882**
DHCP: Elapsed boot time = 0 seconds
DHCP: Flags = 8000
DHCP: 1... .... = Broadcast IP datagrams
DHCP: Client self-assigned IP address = [0.0.0.0]
DHCP: Client IP address = [0.0.0.0]
DHCP: Next Server to use in bootstrap = [0.0.0.0]
DHCP: Relay Agent = [0.0.0.0]
DHCP: **Client hardware address = 0005DCC9C640**
DHCP:
DHCP: Host name = ""
DHCP: Boot file name = ""
DHCP:
DHCP: Vendor Information tag = 63825363
DHCP: **Message Type = 1 (DHCP Discover)**
DHCP: Maximum message size = 1152
DHCP: **Client identifier = 00636973636F2D303030352E646363392E633634302D564C31**
DHCP: Parameter Request List: 7 entries
DHCP: 1 = Client's subnet mask

DHCP: 66 = TFTP Option
DHCP: 6 = Domain name server
DHCP: 3 = Routers on the client's subnet
DHCP: 67 = Boot File Option
DHCP: 12 = Host name server
DHCP: 150 = Unknown Option
DHCP: Class identifier = 646F63736973312E30
DHCP: Option overload =3 (File and Sname fields hold options)
DHCP:

- **Frame 2 - DHCPOFFER** -
- -

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
2[192.168.1.1] [255.255.255.255] 331 0:01:26.825 0.015.172 05/07/2001 11:52:03 AM DHCP: Reply,
Message type: **DHCP Offer**
DLC: ----- DLC Header -----
DLC:
DLC: Frame 2 arrived at 11:52:03.8258; frame size is 331 (014B hex) bytes.
DLC: **Destination = BROADCAST FFFFFFFFFFFF**, Broadcast
DLC: **Source = Station 0005DCC42484**
DLC: Ethertype = 0800 (IP)
DLC:
IP: ----- IP Header -----
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP: 000. .... = routine
IP: ...0 .... = normal delay
IP: .... 0... = normal throughput
IP: .... .0.. = normal reliability
IP: .... ..0. = ECT bit - transport protocol will ignore the CE bit
IP: ....0 = CE bit - no congestion
IP: Total length = 317 bytes
IP: Identification = 5
IP: Flags = 0X
IP: .0.. .... = may fragment
IP: ..0. .... = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 255 seconds/hops
IP: Protocol = 17 (UDP)
IP: Header checksum = F901 (correct)
IP: **Source address = [192.168.1.1]**
IP: **Destination address = [255.255.255.255]**
IP: No options
IP:
UDP: ----- UDP Header -----
UDP:
UDP: Source port = **67 (BootPs/DHCP)**
UDP: Destination port = **68 (BootPc/DHCP)**
UDP: Length = 297
UDP: No checksum
UDP: [289 byte(s) of data]
UDP:
DHCP: ----- DHCP Header -----
DHCP:
DHCP: Boot record type = 2 (Reply)
DHCP: Hardware address type = 1 (10Mb Ethernet)
DHCP: Hardware address length = 6 bytes
DHCP:
DHCP: Hops = 0
DHCP: **Transaction id = 00000882**
DHCP: Elapsed boot time = 0 seconds
DHCP: Flags = 8000

DHCP: 1... .... = Broadcast IP datagrams
DHCP: Client self-assigned IP address = [0.0.0.0]
DHCP: **Client IP address = [192.168.1.2]**
DHCP: Next Server to use in bootstrap = [0.0.0.0]
DHCP: Relay Agent = [0.0.0.0]
DHCP: **Client hardware address = 0005DCC9C640**
DHCP:
DHCP: Host name = ""
DHCP: Boot file name = ""
DHCP:
DHCP: Vendor Information tag = 63825363
DHCP: Message Type = 2 (DHCP Offer)
DHCP: Server IP address = [192.168.1.1]
DHCP: Request IP address lease time = 85535 (seconds)
DHCP: Address Renewal interval = 42767 (seconds)
DHCP: Address Rebinding interval = 74843 (seconds)
DHCP: Subnet mask = [255.255.255.0]
DHCP: **Domain Name Server address = [192.168.1.3]**
DHCP: **Domain Name Server address = [192.168.1.4]**
DHCP: **Gateway address = [192.168.1.1]**
DHCP:

- **Frame 3 - DHCPREQUEST** -
- -

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
3[0.0.0.0] [255.255.255.255] 618 0:01:26.829 0.003.586 05/07/2001 11:52:03 AM DHCP: Request,
Message type: **DHCP Request**
DLC: ----- DLC Header -----
DLC:
DLC: Frame 56 arrived at 11:52:03.8294; frame size is 618 (026A hex) bytes.
DLC: **Destination = BROADCAST FFFFFFFFFFFF**, Broadcast
DLC: **Source = Station 0005DCC9C640**
DLC: Ethertype = 0800 (IP)
DLC:
IP: ----- IP Header -----
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP: 000. .... = routine
IP: ...0 .... = normal delay
IP: .... 0... = normal throughput
IP: .... .0.. = normal reliability
IP: .... ..0. = ECT bit - transport protocol will ignore the CE bit
IP: ....0 = CE bit - no congestion
IP: Total length = 604 bytes
IP: Identification = 10
IP: Flags = 0X
IP: .0.. .... = may fragment
IP: ..0. .... = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 255 seconds/hops
IP: Protocol = 17 (UDP)
IP: Header checksum = B987 (correct)
IP: **Source address = [0.0.0.0]**
IP: **Destination address = [255.255.255.255]**
IP: No options
IP:
UDP: ----- UDP Header -----
UDP:
UDP: **Source port = 68 (BootPc/DHCP)**
UDP: **Destination port = 67 (BootPs/DHCP)**
UDP: Length = 584
UDP: No checksum

UDP: [576 byte(s) of data]
UDP:
DHCP: ----- DHCP Header -----
DHCP:
DHCP: Boot record type = 1 (Request)
DHCP: Hardware address type = 1 (10Mb Ethernet)
DHCP: Hardware address length = 6 bytes
DHCP:
DHCP: Hops = 0
DHCP: **Transaction id = 00000882**
DHCP: Elapsed boot time = 0 seconds
DHCP: Flags = 8000
DHCP: 1... .... = Broadcast IP datagrams
DHCP: Client self-assigned IP address = [0.0.0.0]
DHCP: Client IP address = [0.0.0.0]
DHCP: Next Server to use in bootstrap = [0.0.0.0]
DHCP: Relay Agent = [0.0.0.0]
DHCP: **Client hardware address = 0005DCC9C640**
DHCP:
DHCP: Host name = ""
DHCP: Boot file name = ""
DHCP:
DHCP: Vendor Information tag = 63825363
DHCP: Message Type = 3 (DHCP Request)
DHCP: Maximum message size = 1152
DHCP: **Client identifier = 00636973636F2D303030352E646363392E633634302D564C31**
DHCP: **Server IP address = [192.168.1.1]**
DHCP: **Request specific IP address = [192.168.1.2]**
DHCP: Request IP address lease time = 85535 (seconds)
DHCP: Parameter Request List: 7 entries
DHCP: 1 = Client's subnet mask
DHCP: 66 = TFTP Option
DHCP: 6 = Domain name server
DHCP: 3 = Routers on the client's subnet
DHCP: 67 = Boot File Option
DHCP: 12 = Host name server
DHCP: 150 = Unknown Option
DHCP: Class identifier = 646F63736973312E30
DHCP: Option overload =3 (File and Sname fields hold options)
DHCP:

- **Frame 4 - DHCPACK** -
-

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
4[192.168.1.1] [255.255.255.255] 331 0:01:26.844 0.014.658 05/07/2001 11:52:03 AM DHCP: Reply,
 Message type: **DHCP Ack**
DLC: ----- DLC Header -----
DLC:
DLC: Frame 57 arrived at 11:52:03.8440; frame size is 331 (014B hex) bytes.
DLC: **Destination = BROADCAST FFFFFFFFFFFF**, Broadcast
DLC: **Source = Station 0005DCC42484**
DLC: Ethertype = 0800 (IP)
DLC:
IP: ----- IP Header -----
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP: 000. .... = routine
IP: ...0 .... = normal delay
IP: .... 0... = normal throughput
IP: .... .0.. = normal reliability
IP: .... ..0. = ECT bit - transport protocol will ignore the CE bit
IP: ....0 = CE bit - no congestion

IP: Total length = 317 bytes
IP: Identification = 6
IP: Flags = 0X
IP: .0.. .... = may fragment
IP: ..0. .... = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 255 seconds/hops
IP: Protocol = 17 (UDP)
IP: Header checksum = F900 (correct)
IP: **Source address = [192.168.1.1]**
IP: **Destination address = [255.255.255.255]**
IP: No options
IP:
UDP: ----- UDP Header -----
UDP:
UDP: **Source port = 67 (BootPs/DHCP)**
UDP: **Destination port = 68 (BootPc/DHCP)**
UDP: Length = 297
UDP: No checksum
UDP: [289 byte(s) of data]
UDP:
DHCP: ----- DHCP Header -----
DHCP:
DHCP: Boot record type = 2 (Reply)
DHCP: Hardware address type = 1 (10Mb Ethernet)
DHCP: Hardware address length = 6 bytes
DHCP:
DHCP: Hops = 0
DHCP: **Transaction id = 00000882**
DHCP: Elapsed boot time = 0 seconds
DHCP: Flags = 8000
DHCP: 1... .... = Broadcast IP datagrams
DHCP: Client self-assigned IP address = [0.0.0.0]
DHCP: **Client IP address = [192.168.1.2]**
DHCP: Next Server to use in bootstrap = [0.0.0.0]
DHCP: Relay Agent = [0.0.0.0]
DHCP: **Client hardware address = 0005DCC9C640**
DHCP:
DHCP: Host name = ""
DHCP: Boot file name = ""
DHCP:
DHCP: Vendor Information tag = 63825363
DHCP: Message Type = 5 (DHCP Ack)
DHCP: Server IP address = [192.168.1.1]
DHCP: Request IP address lease time = 86400 (seconds)
DHCP: Address Renewal interval = 43200 (seconds)
DHCP: Address Rebinding interval = 75600 (seconds)
DHCP: Subnet mask = [255.255.255.0]
DHCP: **Domain Name Server address = [192.168.1.3]**
DHCP: **Domain Name Server address = [192.168.1.4]**
DHCP: **Gateway address = [192.168.1.1]**
DHCP:

- **Frame 5 - ARP** -

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
5 0005DCC9C640 Broadcast 60 0:01:26.846 0.002.954 05/07/2001 11:52:03 AM ARP: R PA=[192.168.1.2]
 HA=0005DCC9C640 PRO=IP
DLC: ----- DLC Header -----
DLC:
DLC: Frame 58 arrived at 11:52:03.8470; frame size is 60 (003C hex) bytes.
DLC: Destination = BROADCAST FFFFFFFFFFFF, Broadcast
DLC: Source = Station 0005DCC9C640
DLC: Ethertype = 0806 (ARP)

```
DLC:
ARP: ----- ARP/RARP frame -----
ARP:
ARP: Hardware type = 1 (10Mb Ethernet)
ARP: Protocol type = 0800 (IP)
ARP: Length of hardware address = 6 bytes
ARP: Length of protocol address = 4 bytes
ARP: Opcode 2 (ARP reply)
ARP: Sender's hardware address = 0005DCC9C640
ARP: Sender's protocol address = [192.168.1.2]
ARP: Target hardware address = FFFFFFFFFFFF
ARP: Target protocol address = [192.168.1.2]
ARP:
ARP: 18 bytes frame padding
ARP:

- - - - - - - - - - - - - - - - - - - - - - Frame 6 - ARP - - - - - - - - - - - - - - - - - - - -

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
6 0005DCC9C640 Broadcast 60 0:01:27.355 0.508.778 05/07/2001 11:52:04 AM ARP: R PA=[192.168.1.2]
 HA=0005DCC9C640 PRO=IP
DLC: ----- DLC Header -----
DLC:
DLC: Frame 59 arrived at 11:52:04.3557; frame size is 60 (003C hex) bytes.
DLC: Destination = BROADCAST FFFFFFFFFFFF, Broadcast
DLC: Source = Station 0005DCC9C640
DLC: Ethertype = 0806 (ARP)
DLC:
ARP: ----- ARP/RARP frame -----
ARP:
ARP: Hardware type = 1 (10Mb Ethernet)
ARP: Protocol type = 0800 (IP)
ARP: Length of hardware address = 6 bytes
ARP: Length of protocol address = 4 bytes
ARP: Opcode 2 (ARP reply)
ARP: Sender's hardware address = 0005DCC9C640
ARP: Sender's protocol address = [192.168.1.2]
ARP: Target hardware address = FFFFFFFFFFFF
ARP: Target protocol address = [192.168.1.2]
ARP:
ARP: 18 bytes frame padding
ARP:
```

Dekodieren der Sniffer-Spur von DHCP-Client und -Server, getrennt durch einen Router, der als DHCP-Relay-Agent konfiguriert ist

Sniffer-B-Ablaufverfolgung

```
- - - - - - - - - - - - - - - - - - - - - - Frame 1 - DHCPDISCOVER - - - - - - - - - - - - - - - - - -
- - -

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
1 [0.0.0.0] [255.255.255.255] 618 0:02:05.759 0.025.369 05/31/2001 06:53:04 AM DHCP: Request,
 Message type: DHCP Discover
DLC: ----- DLC Header -----
DLC:
DLC: Frame 124 arrived at 06:53:04.2043; frame size is 618 (026A hex) bytes.
DLC: Destination = BROADCAST FFFFFFFFFFFF, Broadcast
DLC: Source = Station 0005DCF2C441
DLC: Ethertype = 0800 (IP)
DLC:
```

```
IP: ----- IP Header -----
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP: 000. .... = routine
IP: ...0 .... = normal delay
IP: .... 0... = normal throughput
IP: .... .0.. = normal reliability
IP: .... ..0. = ECT bit - transport protocol will ignore the CE bit
IP: .... ...0 = CE bit - no congestion
IP: Total length = 604 bytes
IP: Identification = 183
IP: Flags = 0X
IP: .0.. .... = may fragment
IP: ..0. .... = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 255 seconds/hops
IP: Protocol = 17 (UDP)
IP: Header checksum = B8DA (correct)
IP: Source address = [0.0.0.0]
IP: Destination address = [255.255.255.255]
IP: No options
IP:
UDP: ----- UDP Header -----
UDP:
UDP: Source port = 68 (BootPc/DHCP)
UDP: Destination port = 67 (BootPs/DHCP)
UDP: Length = 584
UDP: No checksum
UDP: [576 byte(s) of data]
UDP:
DHCP: ----- DHCP Header -----
DHCP:
DHCP: Boot record type = 1 (Request)
DHCP: Hardware address type = 1 (10Mb Ethernet)
DHCP: Hardware address length = 6 bytes
DHCP:
DHCP: Hops = 0
DHCP: Transaction id = 00001425
DHCP: Elapsed boot time = 0 seconds
DHCP: Flags = 8000
DHCP: 1... .... .... .... = Broadcast IP datagrams
DHCP: Client self-assigned IP address = [0.0.0.0]
DHCP: Client IP address = [0.0.0.0]
DHCP: Next Server to use in bootstrap = [0.0.0.0]
DHCP: Relay Agent = [0.0.0.0]
DHCP: Client hardware address = 0005DCF2C441
DHCP:
DHCP: Host name = ""
DHCP: Boot file name = ""
DHCP:
DHCP: Vendor Information tag = 63825363
DHCP: Message Type = 1 (DHCP Discover)
DHCP: Maximum message size = 1152
DHCP: Client identifier = 00636973636F2D303065302E316566322E633434312D4574302F30
DHCP: Parameter Request List: 7 entries
DHCP: 1 = Client's subnet mask
DHCP: 6 = Domain name server
DHCP: 15 = Domain name
DHCP: 44 = NetBIOS over TCP/IP name server
DHCP: 3 = Routers on the client's subnet
DHCP: 33 = Static route
DHCP: 150 = Unknown Option
DHCP: Class identifier = 646F63736973312E30
```

DHCP: Option overload =3 (File and Sname fields hold options)
DHCP:

- **Frame 2 - DHCPOFFER** -
- -

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summaryr
125 [192.168.1.1] [255.255.255.255] 347 0:02:05.772 0.012.764 05/31/2001 06:53:04 AM DHCP:
Reply,
 Message type: **DHCP Offer**
DLC: ----- DLC Header -----
DLC:
DLC: Frame 125 arrived at 06:53:04.2171; frame size is 347 (015B hex) bytes.
DLC: **Destination = BROADCAST FFFFFFFFFFFF, Broadcast**
DLC: **Source = Station 003094248F71**
DLC: Ethertype = 0800 (IP)
DLC:
IP: ----- IP Header -----
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP: 000. .... = routine
IP: ...0 .... = normal delay
IP: .... 0... = normal throughput
IP: .... .0.. = normal reliability
IP: .... ..0. = ECT bit - transport protocol will ignore the CE bit
IP: ....0 = CE bit - no congestion
IP: Total length = 333 bytes
IP: Identification = 45
IP: Flags = 0X
IP: .0.. .... = may fragment
IP: ..0. .... = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 255 seconds/hops
IP: Protocol = 17 (UDP)
IP: Header checksum = F8C9 (correct)
IP: **Source address = [192.168.1.1]**
IP: **Destination address = [255.255.255.255]**
IP: No options
IP:
UDP: ----- UDP Header -----
UDP:
UDP: **Source port = 67 (BootPs/DHCP)**
UDP: **Destination port = 68 (BootPc/DHCP)**
UDP: Length = 313
UDP: Checksum = 8517 (correct)
UDP: [305 byte(s) of data]
UDP:
DHCP: ----- DHCP Header -----
DHCP:
DHCP: Boot record type = 2 (Reply)
DHCP: Hardware address type = 1 (10Mb Ethernet)
DHCP: Hardware address length = 6 bytes
DHCP:
DHCP: Hops = 0
DHCP: **Transaction id = 00001425**
DHCP: Elapsed boot time = 0 seconds
DHCP: Flags = 8000
DHCP: 1... .... = Broadcast IP datagrams
DHCP: Client self-assigned IP address = [0.0.0.0]
DHCP: **Client IP address = [192.168.1.2]**
DHCP: Next Server to use in bootstrap = [0.0.0.0]
DHCP: **Relay Agent = [192.168.1.1]**
DHCP: **Client hardware address = 0005DCF2C441**

DHCP:
DHCP: Host name = ""
DHCP: Boot file name = ""
DHCP:
DHCP: Vendor Information tag = 63825363
DHCP: Message Type = 2 (DHCP Offer)
DHCP: Server IP address = [192.168.2.2]
DHCP: Request IP address lease time = 99471 (seconds)
DHCP: Address Renewal interval = 49735 (seconds)
DHCP: Address Rebinding interval = 87037 (seconds)
DHCP: Subnet mask = [255.255.255.0]
DHCP: **Domain Name Server address = [192.168.10.1]**
DHCP: **Domain Name Server address = [192.168.10.2]**
DHCP: **NetBIOS Server address = [192.168.10.1]**
DHCP: **NetBIOS Server address = [192.168.10.3]**
DHCP: **Domain name = "cisco.com"**
DHCP:

- **Frame 3 - DHCPREQUEST** -
- - -

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
3 [0.0.0.0] [255.255.255.255] 618 0:02:05.774 0.002.185 05/31/2001 06:53:04 AM DHCP: Request,
 Message type: **DHCP Request**
DLC: ----- DLC Header -----
DLC:
DLC: Frame 126 arrived at 06:53:04.2193; frame size is 618 (026A hex) bytes.
DLC: **Destination = BROADCAST FFFFFFFFFFFF, Broadcast**
DLC: **Source = Station Cisc14F2C441**
DLC: Ethertype = 0800 (IP)
DLC:
IP: ----- IP Header -----
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP: 000. .... = routine
IP: ...0 .... = normal delay
IP: .... 0... = normal throughput
IP: .... .0.. = normal reliability
IP: .... ..0. = ECT bit - transport protocol will ignore the CE bit
IP: ....0 = CE bit - no congestion
IP: Total length = 604 bytes
IP: Identification = 184
IP: Flags = 0X
IP: .0.. .... = may fragment
IP: ..0. .... = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 255 seconds/hops
IP: Protocol = 17 (UDP)
IP: Header checksum = B8D9 (correct)
IP: **Source address = [0.0.0.0]**
IP: **Destination address = [255.255.255.255]**
IP: No options
IP:
UDP: ----- UDP Header -----
UDP:
UDP: **Source port = 68 (BootPc/DHCP)**
UDP: **Destination port = 67 (BootPs/DHCP)**
UDP: Length = 584
UDP: No checksum
UDP: [576 byte(s) of data]
UDP:
DHCP: ----- DHCP Header -----
DHCP:

DHCP: Boot record type = 1 (Request)
DHCP: Hardware address type = 1 (10Mb Ethernet)
DHCP: Hardware address length = 6 bytes
DHCP:
DHCP: Hops = 0
DHCP: **Transaction id = 00001425**
DHCP: Elapsed boot time = 0 seconds
DHCP: Flags = 8000
DHCP: 1... .... = Broadcast IP datagrams
DHCP: Client self-assigned IP address = [0.0.0.0]
DHCP: Client IP address = [0.0.0.0]
DHCP: Next Server to use in bootstrap = [0.0.0.0]
DHCP: Relay Agent = [0.0.0.0]
DHCP: **Client hardware address = 0005DCF2C441**
DHCP:
DHCP: Host name = ""
DHCP: Boot file name = ""
DHCP:
DHCP: Vendor Information tag = 63825363
DHCP: Message Type = 3 (DHCP Request)
DHCP: Maximum message size = 1152
DHCP: **Client identifier = 00636973636F2D303065302E316566322E633434312D4574302F30**
DHCP: **Server IP address = [192.168.2.2]**
DHCP: **Request specific IP address = [192.168.1.2]**
DHCP: Request IP address lease time = 99471 (seconds)
DHCP: Parameter Request List: 7 entries
DHCP: 1 = Client's subnet mask
DHCP: 6 = Domain name server
DHCP: 15 = Domain name
DHCP: 44 = NetBIOS over TCP/IP name server
DHCP: 3 = Routers on the client's subnet
DHCP: 33 = Static route
DHCP: 150 = Unknown Option
DHCP: Class identifier = 646F63736973312E30
DHCP: Option overload =3 (File and Sname fields hold options)
DHCP:

- **Frame 4 - DHCPACK** -
-

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
4 [192.168.1.1] [255.255.255.255] 347 0:02:05.787 0.012.875 05/31/2001 06:53:04 AM DHCP: Reply,
 Message type: **DHCP Ack**
DLC: ----- DLC Header -----
DLC:
DLC: Frame 127 arrived at 06:53:04.2321; frame size is 347 (015B hex) bytes.
DLC: **Destination = BROADCAST FFFFFFFFFFFF, Broadcast**
DLC: **Source = Station 003094248F71**
DLC: Ethertype = 0800 (IP)
DLC:
IP: ----- IP Header -----
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP: 000. .... = routine
IP: ...0 .... = normal delay
IP: .... 0... = normal throughput
IP: .... .0.. = normal reliability
IP: .... ..0. = ECT bit - transport protocol will ignore the CE bit
IP: ....0 = CE bit - no congestion
IP: Total length = 333 bytes
IP: Identification = 47
IP: Flags = 0X
IP: .0.. .... = may fragment

IP: ..0. .... = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 255 seconds/hops
IP: Protocol = 17 (UDP)
IP: Header checksum = F8C7 (correct)
IP: **Source address = [192.168.1.1]**
IP: **Destination address = [255.255.255.255]**
IP: No options
IP:
UDP: ----- UDP Header -----
UDP:
UDP: **Source port = 67 (BootPs/DHCP)**
UDP: **Destination port = 68 (BootPc/DHCP)**
UDP: Length = 313
UDP: Checksum = 326F (correct)
UDP: [305 byte(s) of data]
UDP:
DHCP: ----- DHCP Header -----
DHCP:
DHCP: Boot record type = 2 (Reply)
DHCP: Hardware address type = 1 (10Mb Ethernet)
DHCP: Hardware address length = 6 bytes
DHCP:
DHCP: Hops = 0
DHCP: **Transaction id = 00001425**
DHCP: Elapsed boot time = 0 seconds
DHCP: Flags = 8000
DHCP: 1... .... = Broadcast IP datagrams
DHCP: Client self-assigned IP address = [0.0.0.0]
DHCP: Client IP address = [192.168.1.2]
DHCP: Next Server to use in bootstrap = [0.0.0.0]
DHCP: **Relay Agent = [192.168.1.1]**
DHCP: **Client hardware address = 0005DCF2C441**
DHCP:
DHCP: Host name = ""
DHCP: Boot file name = ""
DHCP:
DHCP: Vendor Information tag = 63825363
DHCP: Message Type = 5 (DHCP Ack)
DHCP: Server IP address = [192.168.2.2]
DHCP: Request IP address lease time = 172800 (seconds)
DHCP: Address Renewal interval = 86400 (seconds)
DHCP: Address Rebinding interval = 151200 (seconds)
DHCP: Subnet mask = [255.255.255.0]
DHCP: **Domain Name Server address = [192.168.10.1]**
DHCP: **Domain Name Server address = [192.168.10.2]**
DHCP: **NetBIOS Server address = [192.168.10.1]**
DHCP: **NetBIOS Server address = [192.168.10.3]**
DHCP: **Domain name = "cisco.com"**
DHCP:

- **Frame 5 - ARP** -

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
5 Cisc14F2C441 Broadcast 60 0:02:05.798 0.011.763 05/31/2001 06:53:04 AM ARP: R PA=[192.168.1.2]
HA=Cisc14F2C441 PRO=IP
DLC: ----- DLC Header -----
DLC:
DLC: Frame 128 arrived at 06:53:04.2439; frame size is 60 (003C hex) bytes.
DLC: Destination = BROADCAST FFFFFFFFFFFF, Broadcast
DLC: Source = Station Cisc14F2C441
DLC: Ethertype = 0806 (ARP)
DLC:
ARP: ----- ARP/RARP frame -----

```
ARP:
ARP: Hardware type = 1 (10Mb Ethernet)
ARP: Protocol type = 0800 (IP)
ARP: Length of hardware address = 6 bytes
ARP: Length of protocol address = 4 bytes
ARP: Opcode 2 (ARP reply)
ARP: Sender's hardware address = 00E01EF2C441
ARP: Sender's protocol address = [192.168.1.2]
ARP: Target hardware address = FFFFFFFFFFFF
ARP: Target protocol address = [192.168.1.2]
ARP:
ARP: 18 bytes frame padding
ARP:

- - - - - - - - - - - - - - - - - - - - - Frame 6 - ARP - - - - - - - - - - - - - - - - - - - -

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
5 Cisc14F2C441 Broadcast 60 0:02:05.798 0.011.763 05/31/2001 06:53:04 AM ARP: R PA=[192.168.1.2]
 HA=Cisc14F2C441 PRO=IP
DLC: ----- DLC Header -----
DLC:
DLC: Frame 128 arrived at 06:53:04.2439; frame size is 60 (003C hex) bytes.
DLC: Destination = BROADCAST FFFFFFFFFFFF, Broadcast
DLC: Source = Station Cisc14F2C441
DLC: Ethertype = 0806 (ARP)
DLC:
ARP: ----- ARP/RARP frame -----
ARP:
ARP: Hardware type = 1 (10Mb Ethernet)
ARP: Protocol type = 0800 (IP)
ARP: Length of hardware address = 6 bytes
ARP: Length of protocol address = 4 bytes
ARP: Opcode 2 (ARP reply)
ARP: Sender's hardware address = 00E01EF2C441
ARP: Sender's protocol address = [192.168.1.2]
ARP: Target hardware address = FFFFFFFFFFFF
ARP: Target protocol address = [192.168.1.2]
ARP:
ARP: 18 bytes frame padding
ARP:
```

Sniffer-A-Spur

```
- - - - - - - - - - - - - - - - - - - - - Frame 1 - DHCPDISCOVER - - - - - - - - - - - - - - - - - -
- - -

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
118 [192.168.1.1] [192.168.2.2] 618 0:00:51.212 0.489.912 05/31/2001 07:02:54 AM DHCP: Request,
 Message type: DHCP Discover
DLC: ----- DLC Header -----
DLC:
DLC: Frame 118 arrived at 07:02:54.7463; frame size is 618 (026A hex) bytes.
DLC: Destination = Station 0005DC0BF2F4
DLC: Source = Station 003094248F72
DLC: Ethertype = 0800 (IP)
DLC:
IP: ----- IP Header -----
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP: 000. .... = routine
IP: ...0 .... = normal delay
IP: .... 0... = normal throughput
```

IP: .... .0.. = normal reliability
IP: .... ..0. = ECT bit - transport protocol will ignore the CE bit
IP: ....0 = CE bit - no congestion
IP: Total length = 604 bytes
IP: Identification = 52
IP: Flags = 0X
IP: .0.. .... = may fragment
IP: ..0. .... = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 255 seconds/hops
IP: Protocol = 17 (UDP)
IP: Header checksum = 3509 (correct)
IP: **Source address = [192.168.1.1]**
IP: **Destination address = [192.168.2.2]**
IP: No options
IP:
UDP: ----- UDP Header -----
UDP:
UDP: **Source port = 67 (BootPs/DHCP)**
UDP: **Destination port = 67 (BootPs/DHCP)**
UDP: Length = 584
UDP: Checksum = 0A19 (correct)
UDP: [576 byte(s) of data]
UDP:
DHCP: ----- DHCP Header -----
DHCP:
DHCP: Boot record type = 1 (Request)
DHCP: Hardware address type = 1 (10Mb Ethernet)
DHCP: Hardware address length = 6 bytes
DHCP:
DHCP: Hops = 1
DHCP: Transaction id = 000005F4
DHCP: Elapsed boot time = 0 seconds
DHCP: Flags = 8000
DHCP: 1... .... = Broadcast IP datagrams
DHCP: Client self-assigned IP address = [0.0.0.0]
DHCP: Client IP address = [0.0.0.0]
DHCP: Next Server to use in bootstrap = [0.0.0.0]
DHCP: **Relay Agent = [192.168.1.1]**
DHCP: **Client hardware address = 0005DCF2C441**
DHCP:
DHCP: Host name = ""
DHCP: Boot file name = ""
DHCP:
DHCP: Vendor Information tag = 63825363
DHCP: Message Type = 1 (DHCP Discover)
DHCP: Maximum message size = 1152
DHCP: Client identifier = 00636973636F2D303065302E316566322E633434312D4574302F30
DHCP: Parameter Request List: 7 entries
DHCP: 1 = Client's subnet mask
DHCP: 6 = Domain name server
DHCP: 15 = Domain name
DHCP: 44 = NetBIOS over TCP/IP name server
DHCP: 3 = Routers on the client's subnet
DHCP: 33 = Static route
DHCP: 150 = Unknown Option
DHCP: Class identifier = 646F63736973312E30
DHCP: Option overload =3 (File and Sname fields hold options)
DHCP:

- **Frame 2 - DHCPOFFER** -
- -

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary

2 [192.168.2.2] [192.168.1.1] 347 0:00:51.214 0.002.133 05/31/2001 07:02:54 AM DHCP: Request,
 Message type: **DHCP Offer**
DLC: ----- DLC Header -----
DLC:
DLC: Frame 119 arrived at 07:02:54.7485; frame size is 347 (015B hex) bytes.
DLC: **Destination = Station 003094248F72**
DLC: **Source = Station 0005DC0BF2F4**
DLC: Ethertype = 0800 (IP)
DLC:
IP: ----- IP Header -----
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP: 000. .... = routine
IP: ...0 .... = normal delay
IP: .... 0... = normal throughput
IP: .... .0.. = normal reliability
IP: .... ..0. = ECT bit - transport protocol will ignore the CE bit
IP: ....0 = CE bit - no congestion
IP: Total length = 333 bytes
IP: Identification = 41
IP: Flags = 0X
IP: .0.. .... = may fragment
IP: ..0. .... = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 255 seconds/hops
IP: Protocol = 17 (UDP)
IP: Header checksum = 3623 (correct)
IP: **Source address = [192.168.2.2]**
IP: **Destination address = [192.168.1.1]**
IP: No options
IP:
UDP: ----- UDP Header -----
UDP:
UDP: **Source port = 67 (BootPs/DHCP)**
UDP: **Destination port = 67 (BootPs/DHCP)**
UDP: Length = 313
UDP: Checksum = A1F8 (correct)
UDP: [305 byte(s) of data]
UDP:
DHCP: ----- DHCP Header -----
DHCP:
DHCP: Boot record type = 2 (Request)
DHCP: Hardware address type = 1 (10Mb Ethernet)
DHCP: Hardware address length = 6 bytes
DHCP:
DHCP: Hops = 0
DHCP: Transaction id = 000005F4
DHCP: Elapsed boot time = 0 seconds
DHCP: Flags = 8000
DHCP: 1... .... = Broadcast IP datagrams
DHCP: Client self-assigned IP address = [0.0.0.0]
DHCP: Client IP address = [192.168.1.2]
DHCP: Next Server to use in bootstrap = [0.0.0.0]
DHCP: Relay Agent = [192.168.1.1]
DHCP: **Client hardware address = 0005DCF2C441**
DHCP:
DHCP: Host name = ""
DHCP: Boot file name = ""
DHCP:
DHCP: Vendor Information tag = 63825363
DHCP: Message Type = 2 (DHCP Offer)
DHCP: Server IP address = [192.168.2.2]
DHCP: Request IP address lease time = 172571 (seconds)

```
DHCP: Address Renewal interval = 86285 (seconds)
DHCP: Address Rebinding interval = 150999 (seconds)
DHCP: Subnet mask = [255.255.255.0]
DHCP: Domain Name Server address = [192.168.10.1]
DHCP: Domain Name Server address = [192.168.10.2]
DHCP: NetBIOS Server address = [192.168.10.1]
DHCP: NetBIOS Server address = [192.168.10.3]
DHCP: Domain name = "cisco.com"
DHCP:

- - - - - - - - - - - - - - - - - - - - - Frame 3 - DHCPREQUEST - - - - - - - - - - - - - - - - - -
- - -

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
3 [192.168.1.1] [192.168.2.2] 618 0:00:51.240 0.025.974 05/31/2001 07:02:54 AM DHCP: Request,
 Message type: DHCP Request
DLC: ----- DLC Header -----
DLC:
DLC: Frame 120 arrived at 07:02:54.7745; frame size is 618 (026A hex) bytes.
DLC: Destination = Station 0005DC0BF2F4
DLC: Source = Station 003094248F72
DLC: Ethertype = 0800 (IP)
DLC:
IP: ----- IP Header -----
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP: 000. .... = routine
IP: ...0 .... = normal delay
IP: .... 0... = normal throughput
IP: .... .0.. = normal reliability
IP: .... ..0. = ECT bit - transport protocol will ignore the CE bit
IP: .... ...0 = CE bit - no congestion
IP: Total length = 604 bytes
IP: Identification = 54
IP: Flags = 0X
IP: .0.. .... = may fragment
IP: ..0. .... = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 255 seconds/hops
IP: Protocol = 17 (UDP)
IP: Header checksum = 3507 (correct)
IP: Source address = [192.168.1.1]
IP: Destination address = [192.168.2.2]
IP: No options
IP:
UDP: ----- UDP Header -----
UDP:
UDP: Source port = 67 (BootPs/DHCP)
UDP: Destination port = 67 (BootPs/DHCP)
UDP: Length = 584
UDP: Checksum = 4699 (correct)
UDP: [576 byte(s) of data]
UDP:
DHCP: ----- DHCP Header -----
DHCP:
DHCP: Boot record type = 1 (Request)
DHCP: Hardware address type = 1 (10Mb Ethernet)
DHCP: Hardware address length = 6 bytes
DHCP:
DHCP: Hops = 1
DHCP: Transaction id = 000005F4
DHCP: Elapsed boot time = 0 seconds
DHCP: Flags = 8000
```

```
DHCP: 1... .... .... .... = Broadcast IP datagrams
DHCP: Client self-assigned IP address = [0.0.0.0]
DHCP: Client IP address = [0.0.0.0]
DHCP: Next Server to use in bootstrap = [0.0.0.0]
DHCP: Relay Agent = [192.168.1.1]
DHCP: Client hardware address = 0005DCF2C441
DHCP:
DHCP: Host name = ""
DHCP: Boot file name = ""
DHCP:
DHCP: Vendor Information tag = 63825363
DHCP: Message Type = 3 (DHCP Request)
DHCP: Maximum message size = 1152
DHCP: Client identifier = 00636973636F2D303065302E316566322E633434312D4574302F30
DHCP: Server IP address = [192.168.2.2]
DHCP: Request specific IP address = [192.168.1.2]
DHCP: Request IP address lease time = 172571 (seconds)
DHCP: Parameter Request List: 7 entries
DHCP: 1 = Client's subnet mask
DHCP: 6 = Domain name server
DHCP: 15 = Domain name
DHCP: 44 = NetBIOS over TCP/IP name server
DHCP: 3 = Routers on the client's subnet
DHCP: 33 = Static route
DHCP: 150 = Unknown Option
DHCP: Class identifier = 646F63736973312E30
DHCP: Option overload =3 (File and Sname fields hold options)
DHCP:

- - - - - - - - - - - - - - - - - - - - Frame 4 - DHCPACK - - - - - - - - - - - - - - - - - - - -
-

Frame Status Source Address Dest. Address Size Rel. Time Delta Time Abs. Time Summary
4 [192.168.2.2] [192.168.1.1] 347 0:00:51.240 0.000.153 05/31/2001 07:02:54 AM DHCP: Request,
 Message type: DHCP Ack
DLC: ----- DLC Header -----
DLC:
DLC: Frame 121 arrived at 07:02:54.7746; frame size is 347 (015B hex) bytes.
DLC: Destination = Station 003094248F72
DLC: Source = Station 0005DC0BF2F4
DLC: Ethertype = 0800 (IP)
DLC:
IP: ----- IP Header -----
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP: 000. .... = routine
IP: ...0 .... = normal delay
IP: .... 0... = normal throughput
IP: .... .0.. = normal reliability
IP: .... ..0. = ECT bit - transport protocol will ignore the CE bit
IP: .... ...0 = CE bit - no congestion
IP: Total length = 333 bytes
IP: Identification = 42
IP: Flags = 0X
IP: .0.. .... = may fragment
IP: ..0. .... = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live = 255 seconds/hops
IP: Protocol = 17 (UDP)
IP: Header checksum = 3622 (correct)
IP: Source address = [192.168.2.2]
IP: Destination address = [192.168.1.1]
IP: No options
```

```
IP:
UDP: ----- UDP Header -----
UDP:
UDP: Source port = 67 (BootPs/DHCP)
UDP: Destination port = 67 (BootPs/DHCP)
UDP: Length = 313
UDP: Checksum = 7DF6 (correct)
UDP: [305 byte(s) of data]
UDP:
DHCP: ----- DHCP Header -----
DHCP:
DHCP: Boot record type = 2 (Request)
DHCP: Hardware address type = 1 (10Mb Ethernet)
DHCP: Hardware address length = 6 bytes
DHCP:
DHCP: Hops = 0
DHCP: Transaction id = 000005F4
DHCP: Elapsed boot time = 0 seconds
DHCP: Flags = 8000
DHCP: 1... .... .... .... = Broadcast IP datagrams
DHCP: Client self-assigned IP address = [0.0.0.0]
DHCP: Client IP address = [192.168.1.2]
DHCP: Next Server to use in bootstrap = [0.0.0.0]
DHCP: Relay Agent = [192.168.1.1]
DHCP: Client hardware address = 0005DCF2C441
DHCP:
DHCP: Host name = ""
DHCP: Boot file name = ""
DHCP:
DHCP: Vendor Information tag = 63825363
DHCP: Message Type = 5 (DHCP Ack)
DHCP: Server IP address = [192.168.2.2]
DHCP: Request IP address lease time = 172800 (seconds)
DHCP: Address Renewal interval = 86400 (seconds)
DHCP: Address Rebinding interval = 151200 (seconds)
DHCP: Subnet mask = [255.255.255.0]
DHCP: Domain Name Server address = [192.168.10.1]
DHCP: Domain Name Server address = [192.168.10.2]
DHCP: NetBIOS Server address = [192.168.10.1]
DHCP: NetBIOS Server address = [192.168.10.3]
DHCP: Domain name = "cisco.com"
DHCP:
```

Fehlerbehebung bei DHCP, wenn Client-Workstations keine DHCP-Adressen erhalten können

Fallstudie 1: DHCP-Server auf demselben LAN-Segment oder VLAN wie DHCP-Client

Wenn sich der DHCP-Server und der Client im gleichen LAN-Segment oder VLAN befinden und der Client keine IP-Adresse von einem DHCP-Server abrufen kann. Es ist jedoch unwahrscheinlich, dass der lokale Router ein DHCP-Problem verursacht. Das Problem hängt mit den Geräten zusammen, die den DHCP-Server und den DHCP-Client verbinden. Das Problem kann jedoch beim DHCP-Server oder -Client selbst liegen. Diese Module helfen bei der Fehlerbehebung und bei der Feststellung, welches Gerät ein Problem verursacht.

> **Anmerkung:** Um den DHCP-Server auf VLAN-Basis zu konfigurieren, definieren Sie verschiedene DHCP-Pools für jedes VLAN, das DHCP-Adressen für Ihre Clients bereitstellt.

Fallstudie 2: DHCP-Server und DHCP-Client werden durch einen Router getrennt, der für die DHCP/BootP-Relay-Agent-Funktionalität konfiguriert ist.

Wenn sich der DHCP-Server und der Client in den verschiedenen LAN-Segmenten oder VLANs befinden, fungiert der Router als DHCP/BootP Relay Agent, der für die Weiterleitung von DHCPREQUEST an den DHCP-Server zuständig ist. Es sind zusätzliche Schritte erforderlich, um Probleme mit dem DHCP/BootP Relay Agent sowie mit dem DHCP-Server und -Client zu beheben. Wenn Sie diese Module befolgen, können Sie bestimmen, welches Gerät die Probleme verursacht.

DHCP-Server auf Router weist Adressen nicht zu, wenn der POOL ERSCHÖPFT-Fehler auftritt

Es ist möglich, dass einige Adressen immer noch im Besitz von Clients sind, auch wenn sie aus dem Pool freigegeben werden. Dies kann durch **die Ausgabe von ip dhcp** conflict überprüft werden. Ein Adressenkonflikt tritt auf, wenn zwei Hosts dieselbe IP-Adresse verwenden. Bei der Adresszuweisung prüft das DHCP, ob ein Konflikt mit dem Ping und dem unnötigen ARP besteht.

Wenn ein Konflikt erkannt wird, wird die Adresse aus dem Pool entfernt. Die Adresse wird zugewiesen, bis der Administrator den Konflikt löst. **Konfigurieren Sie die IP-DHCP-Konfliktprotokollierung**, um dieses Problem zu beheben.

Module zur DHCP-Fehlerbehebung

Informationen zu möglichen DHCP-Problemen

DHCP-Probleme können aus einer Vielzahl von Gründen auftreten. Die häufigsten Gründe sind Konfigurationsprobleme. Viele DHCP-Probleme können jedoch durch Softwarefehler in Systemen, NIC-Treibern (Network Interface Card) oder DHCP/BootP Relay Agents auf Routern verursacht werden. Aufgrund der Anzahl der potenziell problematischen Bereiche ist ein systematischer Ansatz zur Fehlerbehebung erforderlich.

Kurze Liste möglicher Ursachen von DHCP-Problemen:

- Catalyst Switch-Standardkonfiguration
- Konfiguration des DHCP/BootP-Relay-Agents
- Netzwerkkarten-Kompatibilitätsproblem oder DHCP-Funktionsproblem
- Fehlerhafte Netzwerkkarte oder falsche Installation des Netzwerkkartentreibers
- Intermittierende Netzwerkausfälle aufgrund häufiger Spanning Tree-Berechnungen
- Verhalten des Betriebssystems oder Softwarefehler
- Konfiguration des DHCP-Serverbereichs oder Softwarefehler
- Softwarefehler bei Cisco Catalyst Switch oder Cisco IOS DHCP/BootP Relay Agent
- Die Prüfung für Unicast Reverse Path Forwarding (uRPF) ist fehlgeschlagen, da das DHCP-Angebot an einer anderen als der erwarteten Schnittstelle empfangen wurde. Wenn die Funktion Reverse Path Forwarding (RPF) für eine Schnittstelle aktiviert ist, kann ein Cisco Router Dynamic Host Configuration Protocol (DHCP)- und BOOTstrap Protocol (BOOTP)-Pakete mit Quelladressen von 0.0.0.0 und Zieladressen von 255.255.255.255 verwerfen. Der Router kann auch alle IP-Pakete mit Multicast-IP verwerfen Ziel an der Schnittstelle. Dieses

Problem ist in der Cisco Bug-ID CSCdw31925 dokumentiert.
Hinweis: Nur registrierte Cisco Kunden können auf Fehlerberichte zugreifen.

- Der DHCP-Datenbank-Agent wird nicht verwendet, die DHCP-Konfliktprotokollierung ist jedoch nicht deaktiviert.

A. Überprüfen der physischen Verbindung

Dieses Verfahren gilt für alle Fallstudien.

Überprüfen Sie zunächst die physische Verbindung eines DHCP-Clients und -Servers. Wenn Sie mit einem Catalyst Switch verbunden sind, stellen Sie sicher, dass sowohl der DHCP-Client als auch der DHCP-Server über eine physische Verbindung verfügen. Bei Cisco IOS-basierten Switches wie dem Catalyst 2900XL/3500XL/2950/3550 muss der entsprechende Befehl **show port statusisshow interface <interface> verwendet werden**. Wenn der Status der Schnittstelle etwas Anderes als <Schnittstelle> aktiv ist, das Leitungsprotokoll aktiv ist, leitet der Port keinen Datenverkehr weiter, nicht einmal DHCP-Client-Anfragen. Die Ausgabe der Befehle:

```
Switch#show interface fastEthernet 0/1
FastEthernet0/1 is up, line protocol is up
Hardware is Fast Ethernet, address is 0030.94dc.acc1 (bia 0030.94dc.acc1)
```

Wenn die physische Verbindung verifiziert wurde und tatsächlich keine Verbindung zwischen dem Catalyst Switch und dem DHCP-Client besteht, können Sie den Abschnitt Problembehebung bei Cisco Catalyst Switches mit NIC-Kompatibilitätsproblemen verwenden, um Probleme mit der Konnektivität der physischen Schicht zu beheben.

Übermäßige Datenverbindungsfehler führen dazu, dass Ports auf einigen Catalyst-Switches in den Status "anerrdisable" wechseln. Weitere Informationen finden Sie unterErrdisable Port State Recovery auf den Cisco IOS-Plattformen. Diese beschreiben den errdisable-Status, erläutern die Wiederherstellung und enthalten Beispiele für die Wiederherstellung nach diesem Status.

B. Konfigurieren der Client-Workstation und der statischen IP zum Testen der Netzwerkverbindung

Dieses Verfahren gilt für alle Fallstudien.

Wenn Sie DHCP-Probleme beheben, ist es wichtig, eine statische IP-Adresse auf einer Client-Workstation zu konfigurieren, um die Netzwerkverbindung zu überprüfen. Wenn die Workstation nicht auf die Netzwerkressourcen zugreifen kann, obwohl sie über eine statisch konfigurierte IP-Adresse verfügt, liegt die Ursache des Problems nicht bei DHCP. An diesem Punkt müssen Sie eine Fehlerbehebung für die Netzwerkverbindung durchführen.

C. Überprüfen des Problems als Startproblem

Dieses Verfahren gilt für alle Fallstudien.

Wenn der DHCP-Client beim Start keine IP-Adresse vom DHCP-Server abrufen kann, können Sie den Client manuell zwingen, eine DHCP-Anfrage zu senden. Führen Sie die nächsten Schritte aus, um manuell eine IP-Adresse von einem DHCP-Server für das aufgeführte Betriebssystem zu erhalten.

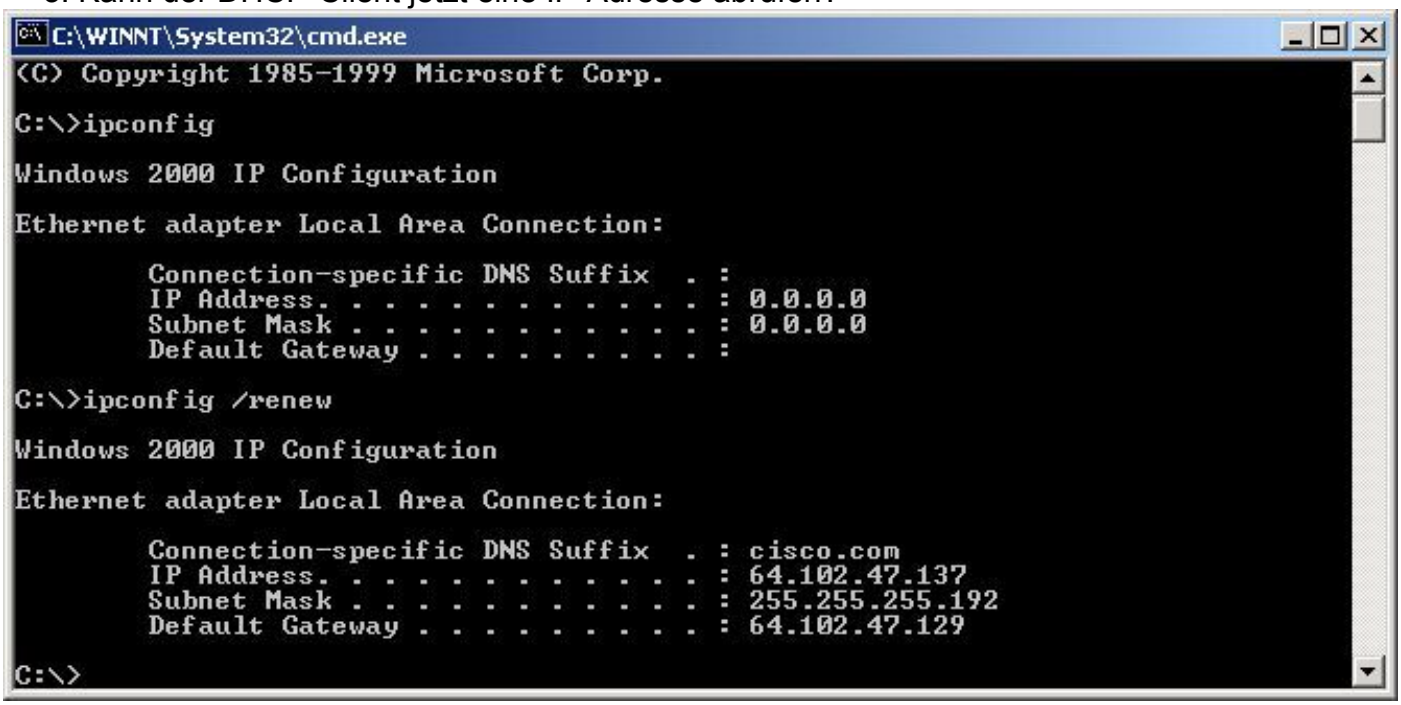
Microsoft Windows 95/98/ME:

1. Klicken Sie auf die Schaltfläche Start, und führen Sie das Programm WINIPCFG.exe aus.
2. Klicken Sie auf **die** Schaltfläche Alle **freigeben**, gefolgt von **der Schaltfläche** Alle **verlängern**.
3. Kann der DHCP-Client jetzt eine IP-Adresse abrufen?

Fenster "IP Configuration"

Microsoft Windows NT/2000:

1. Geben Sie cmdin **dasStart**/Runfield ein, um ein Eingabeaufforderungsfenster zu öffnen.
2. Geben Sie den Befehl **commandipconfig/**reneim Eingabeaufforderungsfenster ein.
3. Kann der DHCP-Client jetzt eine IP-Adresse abrufen?



Befehlszeilenaufforderung

Wenn der DHCP-Client nach Abschluss des Bootvorgangs eine IP-Adresse mit einer manuellen Erneuerung der IP-Adresse beziehen kann, handelt es sich höchstwahrscheinlich um ein DHCP-Startproblem. Wenn der DHCP-Client mit einem Cisco Catalyst Switch verbunden ist, liegt das Problem wahrscheinlich an einem Konfigurationsproblem, das STP-Portfast und/oder Channeling und Trunking betrifft. Weitere mögliche Probleme sind Netzwerkkarten- und Switch-Port-

Startprobleme. Gehen Sie die Schritte D und E durch, um Probleme mit Switch-Ports und NIC-Karten als Ursache des DHCP-Problems auszuschließen.

D. Überprüfen der Switch-Port-Konfiguration (STP PortFast und andere Befehle)

Wenn es sich bei dem Switch um einen Catalyst Switch der Serien 2900/4000/5000/6000 handelt, stellen Sie sicher, dass STP PortFast aktiviert und Trunking/Channeling deaktiviert ist. Die Standardkonfiguration ist "STP portfast disabled" (STP-Portfast deaktiviert) und "trunking/channeling auto" (Trunking/Channeling, falls zutreffend). Für die Switches der Serien 2900XL/3500XL/2950/3550 ist STP PortFast die einzige erforderliche Konfiguration. Diese Konfigurationsänderungen beheben die häufigsten DHCP-Client-Probleme, die bei der Erstinstallation eines Catalyst Switches auftreten.

Weitere Informationen zu den erforderlichen Konfigurationsanforderungen für den Switch-Port, damit DHCP ordnungsgemäß funktioniert, wenn eine Verbindung mit Catalyst-Switches hergestellt wird, finden Sie unter Verwenden von Portfast und anderen Befehlen zur Behebung von Verbindungsverzögerungen beim Starten von Workstations.

Nachdem Sie dieses Dokument gelesen haben, können Sie mit der Problembehebung fortfahren.

E. Überprüfen Sie, ob Probleme mit der Netzwerkkarte oder dem Catalyst Switch bekannt sind.

Wenn die Catalyst Switch-Konfiguration korrekt ist, kann es auf dem Catalyst Switch oder der DHCP-Client-NIC zu einem Problem mit der Softwarekompatibilität kommen, das zu DHCP-Problemen führen kann. Der nächste Schritt zur Fehlerbehebung besteht darin, die Fehlerbehebung bei Cisco Catalyst-Switches auf Kompatibilitätsprobleme mit Netzwerkkarten zu überprüfen und Softwareprobleme mit dem Catalyst-Switch oder der Netzwerkkarte, die zu dem Problem beitragen, auszuschließen.

Um Kompatibilitätsprobleme auszuschließen, sind Kenntnisse des DHCP-Client-Betriebssystems sowie spezifische NIC-Informationen wie Hersteller, Modell und Treiberversion erforderlich.

F. Unterscheiden Sie, ob DHCP-Clients IP-Adressen im gleichen Subnetz oder VLAN wie der DHCP-Server beziehen

Es muss unterschieden werden, ob DHCP korrekt funktioniert, wenn sich der Client im gleichen Subnetz oder VLAN wie der DHCP-Server befindet. Wenn DHCP im gleichen Subnetz oder VLAN wie der DHCP-Server ordnungsgemäß funktioniert, wird das DHCP-Problem hauptsächlich durch den DHCP/BootP Relay Agent verursacht. Wenn das Problem weiterhin besteht, auch wenn Sie DHCP auf demselben Subnetz oder VLAN wie den DHCP-Server testen, kann das Problem tatsächlich beim DHCP-Server liegen.

G. Überprüfen der DHCP/BootP-Relay-Konfiguration des Routers

So überprüfen Sie die Konfiguration:

1. Wenn Sie das DHCP-Relay auf einem Router konfigurieren, stellen Sie sicher, dass sich der Befehl **eip helper-**address auf der richtigen Schnittstelle befindet. **Der Befehl "eip helper-**address" muss an der Eingangsschnittstelle der DHCP-Client-Workstations vorhanden sein und an den richtigen DHCP-Server weitergeleitet werden.

2. Stellen Sie sicher, dass der globale Konfigurationsbefehl **no service** dhcpis nicht vorhanden ist. Dieser Konfigurationsparameter deaktiviert alle DHCP-Server- und Relay-Funktionen auf dem Router. Die Standardkonfiguration service dhcpwird nicht in der Konfiguration angezeigt und ist der Standardkonfigurationsbefehl. Wenn **der Dienst dhcp** nicht aktiviert ist, erhalten die Clients die IP-Adressen nicht vom DHCP-Server.**Anmerkung:** Auf Routern mit älteren Cisco IOS-Versionen übernimmt der Befehl **ip bootp server** die DHCP-Relay-Agent-Funktion anstelle des Befehls **service dhcp**. Aus diesem Grund muss der Befehl **ip bootp server** in diesen Routern aktiviert werden, wenn der Befehl **ip helper-address** so konfiguriert ist, dass er DHCP-UDP-Broadcasts weiterleitet und ordnungsgemäß als DHCP-Relay-Agent für den DHCP-Client fungiert.
3. Wenn Sie **ip helper-**address-Befehle verwenden, um UDP-Broadcasts an eine Subnetz-Broadcast-Adresse weiterzuleiten, stellen Sie sicher, dass no ip directed-broadcast ist nicht auf einer ausgehenden Schnittstelle konfiguriert, die von den UDP-Broadcast-Paketen durchlaufen werden muss. Die Fehlermeldung no ip directed-broadcast blockiert jede Übersetzung einer gerichteten Sendung in eine physische Sendung. Diese Schnittstellenkonfiguration ist die Standardkonfiguration in Softwareversion 12.0 und höher.
4. Wenn DHCP-Broadcasts an die Broadcast-Adresse des DHCP-Servers weitergeleitet werden, kann ein Softwareproblem auftreten. Wenn Sie DHCP-Probleme beheben, versuchen Sie, DHCP UDP-Broadcasts an die IP-Adresse des DHCP-Servers weiterzuleiten:

H. Aktivierung der Option "Subscriber Identification (82)"

Die Funktion DHCP Relay Agent Information (Option 82) ermöglicht es den DHCP Relay Agents (Catalyst Switches), Informationen über sich selbst und den angeschlossenen Client einzugeben, wenn DHCP Anfragen von einem DHCP Client an einen DHCP Server weitergeleitet werden.

Der DHCP-Server kann diese Informationen verwenden, um IP-Adressen zuzuweisen, die Zugriffskontrolle durchzuführen und Quality of Service (QoS)- und Sicherheitsrichtlinien (oder andere Parameterzuweisungsrichtlinien) für jeden Teilnehmer eines Service-Provider-Netzwerks festzulegen. Wenn DHCP-Snooping auf einem Switch aktiviert ist, wird Option 82 automatisch aktiviert. Wenn der DHCP-Server nicht für die Verarbeitung der Pakete mit Option 82 konfiguriert ist, wird die Adressenzuweisung für diese Anforderung beendet. Um dieses Problem zu beheben, deaktivieren Sie die Option zur Teilnehmerkennung (82) in den Switches (Relay Agents) mit dem globalen Konfigurationsbefehl,**no ip dhcp relay information**.

I. DHCP-Datenbank-Agent und DHCP-Konfliktprotokollierung

Ein DHCP-Datenbank-Agent ist ein beliebiger Host (z. B. ein FTP-, TFTP- oder RCP-Server), der die DHCP-Bindungsdatenbank speichert. Sie können mehrere DHCP-Datenbank-Agenten konfigurieren und für jeden Agenten das Intervall zwischen Datenbankaktualisierungen und -übertragungen konfigurieren. Verwenden Sie den Befehl **eip dhcp database**, um einen Datenbank-Agenten und Datenbank-Agent-Parameter zu konfigurieren.

Wenn Sie keinen DHCP-Datenbank-Agent konfigurieren, deaktivieren Sie die Aufzeichnung von DHCP-Adresskonflikten auf dem DHCP-Server. Führen Sie **den Befehl enoip dhcp conflict logging** aus, um die Protokollierung von DHCP-Adresskonflikten zu deaktivieren. Löschen Sie die zuvor protokollierten Konflikte **mit clear ip dhcp conflict**.

Wenn die Konfliktprotokollierung dadurch nicht deaktiviert wird, wird die folgende Fehlermeldung angezeigt:

```
%DHCPD-4-DECLINE_CONFLICT: DHCP address conflict: client
```

J. Überprüfen Sie CDP auf IP-Telefonverbindungen.

Wenn das Cisco Discovery Protocol (CDP) auf dem mit dem Cisco IP-Telefon verbundenen Switch-Port deaktiviert ist, kann der DHCP-Server dem Telefon keine geeignete IP-Adresse zuweisen. Der DHCP-Server weist tendenziell die IP-Adresse zu, die zum Daten-VLAN/Subnetz des Switch-Ports gehört. Wenn CDP aktiviert ist, kann der Switch erkennen, dass das Cisco IP-Telefon DHCP anfordert, und die richtigen Subnetzinformationen bereitstellen. Der DHCP-Server kann dann eine IP-Adresse aus dem Sprach-VLAN/Subnetz-Pool zuweisen. Es sind keine expliziten Schritte erforderlich, um den DHCP-Dienst an das Sprach-VLAN zu binden.

K. Entfernen - SVI unterbricht DHCP-Snooping-Vorgang

Auf den Cisco Catalyst Switches der Serie 6500 wird automatisch eine SVI (im deaktivierten Zustand) erstellt, nachdem sie DHCP so konfiguriert hat, dass Snoop für ein bestimmtes VLAN ausgeführt wird. Das Vorhandensein dieser SVI hat direkte Auswirkungen auf den ordnungsgemäßen Betrieb von DHCP-Snooping.

DHCP-Snooping wird auf den Cisco Catalyst Switches der Serie 6500 mit nativem Cisco IOS hauptsächlich auf dem Routingprozessor (RP oder MSFC) implementiert, nicht auf dem Switch Processor (SP oder Supervisor). Die Cisco Catalyst Serie 6500 fängt Pakete in Hardware mit VACLs ab, die die Pakete an eine vom RP abonnierte Local Target Logic (LTL) liefern. Sobald die Frames den RP erreichen, müssen sie zunächst einer L3-Schnittstellen (SVI)-IDB zugeordnet werden, bevor sie an den Snooping-Teil weitergegeben werden können. Ohne SVI ist diese IDB nicht vorhanden, und die Pakete werden im RP verworfen.

L. Eingeschränkte Broadcast-Adresse

Wenn ein DHCP-Client das Broadcast-Bit in einem DHCP-Paket festlegt, senden der DHCP-Server und der Relay-Agent DHCP-Nachrichten an Clients mit der Broadcast-Adresse aller Clients (255.255.255.255). Wenn der Befehl **eip broadcast-address** so konfiguriert wurde, dass ein Netzwerk-Broadcast gesendet wird, wird der von DHCP gesendete All-One-Broadcast überschrieben. Um dieses Problem zu beheben, verwenden Sie den Befehl **eip dhcp limited-broadcast-address,** um sicherzustellen, dass ein konfigurierter Netzwerk-Broadcast das standardmäßige DHCP-Verhalten nicht außer Kraft setzt.

Einige DHCP-Clients können nur eine All-One-Übertragung akzeptieren und können keine DHCP-Adresse abrufen, es sei denn, dieser Befehl wird auf der mit dem Client verbundenen Router-Schnittstelle konfiguriert.

M. Debuggen von DHCP mit Router-Debugbefehlen

Überprüfen, ob der Router eine DHCP-Anforderung mit Debug-Befehlen empfängt

Auf Routern, die Software unterstützen, die DHCP-Pakete verarbeitet, können Sie überprüfen, ob ein Router die DHCP-Anfrage vom Client erhält. Der DHCP-Prozess schlägt fehl, wenn der Router keine Anfragen vom Client erhält. Konfigurieren Sie in diesem Schritt eine Zugriffsliste, um die Ausgabe zu debuggen. Diese Zugriffsliste wird nur zum Debuggen eines Befehls verwendet und hat keinen Einfluss auf den Router.

Geben Sie im globalen Konfigurationsmodus die folgende Zugriffsliste ein:

access-list 100 permit ip host 0,0.0,0 host 255.255.255.255

Geben Sie im exec-Modus den folgenden Debugbefehl ein:

debug ip packet detail 100

Beispiel für das Ergebnis

```
Router#debug ip packet detail 100
IP packet debugging is on (detailed) for access list 100
Router#
00:16:46: IP: s=0.0.0.0 (Ethernet4/0), d=255.255.255.255, len 604, rcvd 2
00:16:46: UDP src=68, dst=67
00:16:46: IP: s=0.0.0.0 (Ethernet4/0), d=255.255.255.255, len 604, rcvd 2
00:16:46: UDP src=68, dst=67
```

Aus diesem Beispiel geht klar hervor, dass der Router die DHCP-Anfragen aktiv vom Client empfängt. Diese Ausgabe zeigt nur eine Zusammenfassung des Pakets und nicht das Paket selbst. Daher kann nicht festgestellt werden, ob das Paket korrekt ist. Dennoch erhielt der Router ein Broadcast-Paket mit der Quell- und Ziel-IP- und UDP-Ports, die für DHCP richtig sind.

Überprüfen, ob der Router eine DHCP-Anforderung mit dem Befehl debug ip udp empfängt und weiterleitet

Der Befehl **debug ip udp** verfolgt den Pfad einer DHCP-Anforderung über einen Router. In einer Produktionsumgebung ist dieses Debugging jedoch aufdringlich, da alle verarbeiteten Switched-UDP-Pakete in der Konsole angezeigt werden. Dieser Debug-Befehl darf nicht in der Produktion verwendet werden.

> **Warnung:** Der Befehl **debug ip udp** ist aufdringlich und kann eine hohe CPU-Auslastung verursachen.

Geben Sie im exec-Modus den folgenden Debug-Befehl ein: **debug ip udp**

Beispiel für das Ergebnis

```
Router#debug ip udp
UDP packet debugging is on
Router#

00:18:48: UDP: rcvd src=0.0.0.0(68), dst=255.255.255.255(67), length=584

!--- Router receiving DHCPDISCOVER from DHCP client.

00:18:48: UDP: sent src=192.168.1.1(67), dst=192.168.2.2(67), length=604

!--- Router forwarding DHCPDISCOVER unicast to DHCP server using DHCP/BootP Relay Agent source
IP address.

00:18:48: UDP: rcvd src=192.168.2.2(67), dst=192.168.1.1(67), length=313
```

```
!--- Router receiving DHCPOFFER from DHCP server directed to DHCP/BootP Relay Agent IP address.

00:18:48: UDP: sent src=0.0.0.0(67), dst=255.255.255.255(68), length=333

!--- Router forwarding DHCPOFFER from DHCP server to DHCP client via DHCP/BootP Relay Agent.

00:18:48: UDP: rcvd src=0.0.0.0(68), dst=255.255.255.255(67), length=584

!--- Router receiving DHCPREQUEST from DHCP client.

00:18:48: UDP: sent src=192.168.1.1(67), dst=192.168.2.2(67), length=604

!--- Router forwarding DHCPDISCOVER unicast to DHCP server using DHCP/BootP Relay Agent source
IP address.

00:18:48: UDP: rcvd src=192.168.2.2(67), dst=192.168.1.1(67), length=313

!--- Router receiving DHCPACK (or DHCPNAK) from DHCP directed to DHCP/BootP Relay Agent IP
address.

00:18:48: UDP: sent src=0.0.0.0(67), dst=255.255.255.255(68), length=333

!--- Router forwarding DHCPACK (or DHCPNAK) to DHCP client via DHCP/BootP Relay Agent.

00:18:48: UDP: rcvd src=192.168.1.2(520), dst=255.255.255.255(520), length=32

!--- DHCP client verifying IP address not in use by sending ARP request for its own IP address.

00:18:50: UDP: rcvd src=192.168.1.2(520), dst=255.255.255.255(520), length=32

!--- DHCP client verifying IP address not in use by sending ARP request for its own IP address.
```

Überprüfen, ob der Router eine DHCP-Anforderung mit debug ip dhcp server packet command empfängt und weiterleitet

Wenn der Router Cisco IOS 12.0.x.T oder 12.1 ist und die DHCP-Serverfunktionalität von Cisco IOS unterstützt, können Sie den Befehl **debug ip dhcp server packet** verwenden. Dieses Debugging wurde zur Verwendung mit der IOS DHCP-Serverfunktion und zur Fehlerbehebung bei der DHCP/BootP Relay Agent-Funktion konzipiert. Wie bei den vorherigen Schritten können Router-Fehlerbehebungen das Problem nicht genau ermitteln, da das tatsächliche Paket nicht angezeigt werden kann. Debugging erlaubt jedoch Rückschlüsse auf die DHCP-Verarbeitung. Geben Sie im EXEC-Modus den folgenden Debugging-Befehl ein:

debug ip dhcp server paket

```
Router#debug ip dhcp server packet
00:20:54: DHCPD: setting giaddr to 192.168.1.1.

!--- Router received DHCPDISCOVER/REQUEST/INRORM and setting Gateway IP address to 192.168.1.1
for forwarding.

00:20:54: DHCPD: BOOTREQUEST from 0063.6973.636f.2d30.3065.302e.3165.6632.2e63..

!--- BOOTREQUEST includes DHCPDISCOVER, DHCPREQUEST, and DHCPINFORM.


!--- 0063.6973.636f.2d30.3065.302e.3165.6632.2e63 indicates client identifier.
```

```
00:20:54: DHCPD: forwarding BOOTREPLY to client 00e0.1ef2.c441.

!--- BOOTREPLY includes DHCPOFFER and DHCPNAK.


!--- Client's MAC address is 00e0.1ef2.c441.

00:20:54: DHCPD: broadcasting BOOTREPLY to client 00e0.1ef2.c441.

!--- Router is forwarding DHCPOFFER or DHCPNAK broadcast on local LAN interface.

00:20:54: DHCPD: setting giaddr to 192.168.1.1.

!--- Router received DHCPDISCOVER/REQUEST/INFORM and set Gateway IP address to 192.168.1.1 for
forwarding.

00:20:54: DHCPD: BOOTREQUEST from 0063.6973.636f.2d30.3065.302e.3165.6632.2e63..

!--- BOOTREQUEST includes DHCPDISCOVER, DHCPREQUEST, and DHCPINFORM.


!--- 0063.6973.636f.2d30.3065.302e.3165.6632.2e63 indicates client identifier.

00:20:54: DHCPD: forwarding BOOTREPLY to client 00e0.1ef2.c441.

!--- BOOTREPLY includes DHCPOFFER and DHCPNAK.


!--- Client's MAC address is 00e0.1ef2.c441.

00:20:54: DHCPD: broadcasting BOOTREPLY to client 00e0.1ef2.c441.

!--- Router is forwarding DHCPOFFER or DHCPNAK broadcast on local LAN interface.
```

Gleichzeitige Ausführung mehrerer Debugs

Wenn Sie mehrere Debug-Vorgänge gleichzeitig ausführen, kann eine ausreichende Menge an Informationen über den Betrieb des DHCP/BootP-Relay-Agenten und des Servers ermittelt werden. Wenn Sie die vorherigen Konturen für die Fehlerbehebung verwenden, können Sie Rückschlüsse darauf ziehen, wo die Funktionalität des DHCP/BootP-Relay-Agents nicht ordnungsgemäß funktioniert.

```
IP: s=0.0.0.0 (Ethernet0), d=255.255.255.255, len 604, rcvd 2
UDP src=68, dst=67
UDP: rcvd src=0.0.0.0(68), dst=255.255.255.255(67), length=584
DHCPD: setting giaddr to 192.168.1.1.
UDP: sent src=192.168.1.1(67), dst=192.168.2.2(67), length=604
IP: s=192.168.1.1 (local), d=192.168.2.2 (Ethernet1), len 604, sending
UDP src=67, dst=67
DHCPD: BOOTREQUEST from 0063.6973.636f.2d30.3030.302e.3030.3030.2e30.3030.312d.4574.30 forwarded
to 192.168.2.2.
IP: s=192.168.2.2 (Ethernet1), d=192.168.1.1, len 328, rcvd 4
UDP src=67, dst=67
UDP: rcvd src=192.168.2.2(67), dst=192.168.1.1(67), length=308
DHCPD: forwarding BOOTREPLY to client 0000.0000.0001.
DHCPD: broadcasting BOOTREPLY to client 0000.0000.0001.
UDP: sent src=0.0.0.0(67), dst=255.255.255.255(68), length=328
IP: s=0.0.0.0 (Ethernet0), d=255.255.255.255, len 604, rcvd 2
UDP src=68, dst=67
```

```
UDP: rcvd src=0.0.0.0(68), dst=255.255.255.255(67), length=584
DHCPD: setting giaddr to 192.168.1.1.
UDP: sent src=192.168.1.1(67), dst=192.168.2.2(67), length=604
IP: s=192.168.1.1 (local), d=192.168.2.2 (Ethernet1), len 604, sending
UDP src=67, dst=67
DHCPD: BOOTREQUEST from 0063.6973.636f.2d30.3030.302e.3030.3030.2e30.3030.312d.4574.30 forwarded
to 192.168.2.2.
IP: s=192.168.2.2 (Ethernet1), d=192.168.1.1, len 328, rcvd 4
UDP src=67, dst=67
UDP: rcvd src=192.168.2.2(67), dst=192.168.1.1(67), length=308
DHCPD: forwarding BOOTREPLY to client 0000.0000.0001.
DHCPD: broadcasting BOOTREPLY to client 0000.0000.0001.
UDP: sent src=0.0.0.0(67), dst=255.255.255.255(68), length=328.
```

Abruf von Sniffer-Trace und Ermittlung der Ursache des DHCP-Problems

Überprüfen Sie die Dekodierungs-Sniffer-Spur von DHCP-Client und -Server auf demselben LAN-Segment und die Dekodierungs-Sniffer-Spur von DHCP-Client und -Server getrennt durch einen Router, der als DHCP-Relay-Agent konfiguriert ist, Abschnitte

um DHCP-Paket-Traces zu entschlüsseln.

Informationen zum Abrufen von Sniffer-Traces mit der SPAN-Funktion (Switched Port Analyzer) auf Catalyst-Switches finden Sie unter Konfigurieren des SPAN-Konfigurationsbeispiels (Catalyst Switched Port Analyzer).

Alternative Methode der Paketdekodierung mit Debuggen auf dem Router

Mit dem Befehl **debug ip packet detail dump <acl>** auf einem Cisco Router kann ein ganzes Paket in Hex im Systemprotokoll oder in der Befehlszeilenschnittstelle (CLI) angezeigt werden. Überprüfen Sie den AbschnittVerify Router Receives DHCP Request with debug CommandsVerify Router Receives DHCP Request and Forwards Request to DHCP Server with debug CommandsSection (DHCP-Anforderung mit Debug-Befehlen empfangen) mit dem zur Zugriffsliste hinzugefügten Schlüsselwort dump, um dieselben Debuginformationen zu erhalten, jedoch mit den Paketdetails in Hex. Um den Inhalt des Pakets zu bestimmen, muss das Paket übersetzt werden. Ein Beispiel ist Anhang A zu entnehmen.

Anhang A: Cisco IOS - DHCP-Beispielkonfiguration

Die DHCP-Server-Datenbank ist als Baumstruktur organisiert. Der Stamm der Struktur ist der Adresspool für natürliche Netzwerke, Zweigstellen sind Subnetz-Adresspools und Blätter sind manuelle Bindungen an Clients. Subnetzwerke übernehmen Netzwerkparameter, und Clients übernehmen Subnetzwerkparameter. Daher müssen gemeinsame Parameter, z.B. der Domänenname, auf der höchsten Ebene (Netzwerk oder Subnetz) des Trees konfiguriert werden.

Weitere Informationen zur Konfiguration von DHCP und den zugehörigen Befehlen finden Sie in der DHCP Configuration Task List (DHCP-Konfigurationsaufgabenliste).

```
version 12.1
!
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router
```

```
!
enable password cisco
ip subnet-zero
no ip domain-lookup
ip dhcp excluded-address 10.10.1.1 10.10.1.199

!--- Address range excluded from DHCP pools.

ip dhcp pool test_dhcp

!--- DHCP pool (scope) name is test_dhcp.

network 10.10.1.0 255.255.255.0

!--- DHCP pool (address will be assigned in this range) for associated Gateway IP address.

default-router 10.10.1.1

!--- DHCP option for default gateway.

dns-server 10.30.1.1

!--- DHCP option for DNS server(s).

netbios-name-server 10.40.1.1

!--- DHCP option for NetBIOS name server(s) (WINS).

lease 0 0 1

!--- Lease time.

interface Ethernet0
description DHCP Client Network
ip address 10.10.1.1 255.255.255.0
no ip directed-broadcast
!
interface Ethernet1
description Server Network
ip address 10.10.2.1 255.255.255.0
no ip directed-broadcast
!
line con 0
transport input none
line aux 0
transport input all
line vty 0 4
login
!
end
```

Zugehörige Informationen

- Tools und Ressourcen
- Technischer Support – Cisco Systems

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.