Probleemoplossing voor Dynamic Host Configuration Protocol in Catalyst Switch- of ondernemingsnetwerken

Inhoud

Inleiding

Dit document beschrijft hoe u problemen kunt oplossen met Dynamic Host Configuration Protocol (DHCP) in een Cisco Catalyst switch-netwerk.

Voorwaarden

Vereisten

Er zijn geen specifieke voorwaarden van toepassing op dit document.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Opmerking: Alleen geregistreerde Cisco-clients hebben toegang tot interne bugrapporten.

Achtergrondinformatie

DHCP biedt een mechanisme waardoor computers die Transmission Control Protocol/Internet Protocol (TCP/IP) gebruiken, automatisch protocolconfiguratieparameters kunnen verkrijgen via het netwerk. DHCP is een open standaard die is ontwikkeld door de Dynamic Host Configuration-Working Group (DHC-WG) van de Internet Engineering Task Force (IETF).

DHCP is gebaseerd op een paradigma voor clientservers, waarin de DHCP-client, bijvoorbeeld een desktopcomputer, contact opneemt met een DHCP-server voor configuratieparameters. De DHCP-server bevindt zich doorgaans centraal en wordt beheerd door de netwerkbeheerder. Omdat de server wordt uitgevoerd door een netwerkbeheerder, kunnen DHCP-clients betrouwbaar en dynamisch worden geconfigureerd met parameters die geschikt zijn voor de huidige netwerkarchitectuur.

De meeste ondernemingsnetwerken bestaan uit meerdere subnetwerken die in subnetwerken zijn verdeeld die als virtuele LAN's (VLAN's) worden aangeduid, waar routers tussen de subnetwerken routeren. Aangezien routers geen uitzendingen door gebrek overgaan, zou een server van DHCP op elke Subnet worden vereist tenzij de routers worden gevormd om de uitzending van DHCP met de eigenschap van de Agent van DHCP Relay door te sturen.

Belangrijke concepten

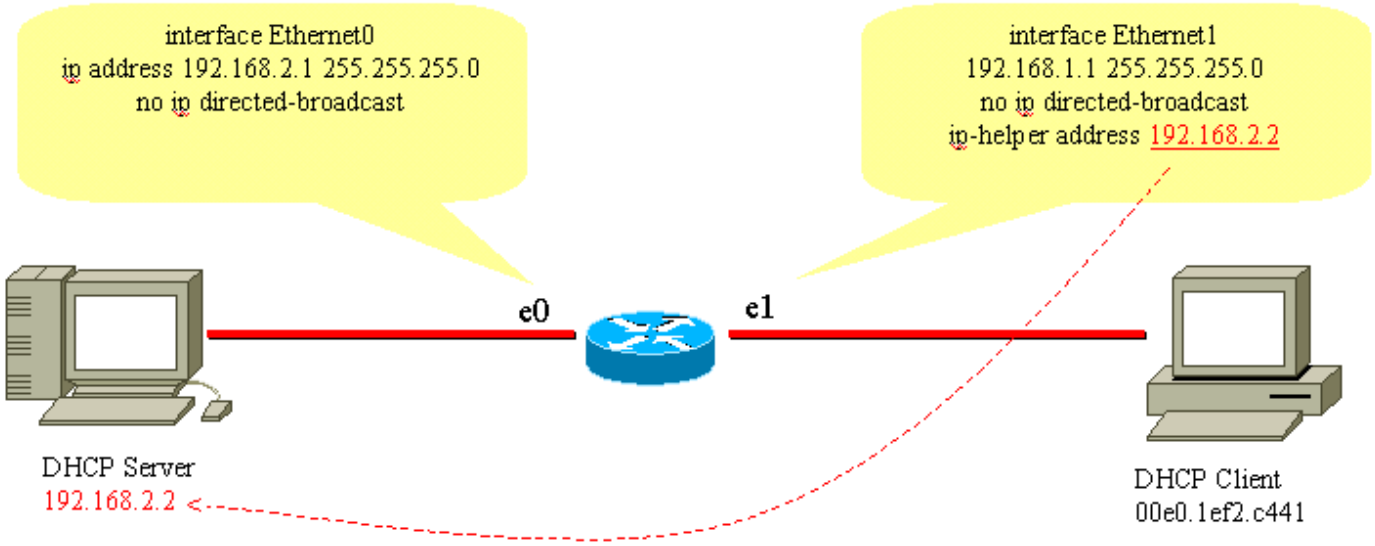
Dit zijn verschillende sleutelconcepten van DHCP:

- DHCP-clients hebben aanvankelijk geen geconfigureerd IP-adres en moeten daarom een uitzendverzoek verzenden om een IP-adres te verkrijgen van een DHCP-server.
- Routers sturen normaal gesproken geen uitzendingen door. Het is noodzakelijk om client-DHCP uitzendingsverzoeken aan te passen als de DHCP-server op een ander uitzenddomein (Layer 3 (L3) netwerk) is. Dit wordt uitgevoerd door gebruik van een DHCP Relay Agent.
- De Cisco router-implementatie van DHCP Relay wordt geleverd door opdrachten voor **IP-helper** op interfaceniveau

Voorbeeldscenario's

Scenario 1: Cisco router-routing tussen DHCP-client- en servernetwerken

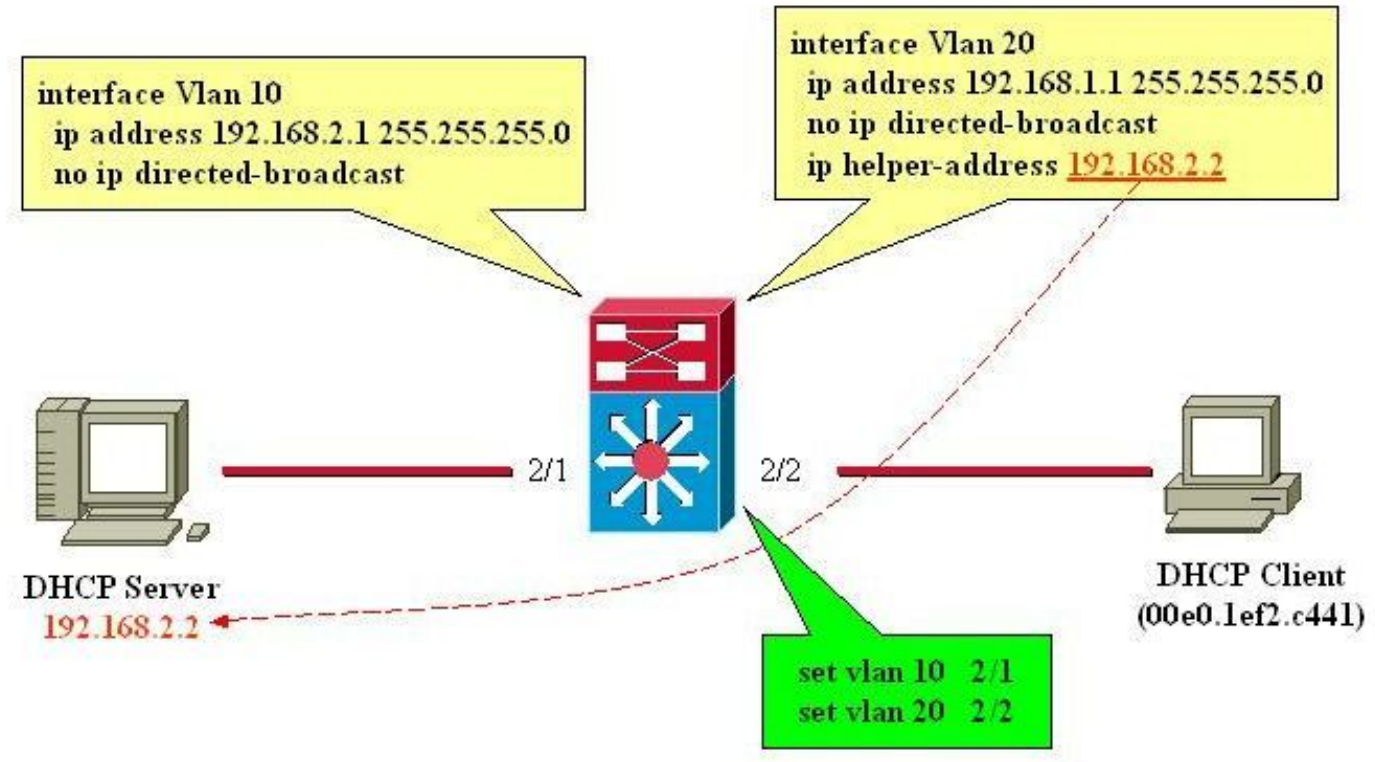
Zoals geconfigureerd in dit diagram, stuurt interface Ethernet1 de client via interface Ethernet1 door naar 192.168.2.2 via interface Ethernet1. De DHCP-server voldoet aan het verzoek via unicast. Geen verdere configuratie aan de router is noodzakelijk in dit voorbeeld.



Routing tussen DHCP-client- en servernetwerken

Scenario 2: Cisco Catalyst Switch met L3-module voor routing tussen DHCP-client- en servernetwerken

Zoals in het diagram is geconfigureerd, wordt met interface VLAN20 de client via interface VLAN10 doorgegeven aan 192.168.2.2. De DHCP-server voldoet aan het verzoek via unicast. Geen verdere configuratie aan de router is noodzakelijk in dit voorbeeld. De switch-poorten moeten als host-poorten worden geconfigureerd en STP-poortfast (Spanning-Tree Protocol) is ingeschakeld, en trunking en kanalisatie zijn uitgeschakeld.



L3-modulerouter tussen DHCP-client- en servernetwerken

DHCP begrijpen

DHCP is oorspronkelijk gedefinieerd in Requirements for Comments (RFCs) 1531 en is sindsdien

achterhaald door RFC 2131. DHCP is gebaseerd op het Bootstrap Protocol (BootP), dat is gedefinieerd in RFC 951.

DHCP wordt gebruikt door werkstations (hosts) om eerste configuratie-informatie te verkrijgen, zoals een IP-adres, subnetmasker en standaardgateway bij opstarten. Met DHCP hoeft u niet elke host handmatig te configureren met een IP-adres. Bovendien, als een host naar een andere IP-subnetserver verplaatst, moet het een ander IP-adres gebruiken dan het adres dat eerder werd gebruikt. DHCP zorgt automatisch voor dit. Het staat de host toe om een IP-adres te kiezen in het juiste IP-netwerk.

Huidige DHCP RFC-referenties

- RFC 2131 - DHCP
- RFC 2132 - DHCP-opties en BootP-uitbreidingen
- RFC 1534 - Interoperation tussen DHCP en BootP
- RFC 1542 - Verduidelijkingen en uitbreidingen voor de BootP
- RFC 2241 - DHCP-opties voor Novell Directory Services
- RFC 2242 - Netware/IP-domeinnaam en -informatie
- RFC 2489 - procedure voor het definiëren van nieuwe DHCP-opties

DHCP gebruikt een client-server model waarbij een of meer servers (DHCP-servers) IP-adressen en andere optionele configuratieparameters toewijzen aan clients (hosts) bij het opstarten van de client. Deze configuratieparameters worden door de server aan de client geleased voor een bepaalde tijd. Wanneer een host opstart, stuurt de TCP/IP stack in de host een uitzending (DHCPDiscover) bericht om een IP-adres en subnetmasker te verkrijgen, naast andere configuratieparameters. Dit initieert een uitwisseling tussen de DHCP-server en de host. Tijdens deze uitwisseling, gaat de cliënt door deze duidelijk gedefinieerde staten:

1. Initialiseren
2. Selecteren
3. Verzoeken
4. gebonden
5. Verlengen
6. herbinding

Om zich tussen deze staten te bewegen, kunnen de cliënt en de server de types van berichten ruilen die in de Lijst van het DHCP- Bericht worden vermeld.

DHCP-berichttabel

Referentie	Bericht	Beschrijving
0x01	DHCPDiscover	De client zoekt beschikbare DHCP-servers.
0x02	DHCPOFFER	De serverreactie op de client DHCPDiscover.
0x03	DHCPREQUEST	De client zendt uit naar de server, verzoeken boden parameters aan van één ser zoals specifiek gedefinieerd in het pakket.
0x04	DHCPDECLINE	De client-to-server communicatie geeft aan dat het netwerkadres al in gebruik is.
0x05	DHCPACK	De server-to-client communicatie met configuratieparameters, samen met een geëngageerd netwerkadres.

0x06	DHCPNAK	De server-to-client communicatie, weigert het verzoek om configuratie paramete
0x07	DHCPRELEASE	De client-to-server communicatie, geeft netwerkadres op en annuleert de rest lea
0x08	DHCPINFORMATION	De client-naar-server communicatie vraagt alleen om lokale configuratieparamet die de client al extern als adres heeft geconfigureerd.

DHCPDiscover

Wanneer een client voor het eerst opstart, wordt gezegd dat deze zich in de initialiserende staat bevindt, en wordt een DHCPDiscover-bericht verzonden op de lokale fysieke subnetserver via User Datagram Protocol (UDP) poort 67 (BootP-server). Aangezien de client geen manier heeft om het subnet te kennen waartoe het behoort, is de DHCPDiscover een uitzending van alle subnetten (IP-adres van bestemming van 255.255.255.255), met een IP-adres van de bron van 0.0.0.0. Het IP-adres van de bron is 0.0.0.0 aangezien de client geen geconfigureerd IP-adres heeft. Als een DHCP-server op dit lokale subnetnummer bestaat en correct is geconfigureerd en werkt, hoort de DHCP-server de uitzending en reageert met een DHCP-bericht. Als een DHCP-server niet bestaat op het lokale subnet, moet er een DHCP/BootP Relay Agent zijn op dit lokale subnet om het DHCPDiscover-bericht door te sturen naar een subnet dat een DHCP-server bevat.

Deze relay-agent kan een speciale host (bijvoorbeeld Microsoft Windows Server) of een router zijn (bijvoorbeeld een Cisco-router die is geconfigureerd met IP-helperinstructies op interfaceniveau).

DHCPOFFER

Een DHCP-server die een DHCPDiscover-bericht ontvangt, kan reageren met een DHCP-bericht op UDP-poort 68 (BootP-client). De client ontvangt de DHCPOFFER en beweegt zich naar de selectiestatus. Dit DHCP-bericht bevat informatie over de eerste configuratie van de client. De DHCP-server vult bijvoorbeeld het opleververveld van het DHCP-bericht in met het gevraagde IP-adres. Het subnetmasker en de standaardgateway worden respectievelijk gespecificeerd in het optieveld, subnetmasker en routeropties. Andere veelgebruikte opties in het DHCPOFFER-bericht zijn IP-adresleasetijd, vernieuwingstijd, domeinnaamserver en NetBIOS-naamserver (WINS). De DHCP-server verstuurt de DHCPOFFER naar het uitzendadres, maar bevat het adres van de client-hardware in het veld Kaarten van het aanbod, zodat de client weet dat het de beoogde bestemming is. In het geval dat de DHCP-server niet op het lokale subnet staat, stuurt de DHCP-server de DHCPcffer, als unicastpakket, op UDP-poort 67, terug naar de DHCP/BootP Relay Agent waar de DHCPDiscover vandaan kwam. De DHCP/BootP Relay Agent zendt vervolgens de DHCP/BootP Relay Agent uit of unicast de DHCPOFFER op het lokale subnetwerkknooppunt op UDP-poort 68, die afhankelijk is van de Broadcast-vlag die is ingesteld door de Boop-client.

DHCPREQUEST

Nadat de client een DHCPOFFER ontvangt, reageert het met een DHCPREQUEST-bericht en geeft aan dat de client de parameters in de DHCPOFFER wil accepteren en naar de Verzoekende staat wil gaan. De client kan meerdere DHCP-berichten ontvangen, één van elke DHCP-server die het oorspronkelijke DHCP-Discover-bericht heeft ontvangen. De client kiest een DHCPOFFER en reageert alleen op die DHCP-server en, impliciet, weigert alle andere DHCPOFFER berichten. De client identificeert de geselecteerde server nadat deze het optieveld Server Identifier heeft

ingevuld met het IP-adres van de DHCP-server. De DHCPREQUEST is ook een uitzending, zodat alle DHCP-servers die een DHCPOFFER verstuurden de DHCPREQUEST zien, en elk weet of zijn DHCPOFFER werd geaccepteerd of geweigerd. Alle aanvullende configuratieopties die de client vereist zijn opgenomen in het optieveld van het DHCPREQUEST-bericht. Hoewel de klant een IP-adres is aangeboden, wordt het DHCPREQUEST-bericht met een IP-bronadres van 0,0.0.0 verzonden. Op dit moment heeft de klant nog geen verificatie ontvangen dat het duidelijk is om het IP-adres te gebruiken.

DHCPACK

Nadat de DHCP-server de DHCPREQUEST ontvangt, erkent het het verzoek met een DHCP-bericht en voltooit vervolgens het initialisatieproces. Het DHCP-bericht heeft een IP-bronadres van de DHCP-server en het doeladres is opnieuw een broadcast en bevat alle parameters die de client heeft gevraagd in het DHCP-bericht. Wanneer de client de DHCPACK ontvangt, komt het in de Bound-staat en is nu vrij om het IP-adres te gebruiken om op het netwerk te communiceren. Ondertussen slaat de DHCP-server de lease op in zijn database en identificeert deze op unieke wijze met de client identifier of het algoritme en het bijbehorende IP-adres. Zowel de client als de server gebruiken deze combinatie van identificatoren om naar de lease te verwijzen. De client identifier is het MAC-adres van het apparaat plus het mediatype.

Alvorens de DHCP-client het nieuwe adres begint te gebruiken, moet de DHCP-client de tijdparameters berekenen die aan een geleasd adres zijn gekoppeld, namelijk huurtijd (LT), verversingstijd (T1) en rebind-tijd (T2). De standaard LT is 72 uur. U kunt kortere leasetijden gebruiken om adressen te besparen, indien nodig.

DHCPNAK

Als de geselecteerde server het DHCPREQUEST bericht niet kan vervullen, reageert de DHCP server met een DHCPNAK bericht. Wanneer de client een DHCPNAK-bericht ontvangt of geen antwoord ontvangt op een DHCPREQUEST-bericht, start de client het configuratieproces opnieuw op wanneer het naar de Verzoekende staat gaat. De client zendt de DHCPREQUEST minstens vier keer opnieuw uit binnen 60 seconden voordat de initialiserende status wordt herstart.

DHCPDECLINE

De klant ontvangt de DHCPACK en voert naar keuze een laatste controle uit op de parameters. De client voert deze procedure uit wanneer de ARP-verzoeken (Address Resolution Protocol) voor het in de DHCPACK opgegeven IP-adres worden verzonden. Als de client detecteert dat het adres al in gebruik is wanneer het een antwoord op het ARP-verzoek ontvangt, stuurt de client een DHCPDECLINE-bericht naar de server en start het configuratieproces opnieuw in de Verzoekende staat.

DHCPINFORMATION

Als een client op een andere manier een netwerkadres heeft verkregen of een handmatig ingesteld IP-adres heeft, kan een client werkstation een DHCPINFORMATION-verzoekbericht gebruiken om andere lokale configuratieparameters te verkrijgen, zoals de domeinnaam en Domeinnaamservers (DNS's). Wanneer DHCP-servers een DHCPINFORMATION-bericht ontvangen, moet u een DHCP-bericht samenstellen met de lokale configuratieparameters die geschikt zijn voor de client zonder een nieuw IP-adres. Deze DHCPACK wordt unicast naar de klant gestuurd.

DHCPRELEASE

Een DHCP-client kan ervoor kiezen om de lease op een netwerkadres op te geven wanneer een DHCP-persbericht naar de DHCP-server wordt verzonden. De klant identificeert de leaseovereenkomst die moet worden vrijgegeven door het gebruik van `het` veld `client` en het netwerkadres in het DHCPRELEASE-bericht. Als u het huidige bereik van de DHCP-pool wilt uitbreiden, verwijdert u de huidige pool van adressen en specificeert u het nieuwe bereik van IP-adressen onder de DHCP-pool. Om specifieke IP-adressen of een reeks adressen die u in de DHCP-pool wilt plaatsen te verwijderen, gebruikt u het **uitgesloten-adres** van de opdracht **ip DHCP**.

> **Opmerking:** Als apparaten BOOTP gebruiken, worden de oneindige lengteleases getoond in de banden van DHCP van routers.

De lease-overeenkomst verlengen

Aangezien het IP-adres alleen van de server wordt geleased, moet de lease van tijd tot tijd worden verlengd. Wanneer de helft van de leasetijd is verlopen (T1=0.5 x LT), probeert de client de leaseovereenkomst te verlengen. De client voert de status Vernieuwen in en stuurt een DHCPREQUEST bericht naar de server, die de huidige lease houdt. De server reageert op het verzoek om te vernieuwen met een DHCPACK bericht als het akkoord gaat om de huurovereenkomst te verlengen. Het DHCPACK-bericht bevat de nieuwe lease en eventuele nieuwe configuratieparameters, in het geval dat eventuele wijzigingen in de server tijdens de vorige lease worden aangebracht. Als de client de server niet kan bereiken wanneer hij de lease om een of andere reden heeft, probeert hij het adres van een DHCP-server te verlengen nadat de oorspronkelijke DHCP-server niet binnen een tijd T2 op de verlengingsverzoeken heeft gereageerd. De standaardwaarde van T2 is (7/8 x LT). Dit betekent T1 < T2< LT.

Als de client eerder een door DHCP toegewezen IP-adres had en opnieuw is opgestart, vraagt de client specifiek het eerder geleasede IP-adres in een DHCPREQUEST-pakket. Deze DHCPREQUEST heeft nog steeds het IP-adres van de bron zoals 0.0.0.0 en de bestemming als IP-uitzendadres 255.255.255.255.

Wanneer een client tijdens de herstart een DHCPREQUEST verstuurt, mag deze niet het veld voor het serveridentificatiekenmerk invullen en moet deze in plaats daarvan het opgevraagde veld voor het IP-adres invullen. Alleen RFC-conforme clients vullen het veld met het gevraagde adres in plaats van het veld DHCP-optie. De DHCP-server accepteert beide methoden. Het gedrag van de DHCP-server hangt af van een aantal factoren, zoals in het geval van Windows NT DHCP-servers, de versie van het systeem dat wordt gebruikt, en andere factoren, zoals superscoping. Als de DHCP-server bepaalt dat de client nog steeds het gevraagde IP-adres kan gebruiken, blijft het stil of stuurt een DHCPACK voor de DHCPREQUEST. Als de server bepaalt dat de client het gevraagde IP-adres niet kan gebruiken, wordt een DHCPNACK teruggestuurd naar de client. De client gaat dan naar de initialiserende staat en verstuurt een DHCPDiscover-bericht.

> **Opmerking:** De DHCP-server wijst het onderste IP-adres uit een pool van IP-adressen toe aan de DHCP-clients. Wanneer de lease van het onderste adres verloopt, wordt het toegewezen aan een andere client als het wordt aangevraagd. U kunt geen wijzigingen aanbrengen in de volgorde DHCP-adressen worden toegewezen.

DHCP-pakkettabel

Het DHCP-bericht heeft een variabele lengte en bestaat uit velden in de DHCP-pakkettabel.

Opmerking: Dit pakket is een aangepaste versie van het oorspronkelijke BootP-pakket.

Veld	Bytes	Name	Beschrijving
bovenwerk	1	Opcode	Identificeert het pakket als verzoek of antwoord: 1=BOOTREQUEST, 2=BOOTREPLIEK
type	1	Type hardware	Specificeert het adrestype van de netwerkhardware.
heuveltje	1	Hardware lengte	Specificeert de lengte van het hardwareadres.
hop	1	hop	De client stelt de waarde in op nul en de waarde wordt verhoogd als het verzoek wordt doorgestuurd via een router.
xid	4	Transactie-ID	Een willekeurig getal dat door de klant wordt gekozen. Alle DHCP-berichten die voor een bepaalde DHCP-transactie worden uitgewisseld, gebruiken de ID (xid).
seconden	2	seconden	Specificeert het aantal seconden sinds het DHCP-proces is gestart.
vlaggen	2	Vlaggen	Geeft aan of het bericht broadcast of unicast is.
cidderen	4	IP-adres van client	Alleen gebruikt wanneer de client zijn IP-adres kent, zoals in het geval van de status Bound, Renew of Rebinding.
opbrengen	4	Uw IP-adres	Als het IP-adres van de client 0.0.0 is, wordt het aangeboden IP-adres van de client in dit veld geplaatst door de DHCP-server.
zuster	4	IP-adres voor servers	Als de client het IP-adres van de DHCP-server kent, wordt in dit veld het DHCP-serveradres ingevuld. Anders, wordt het gebruikt in DHCPOFFER en DHCP van DHCP server.
schepper	4	IP-adres router (GI ADDR)	Het IP-adres van de gateway, ingevuld door de DHCP/BootP Relay Agent.
charmeren	16	MAC-adres client	Het MAC-adres van de DHCP-client.
naam	64	Servernaam	De optionele serverhostnaam.
indienen	128	Naam opstartbestand	De naam van het opstartbestand.
opties	veranderlijk	Optieparameters	De optionele parameters die kunnen worden geleverd door de DHCP-server. RFC 2132 biedt alle mogelijke opties.

Client-Server Conversation voor client die DHCP-adres verkrijgt waar client en DHCP-server op hetzelfde subnet verblijven

PacketDescription	MAC-bronadapter	MAC-adres van bestemming	IP-bronadres	IP-adres voor bestemmi
DHCPDiscover	Klant	uitzenden	0.0.0.0	255.255.255.255
DHCPOFFER	DHCP-server	uitzenden	DHCP-server	255.255.255.255
DHCPREQUEST	Klant	uitzenden	0.0.0.0	255.255.255.255
DHCPACK	DHCP-server	uitzenden	DHCP-server	255.255.255.255

Rol van DHCP/BootP Relay Agent

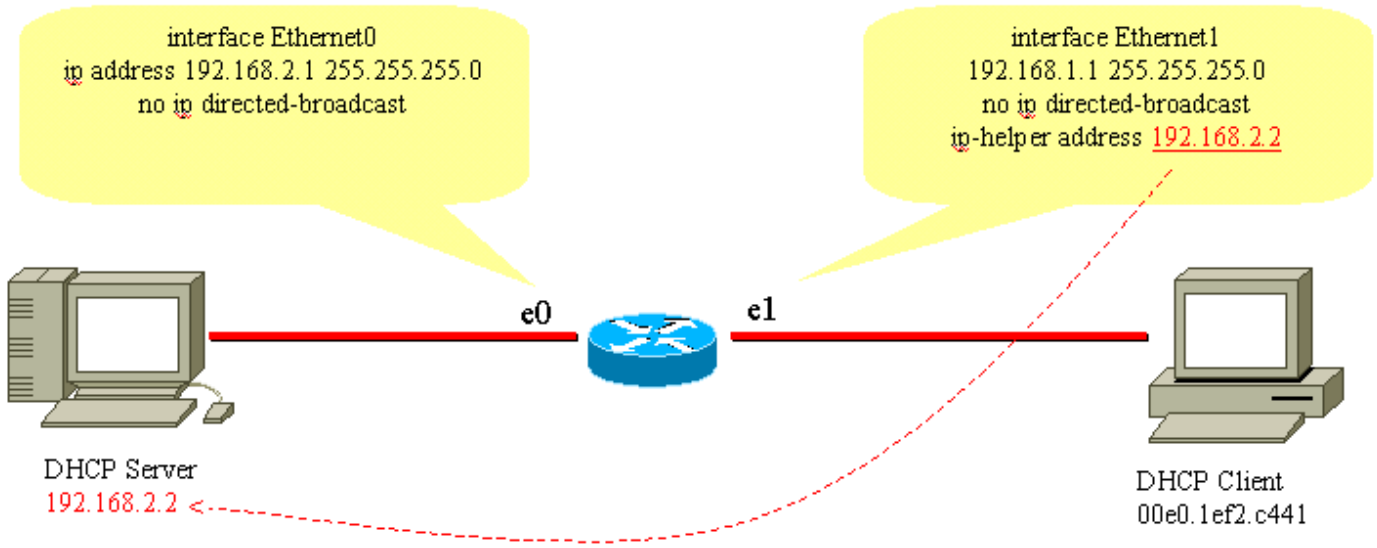
De routers, door gebrek, door:sturen geen pakketten door. Aangezien DHCP-clientberichten het IP-adres van de bestemming van 25.255.255.255 (All Net Broadcast) gebruiken, kunnen DHCP-clients geen verzoeken verzenden naar een DHCP-server op een andere subnetserver, tenzij de DHCP/BootP Relay Agent op de router is geconfigureerd. De DHCP/BootP Relay Agent verstuurt

DHCP-verzoeken namens een DHCP-client naar de DHCP-server. De DHCP/BootP Relay Agent voegt zijn eigen IP-adres toe aan het IP-bronadres van de DHCP-frames die naar de DHCP-server gaan. Hierdoor kan de DHCP-server via unicast reageren op de DHCP/BootP Relay Agent. De DHCP/BootP Relay Agent vult het IP-adresveld van de gateway ook met het IP-adres van de interface waarop het DHCP-bericht van de client wordt ontvangen. De DHCP-server gebruikt het IP-adresveld van de gateway om te bepalen van welke subnetbron het bericht DHCPDiscover, DHCPREQUEST of DHCPINFORMATION afkomstig is.

DHCP/BootP Relay Agent-functie configureren op Cisco IOS® router

Het proces voor het configureren van een Cisco-router voor het doorsturen van BootP- of DHCP-verzoeken is eenvoudig. U hoeft alleen maar een IP-helper-adres te configureren dat verwijst naar de DHCP/BootP-server of naar het subnetuitzendadres van het netwerk waarop de server is ingeschakeld.

Netwerkvoorbeeld:



DHCP/BootP Relay Agent

Om het BootP/DHCP-verzoek van de client naar de DHCP-server door te sturen, wordt **de opdracht helper-address interface** gebruikt. Het IP-helperadres kan worden geconfigureerd om elke UDP-uitzending te doorsturen op basis van het UDP-poortnummer. Standaard worden deze UDP-uitzendingen op het IP-helperadres doorgestuurd:

- Trivial File Transfer Protocol (TFTP) (poort 69)
- DNS (poort 53), tijdservice (poort 37)
- NetBIOS-naamserver (poort 137)
- NetBIOS datagramserver (poort 138)
- Opstartprotocol (DHCP/BootP) client- en serverdatagrammen (poorten 67 en 68)
- Terminal Access Control Access Control System (TACACS)-service (poort 49)
- IENS-16-naamservice (poort 42)

IP-helperadressen kunnen UDP-uitzendingen naar een unicast leiden of IP-adres uitzenden. Gebruik het IP-helperadres echter niet om UDP-uitzendingen van het ene subnetadres naar het

uitzendadres van een ander subnetnummer door te sturen, vanwege de grote hoeveelheid uitzendoverstromingen die kunnen optreden. Meervoudige IP-helperadresgegevens op één interface worden ook ondersteund:

```
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-routers ondersteunen geen taakverdeling van DHCP-servers die als DHCP Relay Agents zijn geconfigureerd. Cisco-routers sturen het DHCPDiscover-bericht door naar alle helperadressen die voor die interface worden vermeld. Het gebruik van twee of meer DHCP-servers om een subnetverbinding te bedienen, verhoogt alleen het DHCP-verkeer omdat de DHCPDiscover-, DHCPOFFER- en DHCPREQUEST-/DHCPDECLINE-berichten worden uitgewisseld tussen elk paar DHCP-client en -server.

Handmatige banden instellen

Er zijn twee manieren om handmatige bindingen op te zetten; een is voor de Windows-host, en de andere is voor niet-Windows-hosts. Er zijn twee verschillende opdrachten die worden gebruikt om te configureren. een voor Microsoft DHCP-clients, en de andere voor niet-Microsoft DHCP-clients: **DHCPclient-identifier** (handmatige binding - Microsoft DHCP-clients) **en DHCPhardware-adres** (handmatige binding - niet-Microsoft DHCP-clients). De reden voor twee verschillende opdrachten is dat een pc die met Windows werkt, zijn MAC's wijzigt, en een **01** wordt toegevoegd aan het begin van het adres. Dit zijn de voorbeeldconfiguraties:

- Dit is een configuratie voor Microsoft DHCP-clients:

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

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

- Dit is een configuratie voor niet-Microsoft DHCP-clients:

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

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

DHCP gebruiken voor secundaire IP-segmenten

Standaard heeft DHCP een beperking in die zin dat de antwoordpakketten alleen worden verzonden als het verzoek wordt ontvangen van de interface die met het primaire IP-adres is geconfigureerd. DHCP-verkeer gebruikt het uitzendadres. Wanneer het DHCP-verzoek door de routerinterface wordt ontvangen, wordt het doorgestuurd naar de DHCP-server (wanneer het IP-helperadres is geconfigureerd) met een bronadres van het primaire IP dat op de interface is geconfigureerd om de DHCP-server te laten weten welke IP-pool het moet gebruiken (voor de client) in het DHCP-antwoordpakket.

Er is geen manier voor de router om te weten als het DHCP uitzendingsverzoek van een apparaat komt dat op het secundaire IP netwerk is dat op de interface wordt gevormd. Als tijdelijke oplossing kunnen subinterfaceconfiguraties (mits het apparaat dat is aangesloten op de router dot1q-tagging ondersteunt) om de twee subnetten te scheiden worden geconfigureerd, zodat beide hun correspondent IP-adressen goed krijgen.

Als het secundaire adres de aangewezen manier is, is er een andere tijdelijke oplossing, die de globale configuratie **commandip dhcp smart-relay** moet toelaten. Dit heeft een beperking in die zin dat het alleen het secundaire IP gebruikt om het DHCP-verzoek door te geven als er geen reactie is van de DHCP-server na drie opeenvolgende verzoeken voor de primaire adrespool.

DHCP-clientservergesprek met DHCP Relay-functie

De volgende tabel toont het proces voor een DHCP-client om een IP-adres te verkrijgen van een DHCP-server. Deze tabel is gemodelleerd naar het vorige configuratienetwerkdiagram van de DHCP/BootP Relay Agent. Elke numerieke waarde in het diagram vertegenwoordigt een pakket dat in deze volgende tabel wordt beschreven. Gebruik deze tabel om de pakketstroom van DHCP-clientservergesprekken te begrijpen. Het helpt je ook om te bepalen waar problemen zich voordoen.

Proces voor een DHCP-client om een IP-adres te verkrijgen

Packet	IP-adres van client	IP-adres voor servers	GI-adres	MAC-adres pakketbron	IP-pakketbronadres	MAC- pakke
1. DHCPDiscover wordt verzonden van de klant.	0.0.0.0	0.0.0.0	0.0.0.0	005.DC9.C640	0.0.0.0	ffff.ffff. (uitzer
2. De router ontvangt de DHCPDiscover op de	0.0.0.0	0.0.0.0	192.168.1.1	Interface E2 MAC-adres	192.168.1.1	MAC- DHCP

E1-interface. De router herkent dat dit pakket een DHCP UDP-uitzending is. De router fungeert nu als DHCP/BootP Relay Agent en vult het veld Gateway IP-adres in met het inkomende IP-adres van de interface, wijzigt het IP-adres van de bron in een inkomend IP-adres van de interface en stuurt het verzoek rechtstreeks door naar de DHCP-server.						
3. De DHCP-server heeft de DHCP-ONTDEKKING ontvangen en stuurt een DHCP-filter naar de DHCP Relay Agent.	192.168.1.2	192.168.2.2	192.168.1.1	MAC-adres van DHCP-server	192.168.2.2	Interfa adres
4. De DHCP Relay Agent ontvangt een DHCPOFFER en verstuurt de DHCPOFFER-uitzending via het lokale LAN.	192.168.1.2	192.168.2.2	192.168.1.1	Interface E1 MAC-adres	192.168.1.1	ffff.ffff (uitzer
5. DHCPREQUEST verzonden van klant.	0.0.0.0	0.0.0.0	0.0.0.0	005.DC9.C640	0.0.0.0	ffff.ffff (uitzer
6. De router ontvangt de DHCPREQUEST op de E1-interface. De router herkent dat dit pakket DHCP UDP broadcast is. De router fungeert nu als DHCP Relay Agent en vult het IP-adresveld van de gateway in met het verzonden IP-interfaceadres, wijzigt het IP-bronadres in een inkomend IP-adres van de interface en stuurt het verzoek rechtstreeks door naar de DHCP-server.	0.0.0.0	0.0.0.0	192.168.1.1	Interface E2 MAC-adres	192.168.1.1	MAC-a DHCP
7. De DHCP-server heeft de DHCP CPREQUEST ontvangen en stuurt een DHCP-computer naar de DHCP/BootP Relay Agent.	192.168.1.2	192.168.2.2	192.168.1.1	MAC-adres van DHCP-server	192.168.2.2	Interfa adres

8. De DHCP/BootP Relay Agent ontvangt de DHCP-aansluiting en verstuurt de DHCP-uitzending via het lokale LAN. De client accepteert de ACK en gebruikt het IP-adres van de client.	192.168.1.2	192.168.2.2	192.168.1.1	Interface E1 MAC-adres	192.168.1.1	ffff.ffff. (uitzen

DHCP-overwegingen bij opstarten van Pre-Execution Environment (PXE)

Pre-Execution Environment (PXE) maakt het mogelijk dat een werkstation wordt opgestart vanaf een server op een netwerk voordat het systeem op de lokale harde schijf wordt opgestart. Een netwerkbeheerder hoeft het specifieke werkstation niet fysiek te bezoeken en handmatig te starten. OS en andere software, zoals diagnostische programma's, kunnen vanaf een server via het netwerk op het apparaat worden geladen. PXE-omgeving gebruikt DHCP om zijn IP-adres te configureren.

De configuratie van de DHCP/BootP Relay Agent moet op de router worden uitgevoerd als de DHCP-server zich op een ander gerouteerd segment van het netwerk bevindt. **Het ip helper-adres** bevel op de lokale routerinterface moet worden gevormd. Raadpleeg de optie DHCP/BootP Relay Agent configureren op de sectie Cisco IOS Routerin dit document voor informatie over de configuratie.

DHCP begrijpen en problemen oplossen met snuffelsporen

Sniffer-tracering van DHCP-client en -server op hetzelfde LAN-segment decoderen

Netwerktopologie waarbij DHCP-client en server op hetzelfde LAN-segment verblijven

Het voorbeeld van het snuffelspoor bestaat uit zes frames. Deze zes frames illustreren een scenario waarin de DHCP-client en -server zich op hetzelfde fysieke of logische segment bevinden. Gebruik het volgende codevoorbeeld om DHCP op te lossen. Het is belangrijk om uw snuifspoor aan de sporen in dit voorbeeld aan te passen. Er kunnen enkele verschillen zijn in vergelijking met de volgende geïllustreerde sporen, maar de algemene pakketstroom moet precies hetzelfde zijn. Het pakketspoor volgt eerdere discussies over hoe DHCP werkt.

```
- - - - - - - - - - - - - - - - - - - - - - - - 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:
```

Sniffer-overtrek van DHCP-client en -server decoderen, gescheiden door een router die is geconfigureerd als DHCP Relay Agent

Sniffer-B-spoor

```
- - - - - - - - - - - - - - - - - - - - - - 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-spoor

```
- - - - - - - - - - - - - - - - - - - - - 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:
```

DHCP oplossen wanneer clientwerkstations geen DHCP-adressen kunnen verkrijgen

Casestudy 1: DHCP-server op hetzelfde LAN-segment of VLAN als DHCP-client

Wanneer de DHCP-server en -client zich op hetzelfde LAN-segment of VLAN bevinden en de client geen IP-adres kan verkrijgen van een DHCP-server. Maar het is onwaarschijnlijk dat de lokale router een DHCP-probleem veroorzaakt. Het probleem heeft betrekking op de apparaten die verbinding maken met de DHCP-server en de DHCP-client. Het probleem kan echter bij de DHCP-server of client zelf liggen. Deze modules helpen bij probleemoplossing en bepalen welk apparaat een probleem veroorzaakt.

> **Opmerking:** Als u de DHCP-server per VLAN wilt configureren, definieert u verschillende DHCP-pools voor elk VLAN dat DHCP-adressen aan uw clients levert.

Casestudy 2: DHCP-server en DHCP-client worden gescheiden door een router die is geconfigureerd voor DHCP/BootP Relay Agent-functionaliteit

Wanneer de DHCP-server en de client zich op de verschillende LAN-segmenten of VLAN's bevinden, functioneert de router als DHCP/BootP Relay Agent die verantwoordelijk is voor het

doorsturen van de DHCP CPREQUEST naar de DHCP-server. Er zijn extra stappen nodig om problemen met de DHCP/BootP Relay Agent en met de DHCP-server en -client op te lossen. Als u deze modules volgt, kunt u bepalen welk apparaat de problemen veroorzaakt.

DHCP-server op router faalt om adressen toe te wijzen met een POLO EXHAUSTED Error

Het is mogelijk dat sommige adressen nog steeds worden gehouden door klanten, zelfs als ze uit de pool worden vrijgegeven. Dit kan worden geverifieerd door **de manier waarop ip dhcp** conflictoutput. Een adresconflict komt voor wanneer twee hosts hetzelfde IP-adres gebruiken. Bij de adrestoewijzing, controleert DHCP conflicten met ping en onnodige ARP.

Als een conflict wordt gedetecteerd, wordt het adres uit de pool verwijderd. Het adres wordt toegewezen tot de beheerder het conflict oplost. **Configuratie van IP DHCP-**logboekregistratie om dit probleem op te lossen.

DHCP-probleemoplossingsmodules

Begrijpen waar DHCP-problemen kunnen optreden

DHCP-problemen kunnen om vele redenen optreden. De meest voorkomende redenen zijn configuratieproblemen. Veel DHCP-problemen kunnen echter worden veroorzaakt door softwaredefecten in systemen, Network Interface Card (NIC)-stuurprogramma's of DHCP/BootP Relay Agents die op routers worden uitgevoerd. Gezien het aantal potentieel problematische gebieden is een systematische benadering van probleemoplossing vereist.

Korte lijst met mogelijke oorzaken van DHCP-problemen:

- Standaardconfiguratie Catalyst switch
- Configuratie DHCP/BootP Relay Agent
- NIC-compatibiliteitsprobleem of DHCP-functieprobleem
- Defecte NIC of onjuiste installatie van NIC-stuurprogramma
- Intermitterende netwerkstroomonderbrekingen als gevolg van frequente overspannende boomberekeningen
- Besturingssysteemgedrag of softwaredefect
- DHCP-servertoepassingsconfiguratie of softwaredefect
- Cisco Catalyst switch voor Cisco IOS DHCP/BootP Relay Agent-softwaredefect
- Unicast Reverse Path Forwarding (uRPF) controleert het mislukken omdat het DHCP-aanbod op een andere interface wordt ontvangen dan verwacht. Wanneer de functie Reverse Path Forwarding (RPF) op een interface is ingeschakeld, kan een Cisco-router Dynamic Host Configuration Protocol (DHCP) en BOOTP-pakketten (BOOTP) met bronadressen van 0,0.0.0 en doeladressen van 255.255.255.255.255 laten vallen. De router kan ook alle IP-pakketten laten vallen die een multicast IP-bestemming op de interface hebben. Dit probleem is gedocumenteerd in Cisco bug-id CSCdw31925

Opmerking: alleen geregistreerde Cisco-clients hebben toegang tot bugrapporten.

- DHCP-databaseagent wordt niet gebruikt, maar DHCP-conflictvastlegging is niet uitgeschakeld

A. Controleer de fysieke connectiviteit

Deze procedure is van toepassing op alle casestudy's.

Controleer eerst de fysieke verbinding van een DHCP-client en -server. Indien aangesloten op een Catalyst switch, controleer dan of zowel de DHCP-client als de server fysiek verbonden zijn. Voor Cisco IOS-gebaseerde switches zoals Catalyst 2900XL/3500XL/2950/3550, dient u de **juiste** opdracht te geven om de **poortstatusinterface <interface> te tonen**. Als de status van de interface iets anders is dan <`interface`> omhoog is, is het lijnprotocol omhoog, gaat de poort geen verkeer over, zelfs niet DHCP-clientverzoeken. De uitvoer van de opdrachten:

```
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)
```

Als de fysieke verbinding is geverifieerd en er inderdaad geen link is tussen de Catalyst switch en DHCP-client, gebruikt u de sectie Problemen oplossen met Cisco Catalyst-Switches voor NIC-compatibiliteitsproblemen om problemen met de fysieke laagconnectiviteit op te lossen.

Door buitensporige datalink-fouten kunnen poorten op bepaalde Catalyst-switches in een niet-compatibele toestand terechtkomen. Raadpleeg voor meer informatie de optie Poortstatus uitschakelen op de Cisco IOS-platforms, waarin de status van de storing wordt beschreven, wordt uitgelegd hoe u ervan kunt herstellen en worden voorbeelden van herstel van deze status gegeven.

B. Het clientwerkstation en de statische IP configureren om de netwerkconnectiviteit te testen

Deze procedure is van toepassing op alle casestudy's.

Wanneer u problemen met DHCP oplost, is het belangrijk om een statisch IP-adres op een clientwerkstation te configureren om de netwerkconnectiviteit te verifiëren. Als het werkstation niet in staat is netwerkbronnen te bereiken ondanks het feit dat het een statisch geconfigureerd IP-adres heeft, is de basisoorzaak van het probleem niet DHCP. Op dit punt moet u problemen oplossen met de netwerkverbinding.

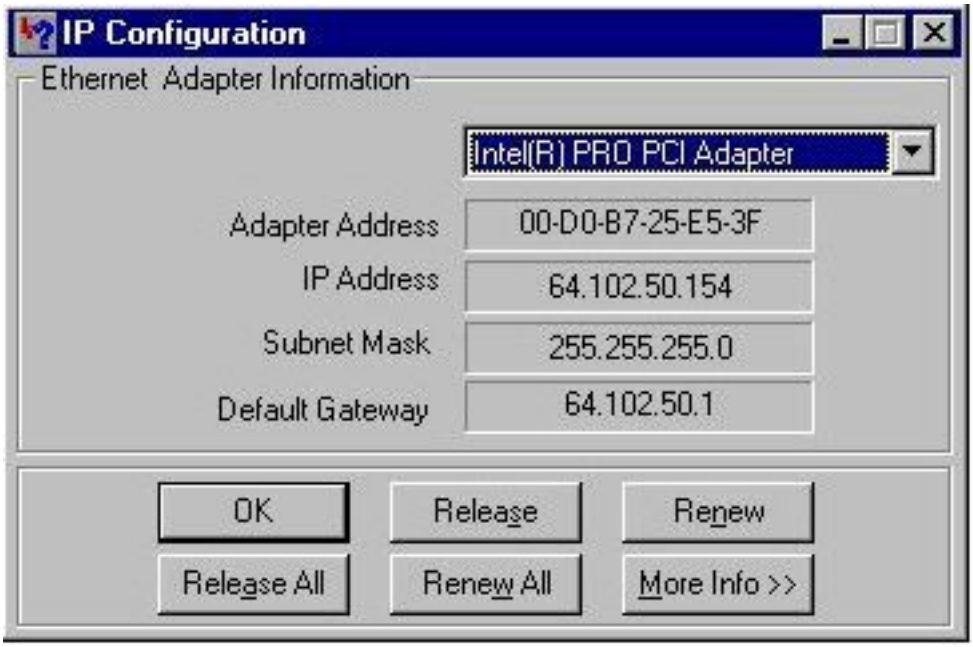
C. Controleer het probleem als opstartprobleem

Deze procedure is van toepassing op alle casestudy's.

Als de DHCP-client bij het opstarten geen IP-adres van de DHCP-server kan verkrijgen, kunt u de client handmatig dwingen een DHCP-verzoek te verzenden. Geef de volgende stappen uit om handmatig een IP-adres te verkrijgen van een DHCP-server voor het genoemde besturingssysteem.

Microsoft Windows 95/98/ME:

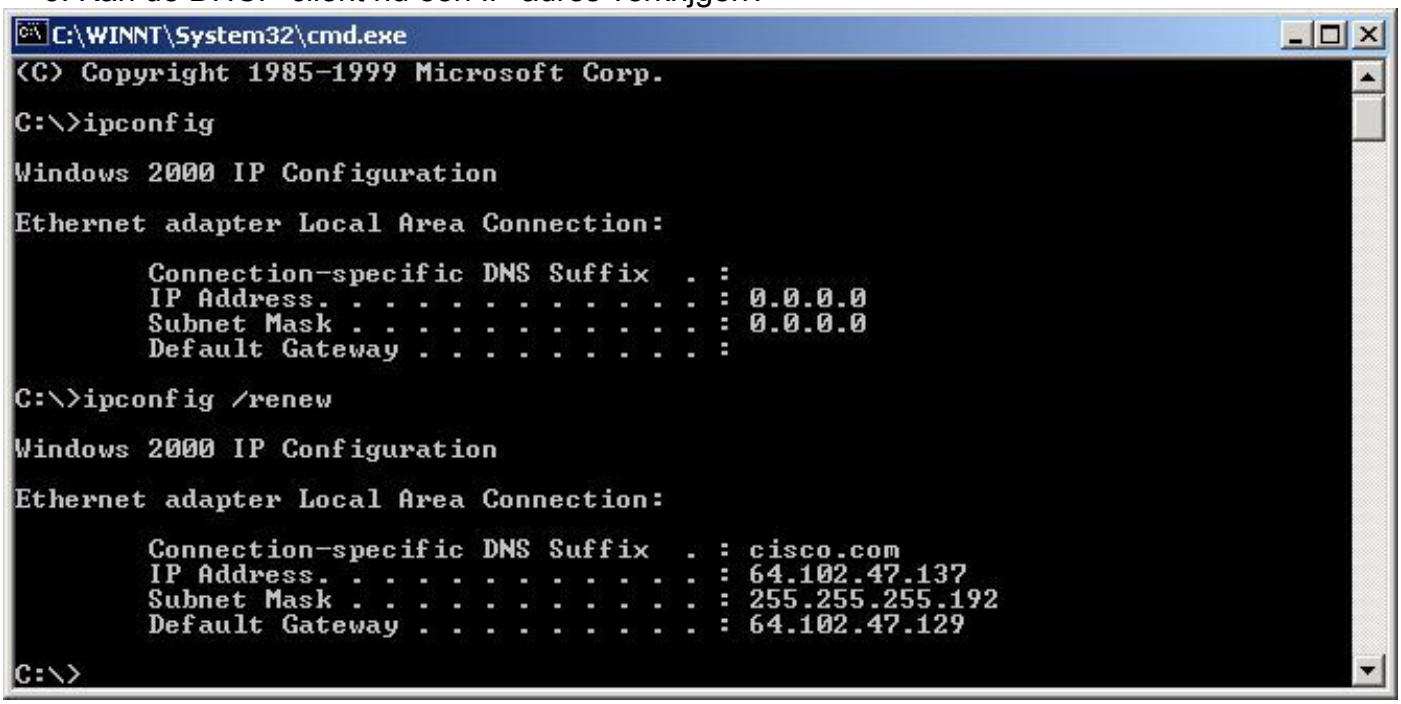
1. Klik op de knop Start en voer het programma WINIPCFG.exe uit.
2. Klik op **de knop** Alles **vrijgeven**, gevolgd door **de knop** Verlengen.
3. Kan de DHCP-client nu een IP-adres verkrijgen?



IP-configuratievenster

Microsoft Windows NT/2000:

1. Voer cmdin **hetStart/**Runfield in om een opdrachtprompt venster te openen.
2. Geef het **commandipconfig/**renewin het opdrachtprompt venster uit.
3. Kan de DHCP-client nu een IP-adres verkrijgen?



Vragen over opdrachtregel

Als de DHCP-client een IP-adres kan verkrijgen met een handmatige vernieuwing van het IP-adres nadat de pc het opstartproces heeft voltooid, is het probleem waarschijnlijk een DHCP-opstartprobleem. Als de DHCP-client is aangesloten op een Cisco Catalyst switch, is het probleem waarschijnlijk het gevolg van een configuratieprobleem dat STP-portfast en/of -kanalisatie en trunking behandelt. Andere mogelijkheden zijn onder meer problemen met de NIC-kaart en problemen met het opstarten van switch-poorten. ReviewStappen D en E om switch poortconfiguratie en NIC kaartproblemen uit te sluiten als de basisoorzaak van het DHCP-probleem.

D. Controleer de poortconfiguratie van de Switch (STP Portfast en andere opdrachten)

Als de switch een Catalyst 2900/4000/5000/6000 is, controleert u of STP-poortfast is ingeschakeld en trunking/kanalisatie is uitgeschakeld. De standaardconfiguratie is STP portfast uitgeschakeld en trunking/kanalisatie auto, indien van toepassing. Voor de 2900XL/3500XL/2950/3550 switches is STP portfast de enige vereiste configuratie. Deze configuratieveranderingen lossen de meest voorkomende DHCP-clientproblemen op die zich voordoen bij een eerste installatie van een Catalyst switch.

Raadpleeg Gebruik Portfast en andere opdrachten om vertragingen bij het opstarten van het werkstation te repareren voor meer informatie over de benodigde configuratievereisten voor de switch switch -poortconfiguratie waardoor DHCP bij een verbinding met Catalyst correct kan werken.

Nadat u dat document hebt bekeken, kunt u deze kwesties blijven oplossen.

E. Controleer op bekende problemen met NIC-kaart of Catalyst Switch

Als de Catalyst switch-configuratie juist is, is het mogelijk dat er een probleem is met de softwarecompatibiliteit op de Catalyst switch of DHCP-client-NIC die de DHCP-problemen kan veroorzaken. De volgende stap bij het oplossen van problemen is het bekijken van Problemen met Cisco Catalyst-Switches voor NIC-compatibiliteitsproblemen en het uitsluiten van softwareproblemen met de Catalyst switch of NIC die tot het probleem bijdragen.

Kennis van het DHCP-client-OS en specifieke NIC-informatie zoals de fabrikant, het model en de driver-versie is nodig om compatibiliteitsproblemen op de juiste manier uit te sluiten.

F. Onderscheid of DHCP-clients IP-adres verkrijgen op hetzelfde subnet of VLAN als DHCP-server

Het is belangrijk om te onderscheiden of DHCP al dan niet correct functioneert wanneer de client zich op dezelfde subnetverbinding of VLAN bevindt als de DHCP-server. Als de DHCP correct aan hetzelfde Subnet of VLAN werkt als de DHCP-server, wordt de DHCP-kwestie meestal veroorzaakt door de DHCP/BootP Relay Agent. Als het probleem blijft bestaan, zelfs wanneer u DHCP test op hetzelfde subnetje of VLAN als de DHCP-server, kan het probleem met de DHCP-server zijn.

G. Controleer de configuratie van de router DHCP/BootP Relay

Zo verifieert u de configuratie:

1. Wanneer u het DHCP-relay op een router vormt, controleert u of **de helper-**addressopdracht zich op de juiste interface bevindt. **Het ip helper-**addresscommando moet aanwezig zijn op de inkomende interface van de DHCP-client werkstations en moet naar de juiste DHCP-server worden geleid.
2. Controleer dat de globale configuratie **commandopost** niet aanwezig is. Deze configuratieparameter schakelt alle DHCP-server en relay functionaliteit op de router uit. De standaardconfiguratie, service dhcpverschijnt niet in de configuratie en is de standaardconfiguratieopdracht. Als **de Service DHCP** niet is ingeschakeld, ontvangen de clients de IP-adressen niet van de DHCP-server.**Opmerking:** In routers die oudere Cisco IOS-releases uitvoeren, verwerkt de opdracht **ip-bootserver** de functie DHCP Relay Agent in plaats van de opdracht **Service DHCP**. Wegens dit, moet het bevel van de **ip bootp server** in

deze routers worden toegelaten als het **ip helper-adres** bevel wordt gevormd om de uitzendingen van DHCP UDP door te sturen en behoorlijk als DHCP relay agent namens de cliënt van DHCP te handelen.

3. Wanneer u **ip helper-**addresscommando's gebruikt om UDP-uitzendingen door te sturen naar een subnetuitzendadres, controleert u of no ip directed-broadcast is niet ingesteld op enige uitgaande interface waarop de UDP-uitzendpakketten moeten worden doorgestuurd. Het no ip directed-broadcast blokkeert elke vertaling van een gerichte uitzending in fysieke uitzendingen. Deze interfaceconfiguratie is de standaardconfiguratie in softwareversies 12.0 en hoger.
4. Wanneer DHCP-uitzendingen worden doorgestuurd naar het uitzendadres van de DHCP-serversubnetserver kan er een softwareprobleem ontstaan. Wanneer u problemen met DHCP oplost, probeert u DHCP UDP-uitzendingen door te sturen naar het IP-adres van de DHCP-server:

H. Subscriber Identification (82) optie ingeschakeld

De voorziening DHCP Relay Agent Information (optie 82) stelt de DHCP Relay Agents (Catalyst switches) in staat om informatie over zichzelf en de aangesloten client op te nemen wanneer DHCP-verzoeken van een DHCP-client naar een DHCP-server worden doorgestuurd.

De DHCP-server kan deze informatie gebruiken om IP-adressen toe te wijzen, toegangscontrole uit te voeren en QoS-kwaliteit (Quality of Service) en beveiligingsbeleid (of ander beleid voor parametertoewijzing) in te stellen voor elke abonnee van een serviceprovider-netwerk. Wanneer DHCP-snuffelen is ingeschakeld op een switch, wordt optie 82 automatisch ingeschakeld. Als de DHCP-server niet is geconfigureerd om de pakketten met optie 82 te verwerken, wordt het adres niet meer toegewezen aan dat verzoek. Om dit probleem op te lossen, schakelt u de optie voor de identificatie van de abonnee (82) in de switches (relay agents) uit met de opdracht voor de globale configuratie, **geen optie voor informatie over de IP DHCP-relay**.

I. DHCP Database Agent en vastlegging van DHCP-conflicten

Een DHCP-databaseagent is een willekeurige host—bijvoorbeeld een FTP-, TFTP- of RCP-server—waarmee de DHCP-bindingsdatabase wordt opgeslagen. U kunt meerdere DHCP database agents configureren en u kunt het interval tussen database updates en overdrachten voor elke agent configureren. Gebruik **het dhcp database** commando om een database agent en database agent parameters te configureren.

Als u ervoor kiest geen DHCP-databaseagent te configureren, schakelt u de opname van DHCP-adresconflicten op de DHCP-server uit. Voer **de opdracht logboekregistratie bij DHCP-conflict uit** om de logboekregistratie bij DHCP-adresconflict uit te schakelen. Wis de eerder geregistreerde conflicten **met duidelijk ip DHCP-conflict**.

Als dit er niet in slaagt om het conflict registreren uit te schakelen, verschijnt deze foutmelding:

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

J. Controleer CDP voor verbindingen met IP-telefoon

Wanneer de switchpoort die is aangesloten op de Cisco IP-telefoon Cisco Discovery Protocol (CDP) heeft uitgeschakeld, kan de DHCP-server geen geschikt IP-adres aan de telefoon toewijzen. De DHCP-server heeft de neiging het IP-adres toe te wijzen dat tot de gegevens VLAN

/ subnett van de switchpoort behoort. Als CDP is ingeschakeld, kan de switch detecteren dat de Cisco IP-telefoon om DHCP vraagt en kan hij de juiste subnetinformatie leveren. De DHCP-server is dan in staat om een IP-adres toe te wijzen uit de spraak VLAN / subnetpool. Er zijn geen expliciete stappen vereist om de DHCP-service aan de spraak-VLAN te binden.

K. Remove Down SVI onderbreekt DHCP-controle

Op de switches van Cisco Catalyst 6500 Series wordt automatisch een SVI (in afsluitstatus) gemaakt nadat de DHCP is geconfigureerd om te snuffelen voor een bepaald VLAN. De aanwezigheid van dit SVI heeft directe implicaties voor de juiste werking van DHCP-spionage.

DHCP-controle op Cisco Catalyst 6500 Series switches die Native Cisco IOS uitvoeren, wordt meestal geïmplementeerd op routeprocessor (RP of MSFC), niet op Switch Processor (SP of Supervisor). De Cisco Catalyst 6500 Series onderschept pakketten in hardware met VACL's die de pakketten leveren aan een Local Target Logic (LTL) waarop de RP is geabonneerd. Zodra de frames de RP binnenkomen, moeten ze eerst worden gekoppeld aan een L3 Interface (SVI) IDB voordat ze kunnen worden doorgegeven aan het snooping onderdeel. Zonder een SVI bestaat deze IDB niet en worden de pakketten in de RP gelaten vallen.

L. Beperkt uitzendadres

Wanneer een DHCP-client de broadcast-bit in een DHCP-pakket instelt, verzenden de DHCP-server en de relay-agent DHCP-berichten naar clients met het All-ones uitzendadres (255.255.255.255). Als **hun uitzending-adres** bevel is gevormd om een netwerkuitzending te verzenden, wordt de all-ones uitzending die door DHCP wordt verzonden met voeten getreden. Om deze situatie te verhelpen, gebruik **het dhcp beperkt-uitzending-adres** bevel om ervoor te zorgen dat een gevormde netwerkuitzending niet het standaardDHCP-gedrag met voeten treedt.

Sommige DHCP-clients kunnen alleen een all-ones uitzending accepteren en kunnen geen DHCP-adres verkrijgen tenzij deze opdracht is geconfigureerd op de routerinterface die is aangesloten op de client.

M. Debug DHCP met router debug opdrachten

Controleer of de router DHCP-verzoek ontvangt met debug commando's

Op routers die software ondersteunen die DHCP-pakketten verwerkt, kunt u verifiëren of een router het DHCP-verzoek van de client ontvangt. Het DHCP-proces mislukt als de router geen verzoeken van de client ontvangt. In deze stap, vorm een toegang-lijst om output te zuiveren. Deze toegang-lijst wordt gebruikt om slechts een bevel te zuiveren en is niet opdringerig aan de router.

Voer in de globale configuratiemodus deze toegangslijst in:

toegang-lijst 100 vergunning ip host 0.0.0.0 host 255.255.255.255

In exec-modus voert u deze opdracht voor debuggen in:

debug ip-pakketdetail 100

voorbeelduitvoer

```
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
```

Van dit outputvoorbeeld, is het duidelijk dat de router actief de DHCP- verzoeken van de cliënt ontvangt. Deze output toont slechts een samenvatting van het pakket en niet het pakket zelf. Daarom is het niet mogelijk om te bepalen of het pakket correct is. Desalniettemin heeft de router een broadcast-pakket ontvangen met de IP- en UDP-poorten van de bron en de bestemming die correct zijn voor DHCP.

Controleer de router ontvangt en doorstuurt DHCP-verzoek met de opdracht debug ip udp

Het debug ip udp bevel kan de weg van een DHCP- verzoek door een router vinden. Dit debug is echter indringend in een productieomgeving, aangezien alle verwerkte switched UDP-pakketten worden weergegeven op de console. Dit debug commando mag niet gebruikt worden in productie.

> **Waarschuwing**: De opdracht **debug ip udp** is opdringerig en kan een hoog CPU-gebruik (Central Processing Unit) veroorzaken.

In de exec-modus voert u deze opdracht voor debuggen in: **debug ip udp**

voorbeelduitvoer

```
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.
```

Controleer of de router DHCP-verzoek ontvangt en doorstuurt met de opdracht IP-DHCP-serverpakket debug

Als de router Cisco IOS 12.0.x.T of 12.1 is en de Cisco IOS DHCP-serverfunctionaliteit ondersteunt, kunt u de opdracht **debug ip DHCP-server** gebruiken. Dit debug was bedoeld voor gebruik met de IOS DHCP-serverfunctie en om de DHCP/BootP Relay Agent-functie ook op te lossen. Zoals met de vorige stappen, verstrekt de router zuivert geen nauwkeurige bepaling van het probleem aangezien het daadwerkelijke pakket niet kan worden bekeken. Met debugs kunnen echter wel gevolgtrekkingen worden gemaakt met betrekking tot DHCP-verwerking. In exec-modus voert u deze debug-opdracht in:

debug ip DHCP-serverpakket

```
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.
```

Meerdere debugs tegelijkertijd uitvoeren

Wanneer u meerdere debugs tegelijk uitvoert, kan een redelijke hoeveelheid informatie worden ontdekt met betrekking tot de werking van de DHCP/BootP Relay Agent en server. Als u de vorige omtrekken gebruikt om problemen op te lossen, kunt u gevolgtrekkingen maken over waar de DHCP/BootP Relay Agent-functionaliteit niet correct werkt.

```
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.
```

Verkrijg het Sniffer Spoor en Bepaal de Oorzaak van de Wortel van DHCP-probleem

Herzie het Sniffer Trace Decode van DHCP-client en -server op hetzelfde LAN-segment en decodeer Sniffer Trace van DHCP-client en -server, gescheiden door router geconfigureerd als DHCP Relay Agent-secties

om DHCP-pakketsporen te ontcijferen.

Raadpleeg voor informatie over het verkrijgen van snuffelsporen met de functie Switched Port Analyzer (SPAN) op Catalyst-switches het configuratievoorbeeld van Catalyst Switched Port Analyzer (SPAN) configureren.

Alternatieve methode voor pakketdecodering met debug op router

Met de opdracht **debug ip-pakketdetaildump <acl>**op een Cisco-router is het mogelijk een volledig pakket in hex te verkrijgen dat in het systeemlogboek of de opdrachtregelinterface (CLI) wordt weergegeven. Bekijk de verify-router ontvangt DHCP-verzoek met debug commando's en controleer de router ontvangt DHCP-verzoek en Forwards-verzoek aan DHCP-server met debug commando-onderdelen hierboven, samen met het dump-trefwoord dat aan de toegangslijst is toegevoegd, om dezelfde debug-informatie te krijgen, maar met de pakketdetails in hexuitdraai. Om de inhoud van het pakket te bepalen, moet het pakket worden vertaald. Een voorbeeld hiervan is opgenomen in bijlage A.

Bijlage A: Cisco IOS DHCP-voorbeeldconfiguratie

Het DHCP-serverdatabase is georganiseerd als een structuur. De wortel van de boom is de adrespool voor natuurlijke netwerken, takken zijn subnetwork adrespools, en de bladeren zijn handband aan cliënten. Subnetwork erft netwerkparameters en clients erven subnetwork parameters. Daarom moeten de gemeenschappelijke parameters, bijvoorbeeld de domeinnaam, op het hoogste (netwerk of subnetwerk) niveau van de boom worden gevormd.

Raadpleeg de taaklijst DHCP-configuratie voor meer informatie over het configureren van DHCP en de opdrachten die eraan zijn gekoppeld.

```
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
```

Gerelateerde informatie

- Tools en bronnen
- Technische ondersteuning – Cisco Systems

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.