



# Understanding and Troubleshooting DHCP in Catalyst Switch or Enterprise Networks

## Contents

### [Introduction](#)

[Example Scenarios](#)

[Background Information](#)

### [Understanding DHCP](#)

[Current DHCP RFC References](#)

[DHCP Message Table](#)

[DHCPDISCOVER](#)

[DHCPOFFER](#)

[DHCPREQUEST](#)

[DHCPPACK](#)

[DHCPNAK](#)

[DHCPDECLINE](#)

[DHCPINFORM](#)

[DHCPRELEASE](#)

[Renewing the Lease](#)

[DHCP Packet](#)

[Client-Server Conversation for Client Obtaining DHCP Address Where Client and DHCP Server Reside on Same Subnet](#)

[Role of DHCP/BootP Relay Agent](#)

### [Configuring DHCP/BootP Relay Agent Feature on Cisco ® IOS Router](#)

[DHCP Client-Server Conversation with DHCP Relay Function](#)

### [Understanding and Troubleshooting DHCP Using Sniffer Traces](#)

[Decoding Sniffer Trace of DHCP Client and Server on the Same LAN Segment](#)

[Frame 1 - DHCPDISCOVER](#)

[Frame 2 - DHCPOFFER](#)

[Frame 3 - DHCPREQUEST](#)

[Frame 4 - DHCPPACK](#)

[Frame 5 - ARP](#)

[Frame 6 - ARP](#)

[Decoding Sniffer Trace of DHCP Client and Server Separated by a Router Configured as a DHCP/BootP Relay Agent](#)

[Sniffer-B Trace](#)

[Frame 1 - DHCPDISCOVER](#)

[Frame 2 - DHCPOFFER](#)

[Frame 3 - DHCPREQUEST](#)

[Frame 4 - DHCPACK](#)

[Frame 5 - ARP](#)

[Frame 6 - ARP](#)

[Sniffer-A Trace](#)

[Frame 1 - DHCPDISCOVER](#)

[Frame 2 - DHCPOFFER](#)

[Frame 3 - DHCPREQUEST](#)

[Frame 4 - DHCPACK](#)

## [Troubleshooting Client Workstations Unable to Obtain DHCP Addresses](#)

[Case Study 1: DHCP Server on the Same LAN Segment or VLAN as DHCP Client](#)

[Case Study 2: DHCP Server and DHCP Client Separated by Router Configured for DHCP relay Agent Functionality](#)

## [DHCP Troubleshooting Modules](#)

[Understanding Where DHCP Problems Can Occur](#)

[Verify Physical Connectivity](#)

[Test Network Connectivity by Configuring Client Workstation with Static IP Address](#)

[Verify Issue as a Startup Problem](#)

[Verify Switch Port Configuration \(STP Portfast and Other Commands\)](#)

[Check for Known NIC or Catalyst Switch Issues](#)

[Distinguish Whether DHCP Clients Obtain an IP Address on the Same Subnet or VLAN as a DHCP Server](#)

[Verify Router DHCP Relay Configuration](#)

[Debugging DHCP Using Router debug Commands](#)

[Verify Router is Receiving DHCP Request Using debug Commands](#)

[Verify Router is Receiving DHCP Request and Forwarding Request to DHCP Server Using \*\*debug\*\* Commands](#)

[Verify Router is Receiving DHCP Request and Forwarding DHCP Request Using the \*\*debug ip udp\*\* Command](#)

[Verify Router is Receiving DHCP Request and Forwarding DHCP Request Using the \*\*debug ip dhcp server packet\*\* Command](#)

[Running Multiple debugs Simultaneously](#)

[Obtain Sniffer Trace and Determine Root Cause of DHCP Problem](#)

[Alternative Method of Packet Decoding Using debug on a Router](#)

## [Appendix A: IOS DHCP Sample Configuration](#)

### [Related Information](#)

---

# Introduction

This document contains information on how to troubleshoot several common Dynamic Host Configuration Protocol (DHCP) issues that can arise within a Cisco Catalyst switch network. This document includes troubleshooting the use of the Cisco ® IOS DHCP/BootP Relay Agent feature.

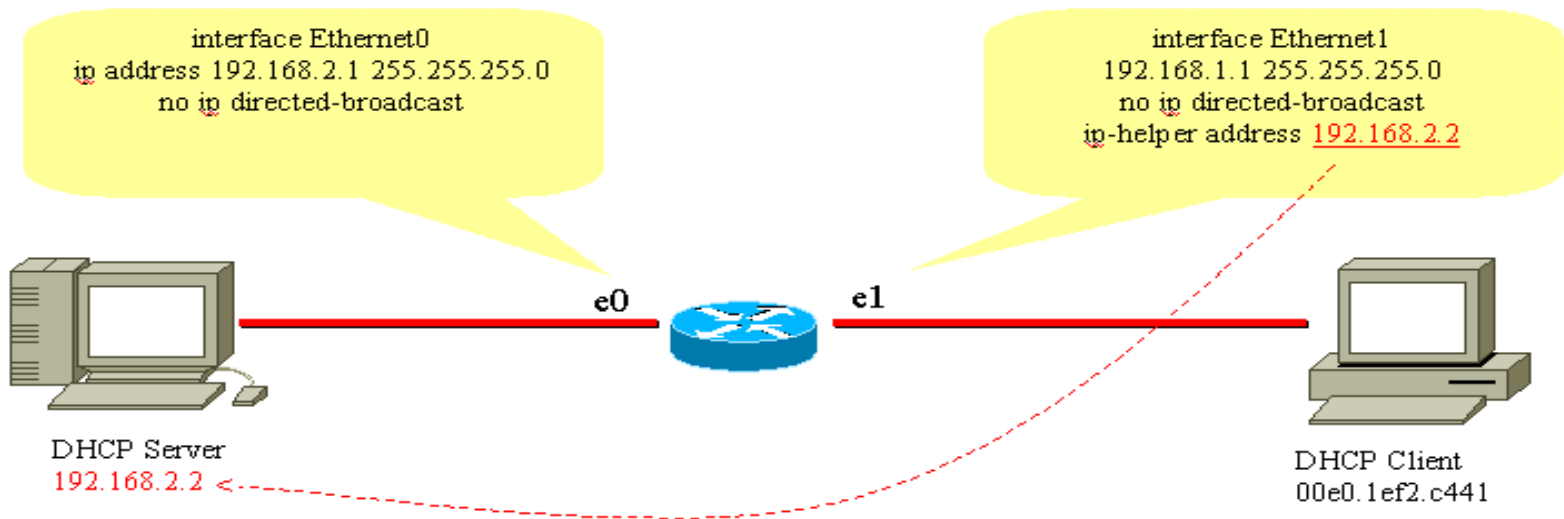
Below are several key concepts of DHCP:

- DHCP clients initially have no configured IP address, and must therefore send a broadcast request to obtain an IP address from a DHCP server.

- Routers, by default, do not forward broadcasts. It is necessary to accommodate client DHCP broadcast requests if the DHCP server is on another broadcast domain (Layer 3 (L3) network). This is performed by use of a DHCP Relay Agent.
- The Cisco router implementation of DHCP Relay is provided via interface-level **ip helper** commands

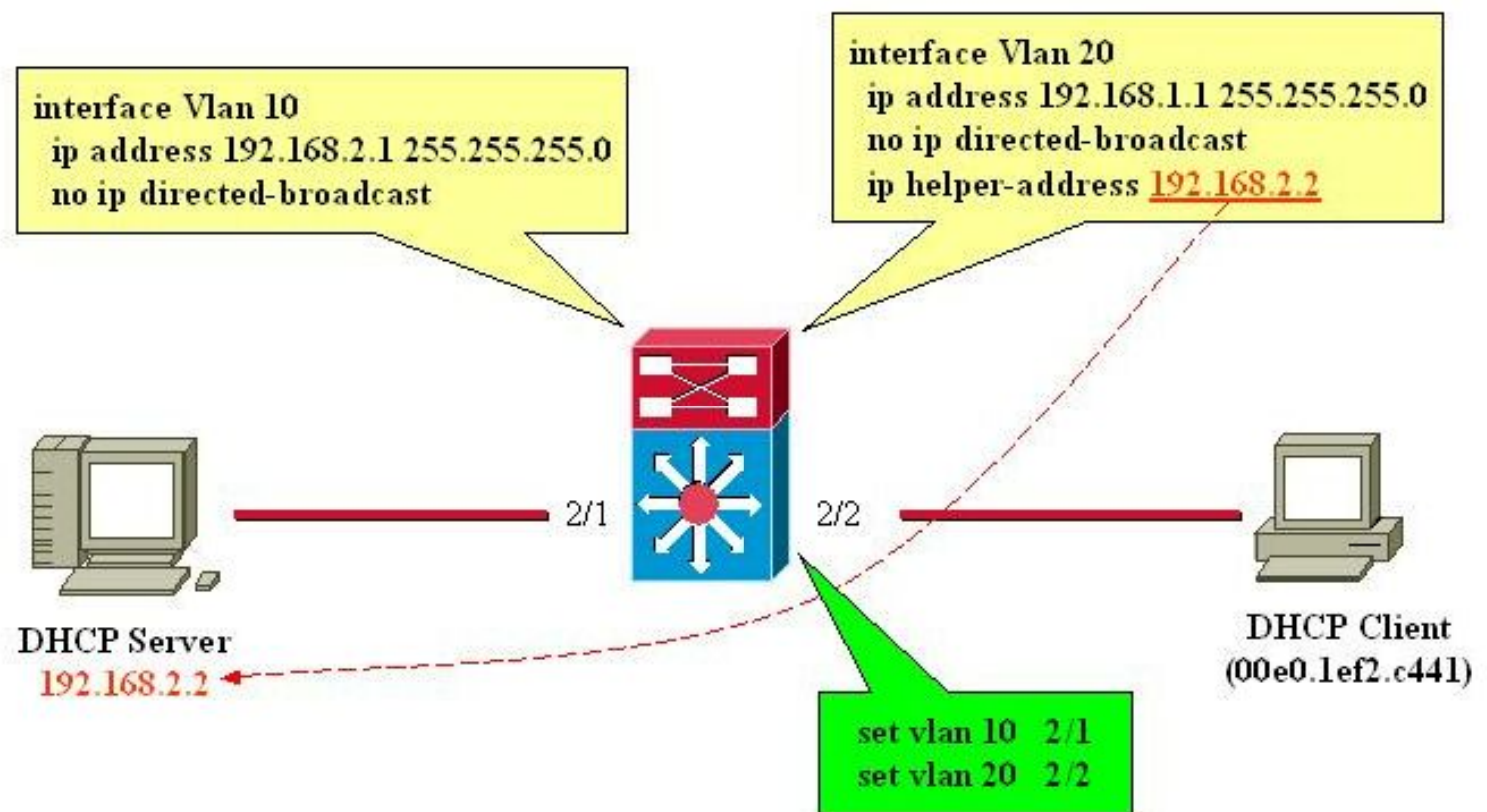
## Example Scenarios

### Scenario 1: Cisco Router Routing between DHCP Client and Server's Networks



As configured in the diagram above, interface Ethernet1 will forward the client's broadcasted DHCPDISCOVER to 192.168.2.2 via interface Ethernet1. The DHCP server will fulfill the request via unicast. No further configuration to the router is necessary in this example.

### Scenario 2: Cisco Catalyst Switch with L3 Module Routing between DHCP Client and Server's Networks



As configured in the diagram above, interface VLAN20 will forward the client's broadcasted DHCPDISCOVER to 192.168.2.2 via interface VLAN10. The DHCP server will fulfill the request via unicast. No further configuration to the router is necessary in this example. The switch ports will need to be configured as host ports and have Spanning-Tree Protocol (STP) portfast enabled, and trunking and channeling disabled.

## Background Information

DHCP provides a mechanism through which computers using Transmission Control Protocol/Internet Protocol (TCP/IP) can obtain protocol configuration parameters automatically through the network. DHCP is an open standard that was developed by the [Dynamic Host Configuration-Working Group](#) (DHC-WG) of the [Internet Engineering Task Force](#) (IETF).

DHCP is based on a client-server paradigm, in which the DHCP client, for example, a desktop computer, contacts a DHCP server for configuration parameters. The DHCP server is typically centrally located and operated by the network administrator. Because the server is run by a network administrator, DHCP clients can be reliably and dynamically configured with parameters appropriate to the current network architecture.

Most enterprise networks consist of multiple subnets divided into subnetworks referred to as Virtual LANS (VLANs), where routers route between the subnetworks. Since routers do not pass broadcasts by default, a DHCP server would be needed on each subnet unless the routers are configured to forward the DHCP broadcast using the DHCP Relay Agent feature.

## Understanding DHCP

DHCP was originally defined in [Requests for Comments \(RFCs\) 1531](#), and has since been obsoleted by [RFC 2131](#). DHCP is based on the Bootstrap Protocol (BootP), which is defined in [RFC 951](#).

DHCP is used by workstations (hosts) to get initial configuration information, such as an IP address, subnet mask, and default gateway upon bootup. Since each host needs an IP address to communicate in an IP network, DHCP eases the administrative burden of manually configuring each host with an IP address. Furthermore, if a host moves to a different IP subnet, it has to use a different IP address than the one it was previously using. DHCP takes care of this automatically, by allowing the host to choose an IP address in the correct IP subnet.

## Current DHCP RFC References

- RFC 2131 - DHCP
- RFC 2132 - DHCP Options and BootP Vendor Extensions
- RFC 1534 - Interoperation between DHCP and BootP
- RFC 1542 - Clarifications and Extensions for the BootP
- RFC 2241 - DHCP Options for Novell Directory Services
- RFC 2242 - Netware/IP Domain Name and Information

DHCP uses a client-server model where one or more servers (DHCP servers) allocate IP addresses and other optional configuration parameters to clients (hosts) upon client bootup. These configuration parameters are leased by the server to the client for some specified amount of time. When a host boots up, the TCP/IP stack in the host transmits a broadcast (DHCPDISCOVER) message in order to gain an IP address and subnet mask, among other configuration parameters. This initiates an exchange between the DHCP server and the host. During this exchange, the client passes through the several well defined states listed below:

1. Initializing
2. Selecting
3. Requesting
4. Bound
5. Renewing
6. Rebinding

In moving between the states listed above, the client and server may exchange the types of messages listed in the [DHCP Message Table](#) below.

## DHCP Message Table

Reference	Message	Use
0x01	DHCPDISCOVER	The client is looking for available DHCP servers.
0x02	DHCPOFFER	The server response to the client DHCPDISCOVER.
0x03	DHCPREQUEST	The client broadcasts to the server, requesting offered parameters from one server specifically, as defined in the packet.
0x04	DHCPDECLINE	The client-to-server communication, indicating that the network address is already in use.
0x05	DHCPACK	The server-to-client communication with configuration parameters, including committed network address.
0x06	DHCPNAK	The server-to-client communication, refusing the request for configuration parameter.
0x07	DHCPRELEASE	The client-to-server communication, relinquishing network address and canceling remaining lease.

0x08	DHCPINFORM	The client-to-server communication, asking for only local configuration parameters that the client already has externally configured as an address.
------	------------	---

## DHCPDISCOVER

When a client boots up for the first time, it is said to be in the Initializing state, and transmits a DHCPDISCOVER message on its local physical subnet over User Datagram Protocol (UDP) port 67 (BootP server). Since the client has no way of knowing the subnet to which it belongs, the DHCPDISCOVER is an all subnets broadcast (destination IP address of 255.255.255.255), with a source IP address of 0.0.0.0. The source IP address is 0.0.0.0, since the client does not have a configured IP address. If a DHCP server exists on this local subnet and is configured and operating correctly, the DHCP server will hear the broadcast and respond with a DHCPOFFER message. If a DHCP server does not exist on the local subnet, there must be a DHCP/BootP Relay Agent on this local subnet to forward the DHCPDISCOVER message to a subnet that contains a DHCP server.

This relay agent can either be a dedicated host (for example, Microsoft Windows Server), or router (for example, a Cisco router configured with interface level IP helper statements).

## DHCPOFFER

A DHCP server that receives a DHCPDISCOVER message may respond with a DHCPOFFER message on UDP port 68 (BootP client). The client receives the DHCPOFFER and moves into the Selecting state. This DHCPOFFER message contains initial configuration information for the client. For example, the DHCP server will fill in the `yiaddr` field of the DHCPOFFER message with the requested IP address. The subnet mask and default gateway are specified in the options field, subnet mask and router options, respectively. Other common options in the DHCPOFFER message include IP Address lease time, renewal time, domain name server, and NetBIOS name server (WINS). The DHCP server will send the DHCPOFFER to the broadcast address, but will include the clients hardware address in the `chaddr` field of the offer, so the client knows that it is the intended destination. In the event that the DHCP server is not on the local subnet, the DHCP server will send the DHCPOFFER, as a unicast packet, on UDP port 67, back to the DHCP/BootP Relay Agent from which the DHCPDISCOVER came. The DHCP/BootP Relay Agent will then broadcast the DHCPOFFER on the local subnet on UDP port 68.

## DHCPREQUEST

After the client receives a DHCPOFFER, it responds with a DHCPREQUEST message, indicating its intent to accept the parameters in the DHCPOFFER, and moves into the Requesting state. The client may receive multiple DHCPOFFER messages, one from each DHCP server that received the original DHCPDISCOVER message. The client chooses one DHCPOFFER and responds to that DHCP server only, implicitly declining all other DHCPOFFER messages. The client identifies the selected server by populating the `Server Identifier` option field with the DHCP server's IP address. The DHCPREQUEST is also a broadcast, so all DHCP servers that sent a DHCPOFFER will see the DHCPREQUEST, and each will know whether its DHCPOFFER was accepted or declined. Any additional configuration options that the client requires will be included in the options field of the DHCPREQUEST message. Even though the client has been offered an IP address, it will send the DHCPREQUEST message with a source IP address of 0.0.0.0. At this time, the client has not yet received verification that it is clear to use the IP address.

## DHCPACK

After the DHCP server receives the DHCPREQUEST, it acknowledges the request with a DHCPACK message, thus completing the initialization process. The DHCPACK message has a source IP address of the DHCP server, and the destination address is once again a broadcast and contains all the parameters that the client requested in the DHCPREQUEST message. When the client receives the DHCPACK, it enters into the Bound state, and is now free to use the IP address to communicate on the network. Meanwhile, the DHCP server stores the lease in its database and uniquely identifies it using the `client identifier` or `chaddr`, and the associated IP address. Both the client and server will use this combination of identifiers to refer to the lease.

Before the DHCP client begins using the new address, the DHCP client must calculate the time parameters associated with a leased address, which are Lease Time (LT), Renewal Time (T1), and Rebind Time (T2). The typical default LT is 72 hours. You can use shorter lease times to conserve addresses, if needed.

## DHCPNAK

If the selected server is unable to satisfy the DHCPREQUEST message, the DHCP server will respond with a DHCPNAK message. When the client receives a DHCPNAK message, or does not receive a response to a DHCPREQUEST message, the client restarts the configuration process by going into the Requesting state. The client will retransmit the DHCPREQUEST at least four times within 60 seconds before restarting the Initializing state.

## DHCPDECLINE

The client receives the DHCPACK and will optionally perform a final check on the parameters. The client performs this procedure by sending Address Resolution Protocol (ARP) requests for the IP address provided in the DHCPACK. If the client detects that the address is already in use by receiving a reply to the ARP request, the client will send a DHCPDECLINE message to the server and restart the configuration process by going into the Requesting state.

## DHCPINFORM

If a client has obtained a network address through some other means or has a manually configured IP address, a client workstation may use a DHCPINFORM request message to obtain other local configuration parameters, such as the domain name and Domain Name Servers (DNSs). DHCP servers receiving a DHCPINFORM message construct a DHCPACK message with any local configuration parameters appropriate for the client without allocating a new IP address. This DHCPACK will be sent unicast to the client.

## DHCPRELEASE

A DHCP client may choose to relinquish its lease on a network address by sending a DHCPRELEASE message to the DHCP server. The client identifies the lease to be released by the use of the `client identifier` field and network address in the DHCPRELEASE message.

## Renewing the Lease

Since the IP address is only leased from the server, the lease must be renewed from time to time. When one half of the lease time has expired ( $T1 = 0.5 \times LT$ ), the client will try to renew the lease. The client enters the Renewing state and sends a DHCPREQUEST message to the server, which holds the current lease. The server will reply to the request to renew with a DHCPACK message if it agrees to renew the lease. The DHCPACK message will contain the new lease and any new configuration parameters, in the event that any changes are made to the server during the time of the previous lease. If the client is unable to reach the server holding the lease for some reason, it will attempt to renew the address from any DHCP server after the original DHCP server has not responded to the renewal requests within a time T2. The default value of T2 is ( $7/8 \times LT$ ). This means  $T1 < T2 < LT$ .

If the client previously had a DHCP assigned IP address and it is restarted, the client will specifically request the previously leased IP address in a DHCPREQUEST packet. This DHCPREQUEST will still have the source IP address as 0.0.0.0, and the destination as the IP broadcast address 255.255.255.255.

A client sending a DHCPREQUEST during a reboot must not fill in the `server identifier` field, and must instead fill in the `requested IP address` option field. Strictly RFC compliant clients will populate the `ciaddr` field with the address requested instead of the DHCP option field. The DHCP server will accept either method. The behavior of the DHCP server depends on a number of factors, such as in the case of Windows NT DHCP servers, the version of the operating system being used, as well as other factors, such as superscoping. If the DHCP server determines that the client can still use the requested IP address, it will either remain silent or send a DHCPACK for the DHCPREQUEST. If the server determines that the client cannot use the requested IP address, it will send a DHCPNACK back to the client. The client will then move to the Initializing state, and send a DHCPDISCOVER message.

## DHCP Packet

The DHCP message is variable in length and consists of fields listed in the table below.

**Note:** This packet is a modified version of the original BootP packet.

Field	Bytes	Name	Description
op	1	OpCode	Identifies the packet as an request or reply: 1=BOOTREQUEST, 2=BOOTREPLY
htype	1	Hardware Type	Specifies the network hardware address type.
hlen	1	Hardware Length	Specifies the length hardware address length.
hops	1	Hops	The client sets the value to zero and the value increments if the request is forwarded across a router.
xid	4	Transaction ID	A random number that is chosen by the client. All DHCP messages exchanged for a given DHCP transaction use the ID (xid).
secs	2	Seconds	Specifies number of seconds since the DHCP process started.
flags	2	Flags	Indicates whether the message will be broadcast or unicast.
ciaddr	4	Client IP address	Only used when client knows its IP address as in the case of the Bound, Renew, or Rebinding states.
yiaddr	4	Your IP address	If the client IP address is 0.0.0.0, the DHCP server will place the offered client IP address in this field.
siaddr	4	Server IP address	If the client knows the IP address of the DHCP server, this field will be populated with the DHCP server address. Otherwise, it is used in DHCPOFFER and DHCPACK from DHCP server.
giaddr	4	Router IP address (GI ADDR)	The Gateway IP address, filled in by the DHCP/BootP Relay Agent.
chaddr	16	Client MAC address	The DHCP client MAC address.
sname	64	Server name	The optional server host name.
file	128	Boot file name	The boot file name.
options	variable	Option parameters	The optional parameters that can be provided by the DHCP server. RFC 2132 gives all possible options.



## Client-Server Conversation for Client Obtaining DHCP Address Where Client and DHCP Server Reside on Same Subnet

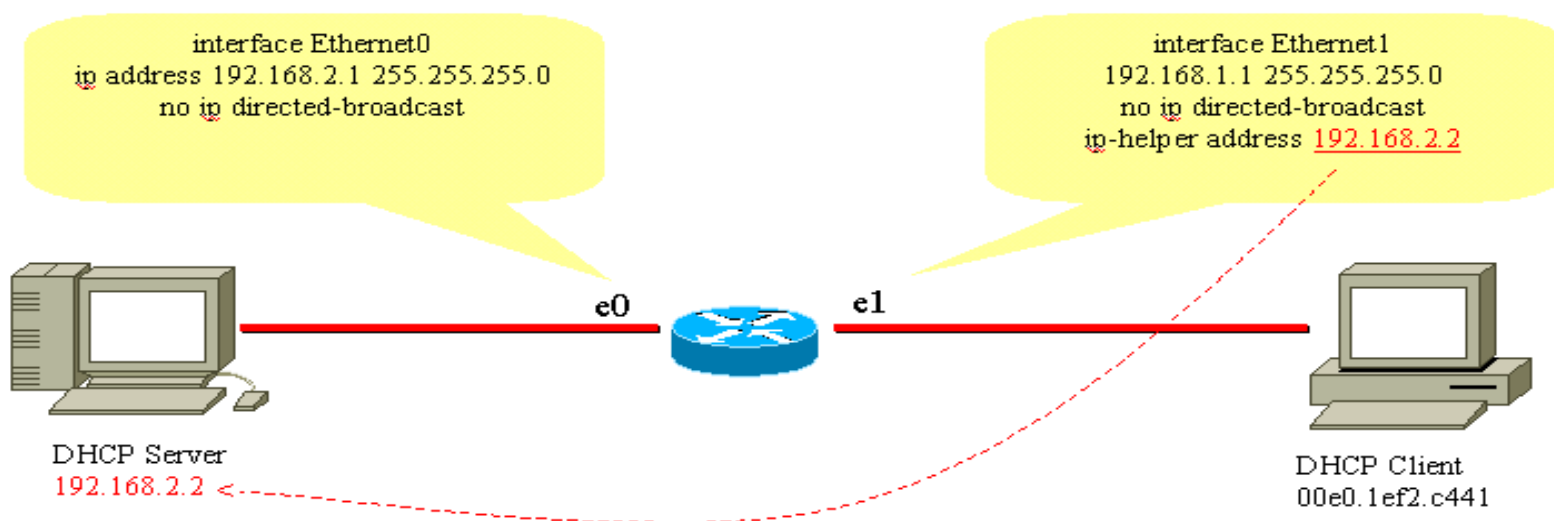
Packet Description	Source MAC Addr	Destination MAC Addr	Source IP Addr	Destination IP Addr
DHCPDISCOVER	Client	Broadcast	0.0.0.0	255.255.255.255
DHCPOFFER	DHCP Server	Broadcast	DHCP Server	255.255.255.255
DHCPREQUEST	Client	Broadcast	0.0.0.0	255.255.255.255
DHCPACK	DHCP Server	Broadcast	DHCP Server	255.255.255.255

## Role of DHCP/BootP Relay Agent

Routers, by default, will not forward broadcast packets. Since DHCP client messages use the destination IP address of 255.255.255.255 (all Nets Broadcast), DHCP clients will not be able to send requests to a DHCP server on a different subnet unless the DHCP/BootP Relay Agent is configured on the router. The DHCP/BootP Relay Agent will forward DHCP requests on behalf of a DHCP client to the DHCP server. The DHCP/BootP Relay Agent will append its own IP address to the source IP address of the DHCP frames going to the DHCP server. This allows the DHCP server to respond via unicast to the DHCP/BootP Relay Agent. The DHCP/BootP Relay Agent will also populate the Gateway IP address field with the IP address of the interface on which the DHCP message is received from the client. The DHCP server uses the Gateway IP address field to determine the subnet from which the DHCPDISCOVER, DHCPREQUEST, or DHCPINFORM message originates.

## Configuring DHCP/BootP Relay Agent Feature on Cisco IOS Router

Configuring a Cisco router to forward BootP or DHCP requests is simple - configure an IP helper-address pointing to the DHCP/BootP server, or pointing to the subnet broadcast address of the network the server is on. For example, consider the following network diagram:



To forward the BootP/DHCP request from the client to the DHCP server, the **ip helper-address interface** command is used. The IP helper-address can be configured to forward any UDP broadcast based on UDP port number. By default, the IP helper-address will forward the following UDP broadcasts:

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

- DNS (port 53), time service (port 37)
- NetBIOS name server (port 137)
- NetBIOS datagram server (port 138)
- Boot Protocol (DHCP/BootP) client and server datagrams (ports 67 and 68)
- Terminal Access Control Access Control System (TACACS) service (port 49)
- IEN-116 name service (port 42)

IP helper-addresses can direct UDP broadcasts to a unicast or broadcast IP address. **However, it is not recommended to use the IP helper-address to forward UDP broadcasts from one subnet to the broadcast address of another subnet, due to the large amount of broadcast flooding that may occur.** Multiple IP helper-address entries on a single interface are supported as well, as shown below:

```
!
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 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
```

## DHCP Client-Server Conversation with DHCP Relay Function

The table below illustrates the process for a DHCP client to obtain an IP address from a DHCP server. This table is modeled after the [network diagram](#) above. Each numerical value in the diagram represents a packet that is described below. This table is a point of reference for understanding the packet flow of DHCP client-server conversation. This table is also useful for determining where DHCP problems may be occurring.

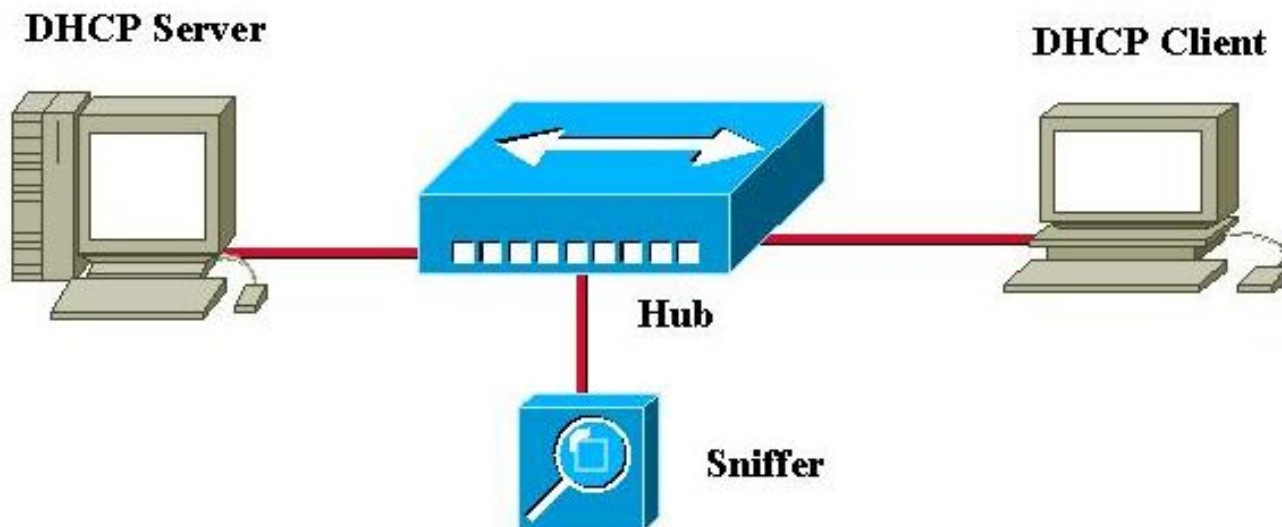
Packet	Client IP Address	Server IP Address	GI Address	Packet Source MAC Address	Packet Source IP Address	Packet Destination MAC Address	Packet Destination IP Address
1. DHCPDISCOVER is sent from client.	0.0.0.0	0.0.0.0	0.0.0.0	0005.DCC9.C640	0.0.0.0	ffff.ffff.ffff (broadcast)	255.255.255.255
2. The router receives the DHCPDISCOVER on the E1 interface. The router recognizes that this packet is a DHCP UDP broadcast. The router will now act as a DHCP/BootP Relay Agent and fill in the Gateway IP address field with the incoming interface IP address, change the source IP address to an incoming interface IP address, and forward the request directly to the DHCP server.	0.0.0.0	0.0.0.0	192.168.1.1	Interface E2 MAC Address	192.168.1.1	MAC Address of DHCP Server	192.168.2.2
3. The DHCP server has received the DHCPDISCOVER and is sending a DHCPOFFER to the DHCP Relay Agent.	192.168.1.2	192.168.2.2	192.168.1.1	MAC Address of DHCP Server	192.168.2.2	Interface E2 MAC Address	192.168.1.1
4. The DHCP Relay Agent receives a DHCPOFFER, and will forward the DHCPOFFER broadcast on the local LAN.	192.168.1.2	192.168.2.2	192.168.1.1	Interface E1 MAC Address	192.168.1.1	ffff.ffff.ffff (broadcast)	255.255.255.255
5. DHCPREQUEST sent from client.	0.0.0.0	0.0.0.0	0.0.0.0	0005.DCC9.C640	0.0.0.0	ffff.ffff.ffff (broadcast)	255.255.255.255

6. The router receives the DHCPREQUEST on the E1 Interface. The router recognizes that this packet is DHCP UDP broadcast. The router will now act as a DHCP Relay Agent and fill in the Gateway IP address field with the incoming interface IP Address, change the source IP address to an incoming interface IP address, and forward the request directly to the DHCP server.	0.0.0.0	0.0.0.0	192.168.1.1	Interface E2 MAC Address	192.168.1.1	MAC Address of DHCP Server	192.168.2.2
7. The DHCP server has received the DHCPREQUEST and is sending a DHCPACK to the DHCP/BootP Relay Agent.	192.168.1.2	192.168.2.2	192.168.1.1	MAC Address of DHCP Server	192.168.2.2	Interface E2 MAC Address	192.168.1.1
8. The DHCP/BootP Relay Agent receives the DHCPACK, and will forward the DHCPACK broadcast on the local LAN. The client will accept the ACK and use the client's IP address.	192.168.1.2	192.168.2.2	192.168.1.1	Interface E1 MAC Address	192.168.1.1	ffff.ffff.ffff (broadcast)	255.255.255.255

## Understanding and Troubleshooting DHCP Using Sniffer Traces

# Decoding Sniffer Trace of DHCP Client and Server on Same LAN Segment

## Network Topology where DHCP Client and Server Reside on Same LAN Segment



The sniffer trace below is comprised of six frames. These six frames illustrate a working scenario for DHCP, where the DHCP client and server reside on the same physical or logical segment. When troubleshooting DHCP, it is important to match your sniffer trace to the traces below. There may be some differences compared to the traces below, but the general packet flow should be exactly the same. The packet trace follows previous discussions of how DHCP works.

### ----- 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 1 arrived at 11:52:03.8106; frame size is 618 (026A hex) bytes.

DLC: **Destination = BROADCAST FFFFFFFF**, 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 FFFFFFFF**, 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 FFFFFFFF**, 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 FFFFFFFF**, 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 FFFFFFFF, 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 = FFFFFFFF  
 ARP: Target protocol address = [192.168.1.2]  
 ARP:  
 ARP: 18 bytes frame padding  
 ARP:

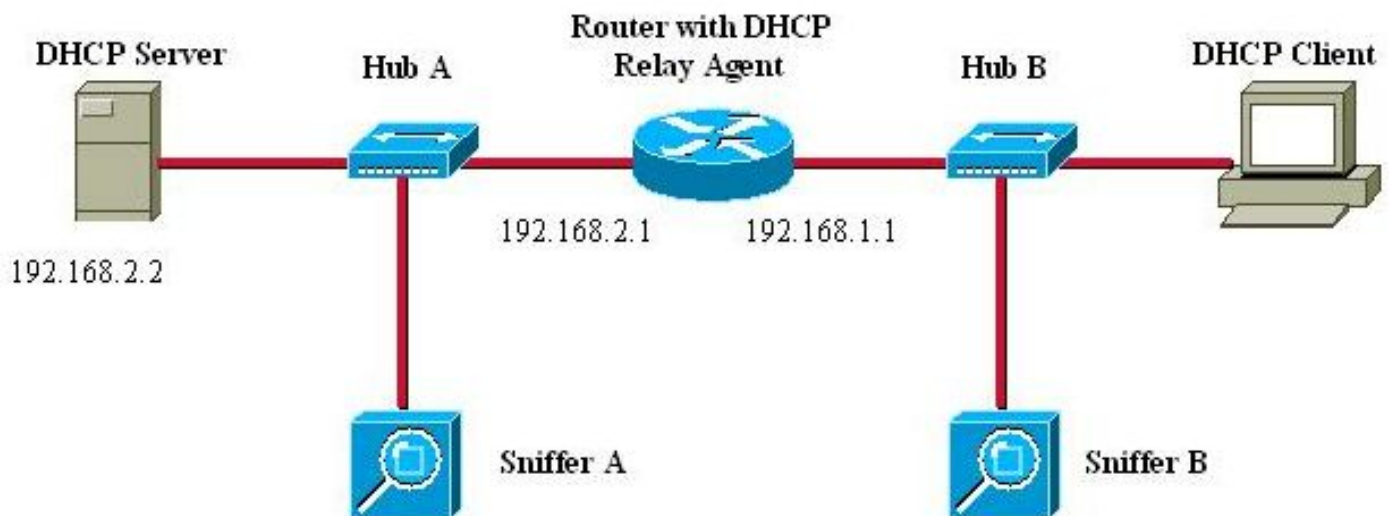
----- **Frame 6 - ARP** -----

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 FFFFFFFF, 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 = FFFFFFFF
ARP: Target protocol address = [192.168.1.2]
ARP:
ARP: 18 bytes frame padding
ARP:
```

## Decoding Sniffer Trace of DHCP Client and Server Separated by a Router that is Configured as a DHCP Relay Agent

### DHCP Client and Server separated by router configured as DHCP Relay Agent



### Sniffer-B Trace

----- 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 FFFFFFFF, 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	Summary
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 FFFFFFFF, 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 FFFFFFFF, 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 FFFFFFFF, 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 FFFFFFFF, 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 = FFFFFFFF  
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 FFFFFFFF, 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 = FFFFFFFF  
ARP: Target protocol address = [192.168.1.2]  
ARP:  
ARP: 18 bytes frame padding  
ARP:

**Sniffer-A Trace**

----- **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 - DHCP OFFER** -----

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:

## Troubleshooting DHCP when Client Workstations are Unable to Obtain DHCP Addresses

### Case Study #1: DHCP Server on Same LAN Segment or VLAN as DHCP Client

When the DHCP server and client reside on the same LAN segment or VLAN and the client is unable to obtain an IP address from a DHCP server, it is unlikely that the local router is causing a DHCP problem. The problem is most likely

related to the devices that connect the DHCP server and DHCP client. However, the problem may be with the DHCP server or client itself. Following the troubleshooting modules below should determine what device is causing the issue.

## Case Study #2: DHCP Server and DHCP Client are Separated by a Router Configured for DHCP/BootP Relay Agent Functionality

When the DHCP server and client reside on the different LAN segments or VLANs, the router functioning as a DHCP/BootP Relay Agent is responsible for forwarding the DHCPREQUEST to the DHCP server. Additional troubleshooting steps are required to troubleshoot the DHCP/BootP Relay Agent, as well as the DHCP server and client. Following the troubleshooting modules below should determine which device is causing the issue.

# DHCP Troubleshooting Modules

## Understanding Where DHCP Problems Can Occur

DHCP problems can arise due to a multitude of reasons. The most common reasons are configuration issues. However, many DHCP problems can be caused by software defects in operating systems, Network Interface Card (NIC) drivers, or DHCP/BootP Relay Agents running on routers. Due to the number of potentially problematic areas, a systematic approach to troubleshooting is required.

### Short List of Possible Causes of DHCP Problems:

- Catalyst switch default configuration
- DHCP/BootP Relay Agent configuration
- NIC compatibility issue or DHCP feature issue
- Operating system behavior or software defect
- DHCP server scope configuration or software defect
- Cisco Catalyst switch or IOS DHCP/BootP Relay Agent software defect

This document will use troubleshooting modules below to determine the root cause, as indicated in the list above.

### A. Verify Physical Connectivity

This procedure is applicable to all case studies.

First, verify physical connectivity of a DHCP client and server. If connected to a Catalyst switch, verify that both the DHCP client and server have physical connectivity.

For Catalyst CatOS switches such as the 2948G, 4000, 5000, and 6000 series switches, use the **show port <mod#>/<port\_range>** command to note the port status. If the port status is anything other than **connected**, the port will not pass any traffic, including DHCP client requests. The output from the commands is as follows:

```
Switch (enable) show port 5/1
Port Name Status Vlan Duplex Speed Type
-----
5/1 connected 1 a-full a-100 10/100BaseTX
```

For IOS based switches such as the Catalyst 2900XL/3500XL/2950/3550, the equivalent command to **show port status** is **show interface <interface>**. If the state of the interface is anything other than **<interface> is up, line protocol is up**, the port will not pass traffic, including DHCP client requests. The output from the commands is as follows:

```
Switch#show interface fastEthernet 0/1
```

```
FastEthernet0/1 is up, line protocol is up
Hardware is Fast Ethernet, address is 0030.94dc.accl (bia 0030.94dc.accl)
```

If the physical connection has been verified and there is indeed no link between the Catalyst switch and DHCP client, consult the [Troubleshooting Cisco Catalyst Switches to Network Interface Card \(NIC\) Compatibility](#) document for additional troubleshooting in regards to the physical layer connectivity issue.

## B. Test Network Connectivity by Configuring Client Workstation with Static IP Address

This procedure is applicable to all case studies.

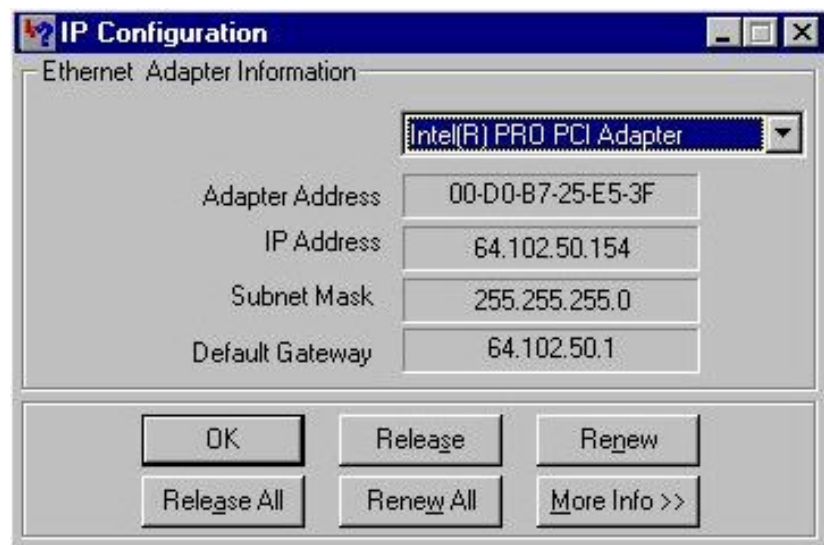
When troubleshooting any DHCP Issue, it is important to verify network connectivity by configuring a static IP address on a client workstation. If the workstation is unable to reach network resources despite having a statically configured IP address, the root cause of the problem is not DHCP. At this point, network connectivity troubleshooting is required.

## C. Verify Issue as a Startup Problem

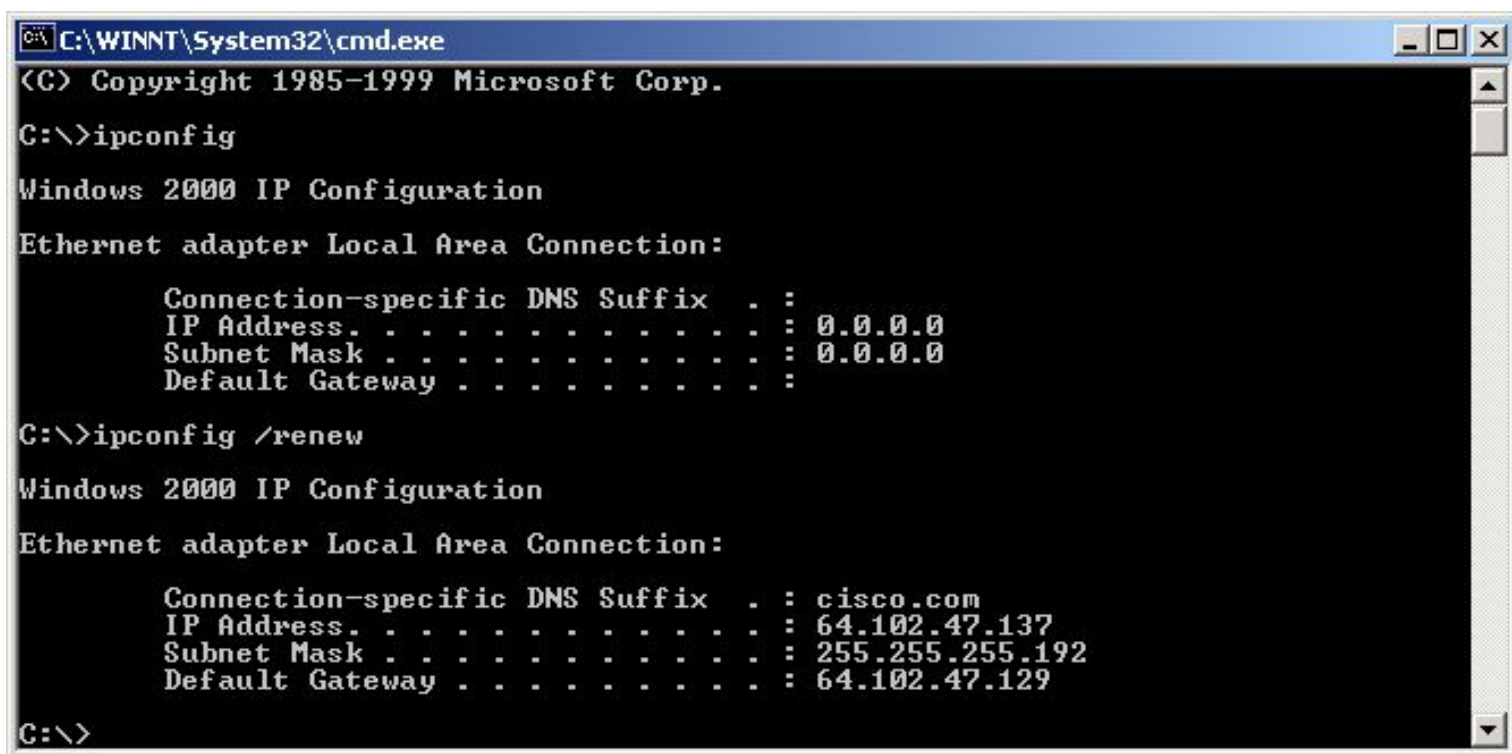
This procedure is applicable to all case studies.

If the DHCP client is unable to obtain an IP address from the DHCP server on startup, attempt to obtain an IP address from the DHCP server by manually forcing the client to send a DHCP request. Issue the following steps to manually obtain an IP address from a DHCP server for the operating systems listed below.

**Microsoft Windows 95/98/ME:** Click the **Start** button, and run the WINIPCFG.exe program. Click the **Release All** button, followed by the **Renew All** button. Is the DHCP client now able to obtain an IP address?



**Microsoft Windows NT/2000:** Open a command prompt window by typing **cmd** in the **Start/Run** field. Issue the command **ipconfig/renew** in the command prompt window, as shown below. Is the DHCP client now able to obtain an IP Address?



```

C:\WINNT\System32\cmd.exe
(C) Copyright 1985-1999 Microsoft Corp.

C:\>ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 0.0.0.0
    Subnet Mask . . . . . : 0.0.0.0
    Default Gateway . . . . . : 

C:\>ipconfig /renew

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : cisco.com
    IP Address. . . . . : 64.102.47.137
    Subnet Mask . . . . . : 255.255.255.192
    Default Gateway . . . . . : 64.102.47.129

C:\>

```

If the DHCP client is able to obtain an IP address by manually renewing the IP address after the PC has completed the bootup process, the issue is most likely a DHCP startup issue. If the DHCP client is attached to a Cisco Catalyst switch, the problem is most likely due to a configuration issue dealing with STP portfast and/or channeling and trunking. Other possibilities include NIC card issues and switch port startup issues. Troubleshooting [Steps D](#) and [E](#) should be reviewed to rule out switch port configuration and NIC card issues as the root cause of the DHCP problem.

#### D. Verify Switch Port Configuration (STP Portfast and Other Commands)

If the switch is a Catalyst 2900/4000/5000/6000, verify that the port has STP portfast enabled and trunking/channeling disabled. The default configuration is STP portfast disabled and trunking/channeling auto, if applicable. For the 2900XL/3500XL/2950/3550 switches, STP portfast is the only required configuration. These configuration changes resolve the most common DHCP client issues that occur with an initial installation of a Catalyst switch.

For more documentation regarding the necessary switch port configuration requirements for DHCP to operate properly when connected to Catalyst switches, please review the following document:

[Using Portfast and Other Commands to Fix Workstation Startup Connectivity Delays](#)

After reviewing the configuration guidelines in the document above, return to this document for additional troubleshooting.

#### E. Check for Known NIC Card or Catalyst Switch Issues

If the Catalyst switch configuration is correct, it is possible that a software compatibility issue may exist on the Catalyst switch or DHCP client's NIC that could be causing DHCP issues. The next step in troubleshooting is to review the following document and rule out any software issues with the Catalyst switch or NIC that may be contributing to the problem:

[Troubleshooting Cisco Catalyst Switches to Network Interface Card \(NIC\) Compatibility Issues](#)

Knowledge of the DHCP client's operating system as well as specific NIC information such as the manufacturer, model, and driver version will be needed to properly rule out any compatibility issues.

#### F. Distinguishing whether DHCP Clients Obtain IP Address on the Same Subnet or VLAN as DHCP Server

It is important to distinguish whether or not DHCP is functioning correctly when the client is on same subnet or VLAN as the DHCP server. If the DHCP is working correctly on the same subnet or VLAN as the DHCP server, the DHCP issue may

be with the DHCP/BootP Relay Agent. If the problem persists even with testing DHCP on the same subnet or VLAN as the DHCP server, the problem may actually be with the DHCP server.

## G. Verify Router DHCP/BootP Relay Configuration

Issue the steps below to verify the configuration:

1. When configuring DHCP relay on a router, verify that the **ip helper-address** command is located on the correct interface. The **ip helper-address** command must be present on the inbound interface of the DHCP client workstations and must be directed to the correct DHCP server.
2. Verify that the global configuration command **no service dhcp** is not present. This configuration parameter will disable all DHCP server and relay functionality on the router. The default configuration, **service dhcp**, will not appear in the configuration, and is the default configuration command.
3. When applying **ip helper-address** commands to forward UDP broadcasts to a subnet broadcast address, verify that no **ip directed-broadcast** is not configured on any outbound interface that the UDP broadcast packets needs to traverse. The **no ip directed-broadcast** will block on any translation of a directed broadcast to physical broadcasts. This interface configuration is default configuration in software versions 12.0 and higher.
4. Forwarding DHCP broadcasts to the DHCP server's subnet broadcast address is an occasional software issue. When troubleshooting DHCP, always attempt to forward DHCP UDP broadcasts to the DHCP server's IP address, as shown below:

```
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption

no service dhcp !- (2)
This configuration command will disable all DHCP server and relay functionality on the router.
!
hostname router
!
!
!
interface Ethernet0
ip address 192.168.2.1 255.255.255.0
no ip directed-broadcast !- (3)
This configuration will prevent translation of a directed broadcast to a physical broadcast.
!
interface Ethernet1 !- (1)
DHCP client workstations reside of this interface.
ip address 192.168.1.1 255.255.255.0
ip helper-address 192.168.2.255 !- (4)
IP helper-address pointing to DHCP server's subnet.
no ip directed-broadcast
!
!
!
line con 0
exec-timeout 0 0
transport input none
```

```

line aux 0
line vty 0 4
login
!
end

```

## H. Debugging DHCP Using Router debug Commands

### Verify Router is Receiving DHCP Request Using debug Commands

On routers that support software processing of DHCP packets, you can verify whether a router is receiving the DHCP request from the client. The DHCP process will fail if the router is not receiving requests from the client. This troubleshooting step involves configuring an access-list for debugging output. This access-list is for debugging purposes only and is not intrusive to the router.

In global configuration mode, enter the following access-list:

**access-list 100 permit ip host 0.0.0.0 host 255.255.255.255**

In exec mode, enter the following debug command:

**debug ip packet detail 100**

Sample output:

```

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

```

From the output above, it is clear that the router is receiving the DHCP requests from the client. This output only shows a summary of the packet and not the packet itself. Therefore, it is not possible to determine if the packet is correct. Nevertheless, the router did receive a broadcast packet with the source and destination IP and UDP ports that are correct for DHCP.

### Verify Router is Receiving DHCP Request and Forwarding Requests to DHCP Server Using debug Commands

Additional entries in the access-list can be added to see if the router is communicating successfully with the DHCP server. Again, these debugs do not look into the packet, but you can confirm whether or not the DHCP relay agent is forwarding requests to the DHCP server.

In global configuration mode, create the following access-list:

**access-list 100 permit ip host 0.0.0.0 host 255.255.255.255**

**access-list 100 permit udp host <dhcp\_relay\_agent> host <dhcp\_server> eq 67**

**access-list 100 permit udp host <dhcp\_server> host <dhcp\_relay\_agent> eq 67**

For example:

**access-list 100 permit ip host 0.0.0.0 host 255.255.255.0**

**access-list 100 permit udp host 192.168.1.1 host 192.168.2.2 eq 67**

**access-list 100 permit udp host 192.168.1.1 host 192.168.2.2 eq 68**

**access-list 100 permit udp host 192.168.2.2 host 192.168.1.1 eq 67**

**access-list 100 permit udp host 192.168.2.2 host 192.168.1.1 eq 68**

In exec mode, enter the following debug command:

```
Router#
00:23:44: IP: s=0.0.0.0 (Ethernet4/0), d=255.255.255.255, len 604, rcvd 2
00:23:44: UDP src=68, dst=67
!- Router receiving DHCPDISCOVER from DHCP client.
00:23:44: IP: s=192.168.1.1 (local), d=192.168.2.2 (Ethernet4/1), len 604, sendg
00:23:44: UDP src=67, dst=67
!- Router forwarding DHCPDISCOVER unicast to DHCP server using
DHCP/BootP Relay Agent source IP address.
00:23:44 IP: s=192.168.2.2 (Ethernet1), d=192.168.1.1, len 328, rcvd 4
00:23:44 UDP src=67, dst=67
!- DHCP server sending DHCP OFFER to DHCP/BootP Relay Agent.
00:23:44: IP: s=0.0.0.0 (Ethernet4/0), d=255.255.255.255, len 604, rcvd 2
00:23:44: UDP src=68, dst=67
!- Router receiving DHCPREQUEST from DHCP client.
00:23:44: IP: s=192.168.1.1 (local), d=192.168.2.2 (Ethernet4/1), len 604, sendg
00:23:44: UDP src=67, dst=67
!- Router forwarding DHCPDISCOVER unicast to DHCP server using
DHCP/BootP Relay Agent source IP address.
00:23:44 IP: s=192.168.2.2 (Ethernet1), d=192.168.1.1, len 328, rcvd 4
00:23:44 UDP src=67, dst=67
!- DHCP server sending DHCPACK back to DHCP/BootP Relay Agent.
```

From the output above, it is clear that the router is receiving the DHCP requests from the client and forwarding the request, per the DHCP/BootP Relay Agent configuration, to the DHCP server. The DHCP server also replied directly to the DHCP/BootP Relay Agent. This output only shows a summary of the packet and not the packet itself. Therefore, it is not possible to determine if the packet is correct or whether the server is replying with a DHCPNAK. Nevertheless, the router did receive a broadcast packet with the source and destination IP and UDP ports that are correct for DHCP, and there is two-way communication with the DHCP server.

## Verify Router is Receiving and Forwarding DHCP Request Using debug ip udp Command

The **debug ip udp** command can be used to trace the path of a DHCP request through a router. However, this debug is intrusive in a production environment, since all processed switched UDP packets will be displayed to the console. This debug should not be used in production.

**Warning:** The **debug ip udp** command is intrusive, and may cause high Central Processing Unit (CPU) utilization.

In exec mode, enter the following debug command:

**debug ip udp**

Sample output:

```
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 DHCPPOFFER 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 DHCPPOFFER 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.

```

## Verify Router is Receiving and Forwarding DHCP Request Using debug ip dhcp server packet Command

If the router IOS is 12.0.x.T or 12.1 and supports the IOS DHCP server functionality, additional debugging can be done using the **debug ip dhcp server packet** command. This debug was intended for use with the IOS DHCP server feature, but can be used for troubleshooting the DHCP/BootP Relay Agent feature as well. As with the previous troubleshooting steps, router debugs do not provide an exact determination of the problem since the actual packet cannot be viewed. However, debugs do allow inferences to be made regarding DHCP processing.

In exec mode, enter the following debug command:

**debug ip dhcp server packet**

```

Router#debug ip dhcp server packet
00:20:54: DHCPD: setting giaddr to 192.168.1.1.
!- Router received DHCPDISCOVER/REQUEST/INFORM 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 DHCPPOFFER and DHCPNAK.
!- Client's MAC address is 00e0.1ef2.c441.
00:20:54: DHCPD: broadcasting BOOTREPLY to client 00e0.1ef2.c441.
!- Router is forwarding DHCPPOFFER 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.

```

## Running Multiple Debugs Simultaneously

When running multiple debugs simultaneously, a fair amount of information can be discovered regarding the operation of the DHCP/BootP Relay Agent and server. Using the above troubleshooting outlines, you can make inferences about where the DHCP/BootP Relay Agent functionality may not be operating correctly.

```

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.

```

## Obtain Sniffer Trace and Determine Root Cause of DHCP Problem

Using router debugging techniques will not always determine the exact root cause of a DHCP problem. The ultimate step in

resolving a DHCP issue is to obtain a sniffer trace and note where the process is not functioning correctly. DHCP packet traces can be deciphered by referencing the Decoding Sniffer Trace of DHCP Client and Server on Same LAN Segment and Decoding Sniffer Trace of DHCP Client and Server Separated by Router Configured as a DHCP Relay Agent sections of this document.

For information on obtaining sniffer traces using the Switched Port Analyzer (SPAN) feature on Catalyst switches, refer to the following document:

- [Configuring the Catalyst Switched Port Analyzer \(SPAN\) Feature.](#)

## Alternative Method of Packet Decoding Using debug on Router

By using the **debug ip packet detail dump <acl>** command on a Cisco router, it is possible to get an entire packet in hex displayed in the system log or Command Line Interface (CLI). Using the Verify Router is Receiving DHCP Request Using debug Commands and Verify Router is Receiving DHCP Request and Forwarding Request to DHCP Server Using debug Commands sections above, along with the dump keyword added to the access-list, will provide the same debug information, but with the packet detail in hex. To determine the contents of the packet, the packet will need to be translated. An example is given in [Appendix A](#).

# Appendix A: IOS DHCP Sample Configuration

The DHCP server database is organized as a tree. The root of the tree is the address pool for natural networks, branches are subnetwork address pools, and leaves are manual bindings to clients. Subnetworks inherit network parameters and clients inherit subnetwork parameters. Therefore, common parameters, for example the domain name, should be configured at the highest (network or subnetwork) level of the tree.

For more information on how to configure DHCP and the commands associated with it, refer to the following link:

- [DHCP Configuration Task List](#)

```
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
```

---

## Related Information

- [Technical Support-Cisco Systems](#)
- [Tools and Utilities](#)

---

<a href="#">Home</a>	<a href="#">What's New</a>	<a href="#">How to Buy</a>	<a href="#">Login</a>	<a href="#">Profile</a>	<a href="#">Feedback</a>	<a href="#">Search</a>	<a href="#">Map/Help</a>
----------------------	----------------------------	----------------------------	-----------------------	-------------------------	--------------------------	------------------------	--------------------------

All contents are Copyright © 1992--2002 Cisco Systems Inc. All rights reserved. [Important Notices](#) and [Privacy Statement](#).

---

Updated: Oct 09, 2002

Document ID: 27470

---