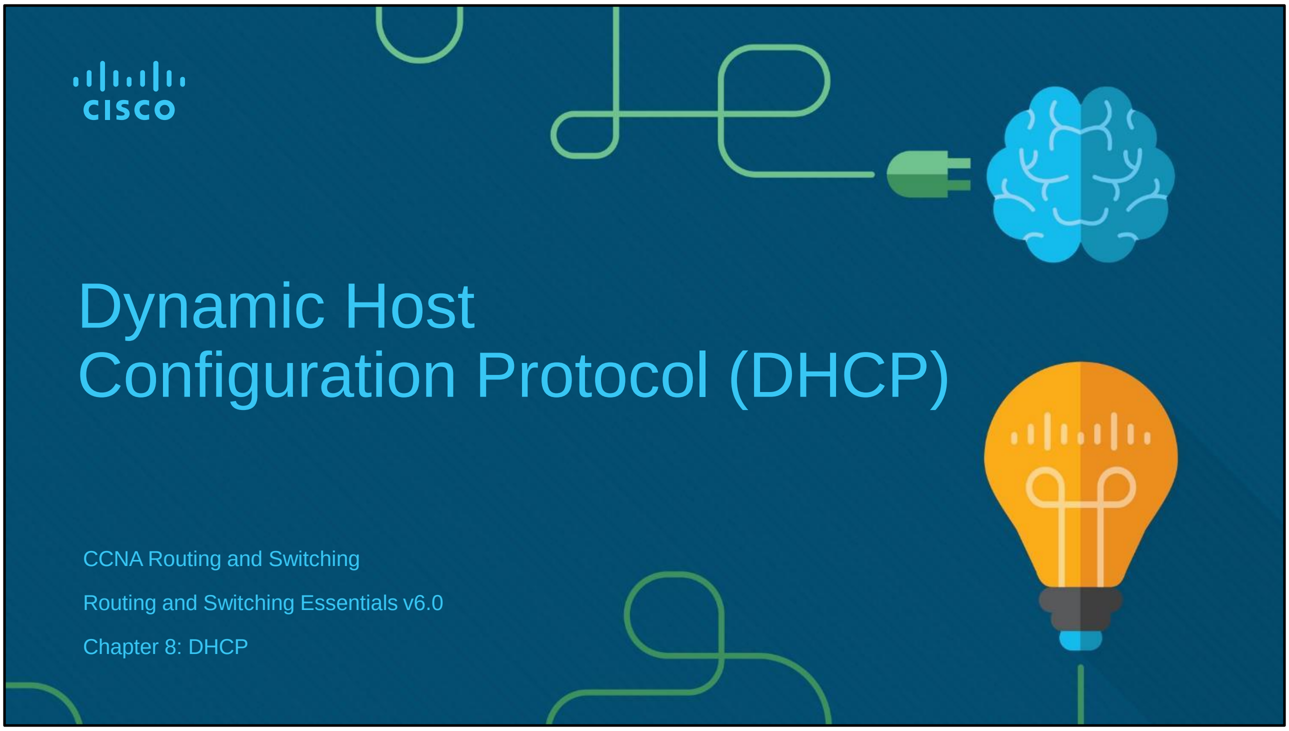
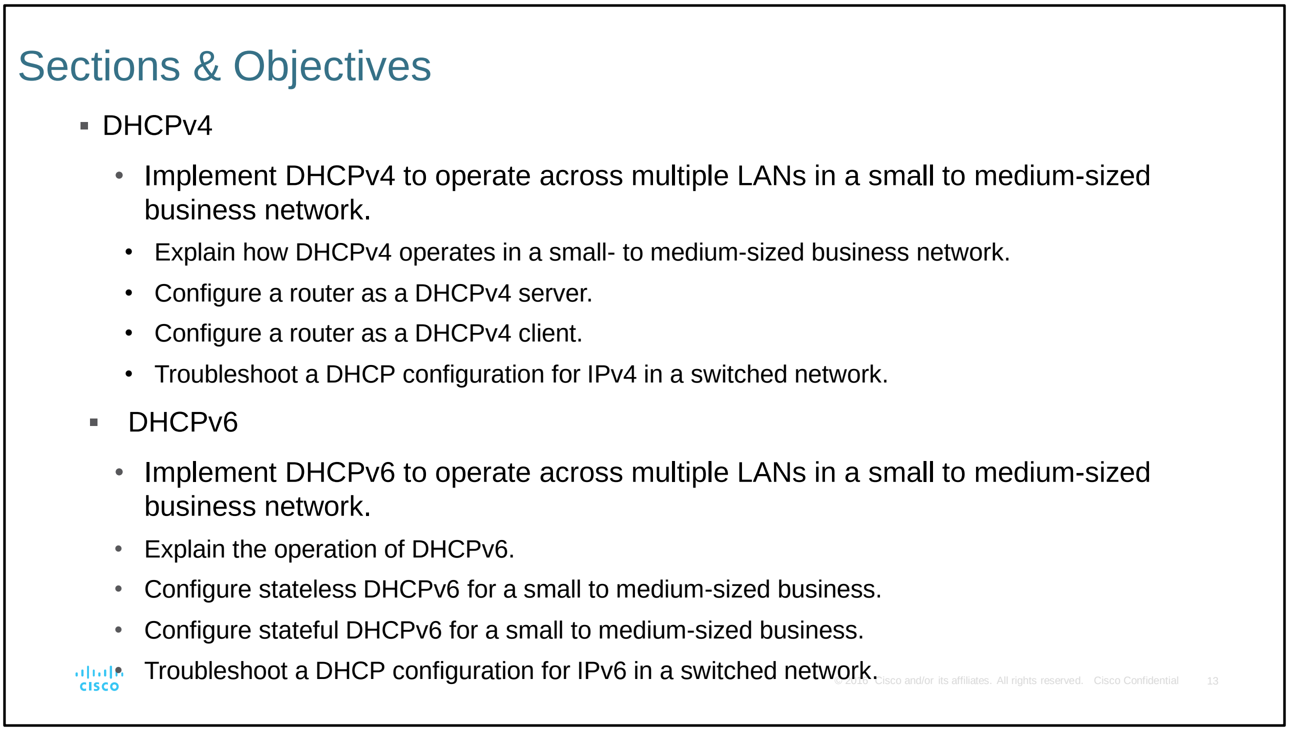


Dynamic Host Configuration Protocol (DHCP)

CCNA Routing and Switching

Routing and Switching Essentials v6.0

Chapter 8: DHCP



Sections & Objectives

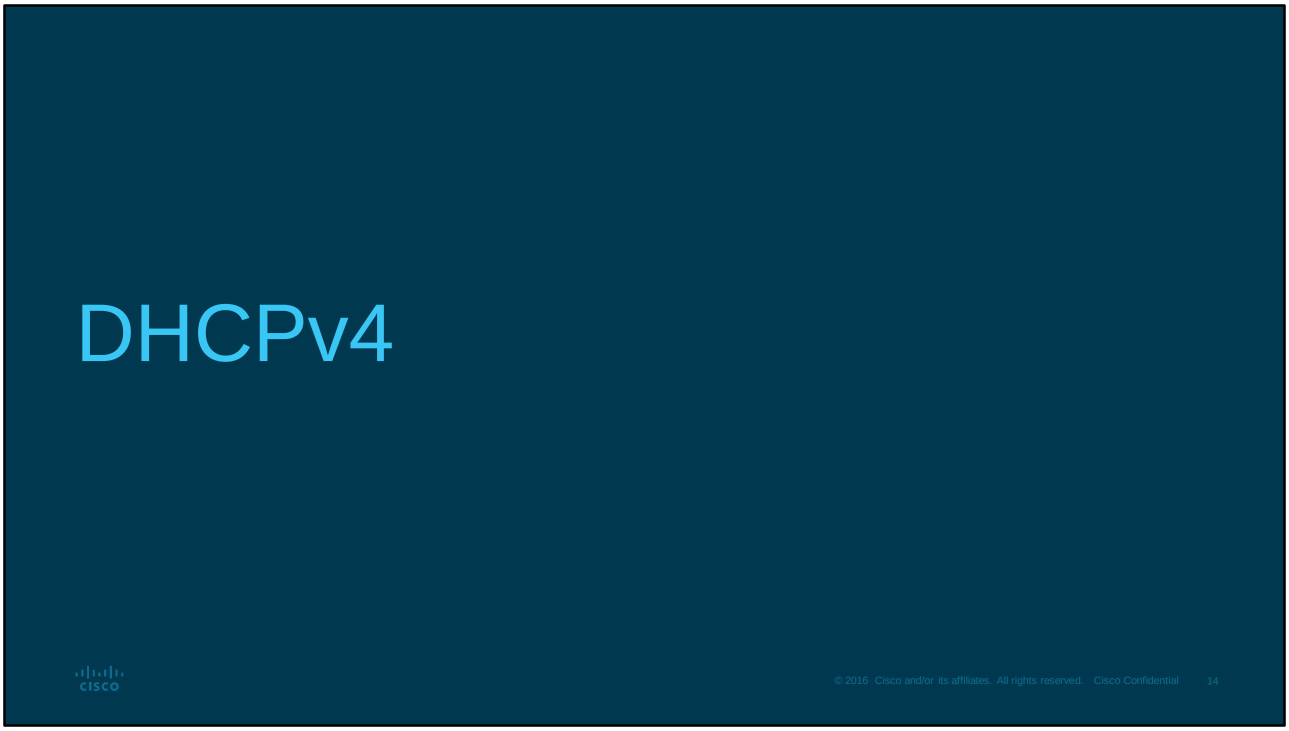
- DHCPv4
  - Implement DHCPv4 to operate across multiple LANs in a small to medium-sized business network.
    - Explain how DHCPv4 operates in a small- to medium-sized business network.
    - Configure a router as a DHCPv4 server.
    - Configure a router as a DHCPv4 client.
    - Troubleshoot a DHCP configuration for IPv4 in a switched network.
- DHCPv6
  - Implement DHCPv6 to operate across multiple LANs in a small to medium-sized business network.
  - Explain the operation of DHCPv6.
  - Configure stateless DHCPv6 for a small to medium-sized business.
  - Configure stateful DHCPv6 for a small to medium-sized business.
  - Troubleshoot a DHCP configuration for IPv6 in a switched network.

Every device that connects to a network needs a unique IP address. Network administrators assign static IP addresses to routers, servers, printers, and other network devices whose locations (physical and logical) are not likely to change. These are usually devices that provide services to users and devices on the network; therefore, the addresses assigned to them should remain constant. Additionally, static addresses enable administrators to manage these devices remotely. It is easier for network administrators to access a device when they can easily determine its IP address.

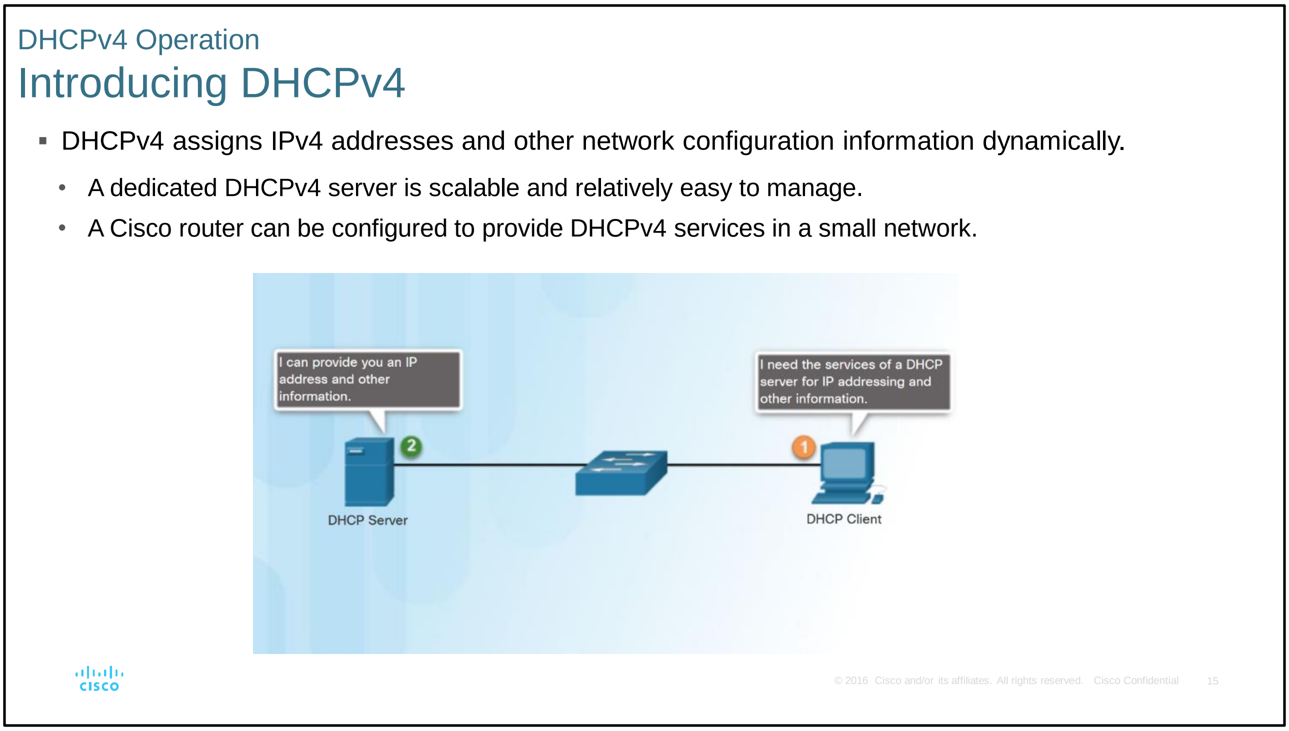
However, computers and users in an organization often change locations, physically and logically. It can be difficult and time consuming for administrators to assign new IP addresses every time an employee moves. Additionally, for mobile employees working from remote locations, manually setting the correct network parameters can be challenging. Even for desktop clients, the manual assignment of IP addresses and other addressing information presents an administrative burden, especially as the network grows.

Introducing a Dynamic Host Configuration Protocol (DHCP) server to the local network simplifies IP address assignment to both desktop and mobile devices. Using a centralized DHCP server enables organizations to administer all dynamic IP address assignments from a single server. This practice makes IP address management more effective and ensures consistency across the organization, including branch offices.

DHCP is available for both IPv4 (DHCPv4) and for IPv6 (DHCPv6). This chapter explores the functionality, configuration, and troubleshooting of both DHCPv4 and DHCPv6.



DHCPv4



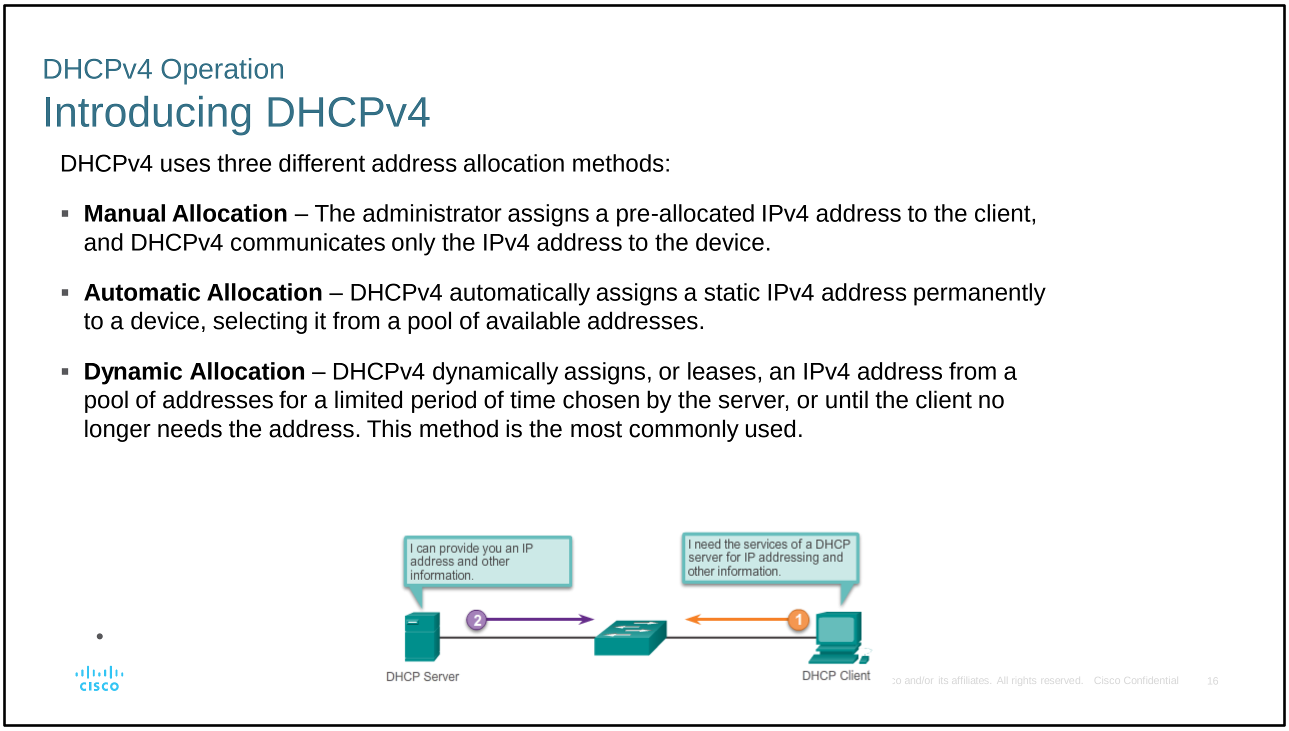
DHCPv4 Operation

Introducing DHCPv4

- DHCPv4 assigns IPv4 addresses and other network configuration information dynamically.
  - A dedicated DHCPv4 server is scalable and relatively easy to manage.
  - A Cisco router can be configured to provide DHCPv4 services in a small network.

I can provide you an IP address and other information.
2
DHCP Server
I need the services of a DHCP server for IP addressing and other information.
1
DHCP Client

DHCPv4 assigns IPv4 addresses and other network configuration information dynamically. Because desktop clients typically make up the bulk of network nodes, DHCPv4 is an extremely useful and timesaving tool for network administrators.
A dedicated DHCPv4 server is scalable and relatively easy to manage. However, in a small branch or SOHO location, a router can be configured to provide DHCPv4 services without the need for a dedicated server.



DHCPv4 Operation

Introducing DHCPv4

DHCPv4 uses three different address allocation methods:

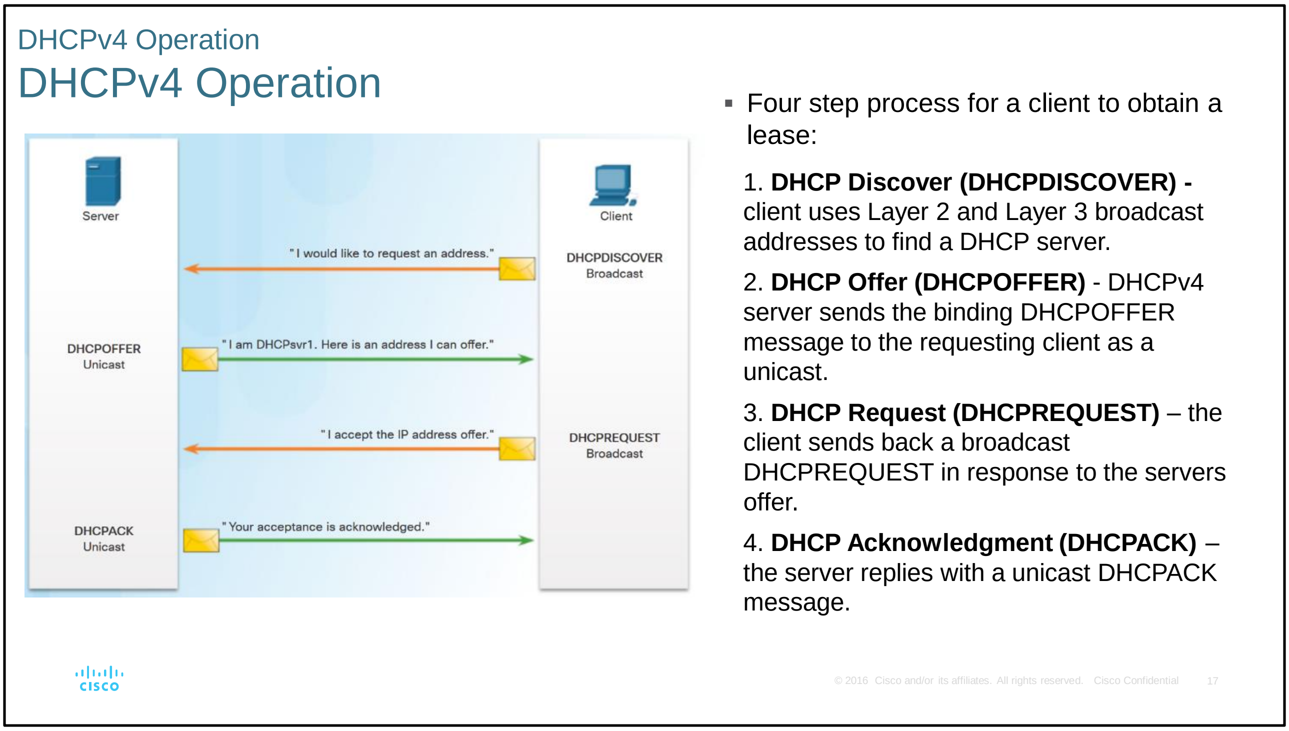
- **Manual Allocation** – The administrator assigns a pre-allocated IPv4 address to the client, and DHCPv4 communicates only the IPv4 address to the device.
- **Automatic Allocation** – DHCPv4 automatically assigns a static IPv4 address permanently to a device, selecting it from a pool of available addresses.
- **Dynamic Allocation** – DHCPv4 dynamically assigns, or leases, an IPv4 address from a pool of addresses for a limited period of time chosen by the server, or until the client no longer needs the address. This method is the most commonly used.

I can provide you an IP address and other information.
I need the services of a DHCP server for IP addressing and other information.
2
1
DHCP Server
DHCP Client

Typically, DHCPv4 includes three different address allocation mechanisms to provide flexibility when assigning IP addresses:

- **Manual Allocation** - The administrator assigns a pre-allocated IPv4 address to the client, and DHCPv4 communicates only the IPv4 address to the device.
- **Automatic Allocation** - DHCPv4 automatically assigns a static IPv4 address permanently to a device, selecting it from a pool of available addresses. There is no lease and the address is permanently assigned to the device.
- **Dynamic Allocation** - DHCPv4 dynamically assigns, or leases, an IPv4 address from a pool of addresses for a limited period of time chosen by the server, or until the client no longer needs the address.

Dynamic allocation is the most commonly used DHCPv4 mechanism and is the focus of this section. When using dynamic allocation, clients lease the information from the server for an administratively defined period, as shown in the figure. Administrators configure DHCPv4 servers to set the leases to time out at different intervals. The lease is typically anywhere from 24 hours to a week or more. When the lease expires, the client must ask for another address, although the client is typically reassigned the same address.



DHCPv4 Operation

DHCPv4 Operation

Server
Client
"I would like to request an address."
DHCPDISCOVER Broadcast
DHCPOFFER Unicast
"I am DHCPsvr1. Here is an address I can offer."
"I accept the IP address offer."
DHCPREQUEST Broadcast
DHCPACK Unicast
"Your acceptance is acknowledged."

- Four step process for a client to obtain a lease:

1. **DHCP Discover (DHCPDISCOVER) -** client uses Layer 2 and Layer 3 broadcast addresses to find a DHCP server.
2. **DHCP Offer (DHCPOFFER)** - DHCPv4 server sends the binding DHCPOFFER message to the requesting client as a unicast.
3. **DHCP Request (DHCPREQUEST)** – the client sends back a broadcast DHCPREQUEST in response to the servers offer.
4. **DHCP Acknowledgment (DHCPACK)** – the server replies with a unicast DHCPACK message.

As shown in figure, DHCPv4 works in a client/server mode. When a client communicates with a DHCPv4 server, the server assigns or leases an IPv4 address to that client. The client connects to the network with that leased IP address until the lease expires. The client must contact the DHCP server periodically to extend the lease. This lease mechanism ensures that clients that move or power off do not keep addresses that they no longer need. When a lease expires, the DHCP server returns the address to the pool where it can be reallocated as necessary.

Lease Origination

When the client boots (or otherwise wants to join a network), it begins a four-step process to obtain a lease. As shown in figure, a client starts the process with a broadcast DHCPDISCOVER message with its own MAC address to discover available DHCPv4 servers.

DHCP Discover (DHCPDISCOVER)

The DHCPDISCOVER message finds DHCPv4 servers on the network. Because the client has no valid IPv4 information at bootup, it uses Layer 2 and Layer 3 broadcast addresses to communicate with the server.

DHCP Offer (DHCPOFFER)

When the DHCPv4 server receives a DHCPDISCOVER message, it reserves an available IPv4 address to lease to the client. The server also creates an ARP entry consisting of the MAC address of the requesting client and the leased IPv4 address of the client. The DHCPv4 server sends the binding DHCPOFFER message to the requesting client.

The DHCPOFFER message is sent as a unicast, using the Layer 2 MAC address of the server as the source address and the Layer 2 MAC address of the client as the destination.

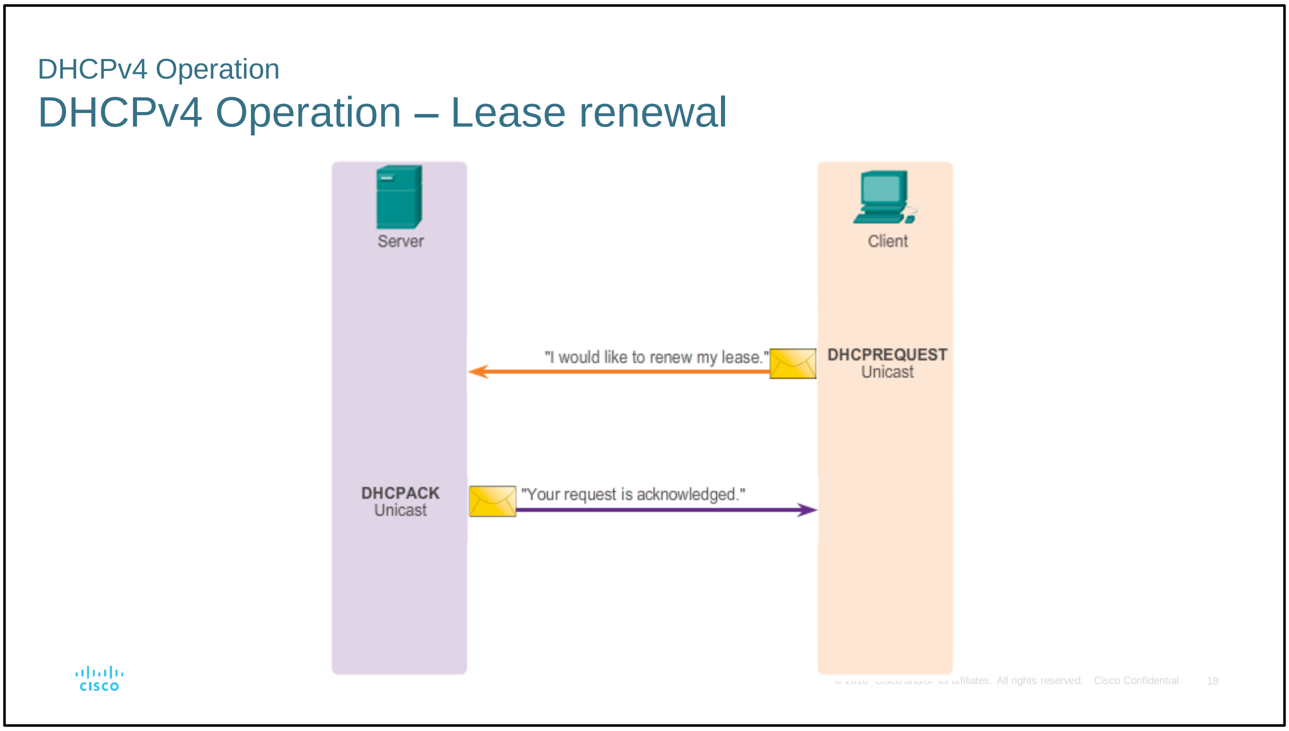
DHCP Request (DHCPREQUEST)

When the client receives the DHCPOFFER from the server, it sends back a DHCPREQUEST message as shown in figure. This message is used for both lease origination and lease renewal. When used for lease origination, the DHCPREQUEST serves as a binding acceptance notice to the selected server for the parameters it has offered and an implicit decline to any other servers that may have provided the client a binding offer.

Many enterprise networks use multiple DHCPv4 servers. The DHCPREQUEST message is sent in the form of a broadcast to inform this DHCPv4 server and any other DHCPv4 servers about the accepted offer.

DHCP Acknowledgment (DHCPACK)

On receiving the DHCPREQUEST message, the server verifies the lease information with an ICMP ping to that address to ensure it is not being used already, creates a new ARP entry for the client lease, and replies with a unicast DHCPACK message. The DHCPACK message is a duplicate of the DHCPOFFER, except for a change in the message type field. When the client receives the DHCPACK message, it logs the configuration information and performs an ARP lookup for the assigned address. If there is no reply to the ARP, the client knows that the IPv4 address is valid and starts using it as its own.



DHCPv4 Operation

DHCPv4 Operation – Lease renewal

Server

Client

"I would like to renew my lease."

DHCPREQUEST
Unicast

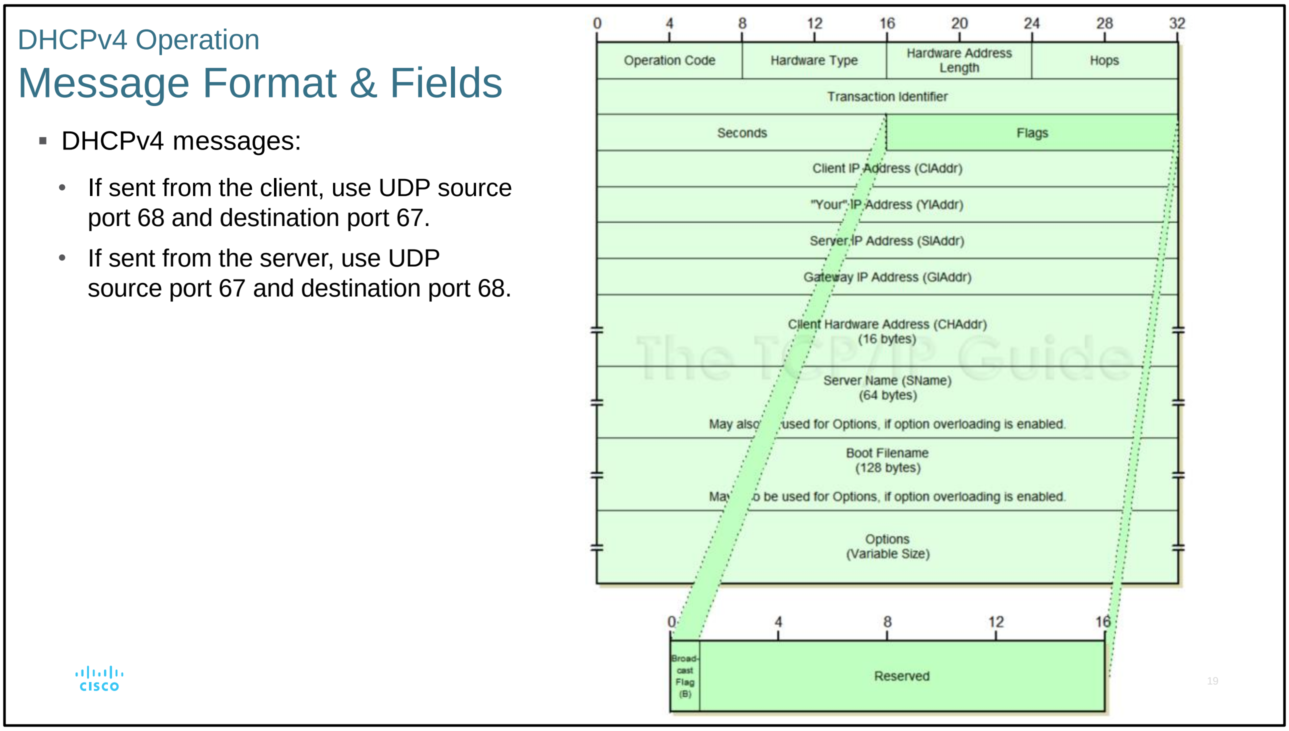
DHCPACK
Unicast

"Your request is acknowledged."

Lease Renewal

DHCP Request (DHCPREQUEST)
As shown in figure, when the lease has expired, the client sends a DHCPREQUEST message directly to the DHCPv4 server that originally offered the IPv4 address. If a DHCPACK is not received within a specified amount of time, the client broadcasts another DHCPREQUEST so that one of the other DHCPv4 servers can extend the lease.

DHCP Acknowledgment (DHCPACK)
On receiving the DHCPREQUEST message, the server verifies the lease information by returning a DHCPACK.



DHCPv4 Operation

Message Format & Fields

- DHCPv4 messages:
  - If sent from the client, use UDP source port 68 and destination port 67.
  - If sent from the server, use UDP source port 67 and destination port 68.

0
4
8
12
16
20
24
28
32
Operation Code
Hardware Type
Hardware Address Length
Hops
Transaction Identifier
Seconds
Flags
Client IP Address (CIAddr)
"Your" IP Address (YIAddr)
Server IP Address (SIAddr)
Gateway IP Address (GIAddr)
Client Hardware Address (CHAddr) (16 bytes)
Server Name (SName) (64 bytes)
May also be used for Options, if option overloading is enabled.
Boot Filename (128 bytes)
May also be used for Options, if option overloading is enabled.
Options (Variable Size)
0
4
8
12
16
Broad-cast Flag (B)
Reserved

CISCO

Operation Code: Specifies the general type of message. A value of 1 indicates a request message, while a value of 2 is a reply message.

This code represents the general category of the DHCP message; a client sending a request to a server uses an *Op* code of 1, while a server replying uses a code of 2. So, for example, a *DHCPREQUEST* would be a request, while a *DHCPACK* or *DHCPNAK* is a reply. The actual specific type of DHCP message is encoded using the DHCP Message Type option.

Hardware Type - Identifies the type of hardware used in the network. For example, 1 is Ethernet, 15 is Frame Relay, and 20 is a serial line. These are the same codes used in ARP messages.

Hardware Address Length: Specifies how long hardware addresses are in this message. For Ethernet or other networks using IEEE 802 MAC addresses, the value is 6. This is also the same as a field in the ARP field format, *HLN*.

Hops: Set to 0 by a client before transmitting a request and used by relay agents to control the forwarding of BOOTP and/or DHCP messages.

Transaction Identifier: A 32-bit identification field generated by the client, to allow it to match up the request with replies received from DHCP servers.

Seconds: In BOOTP this field was vaguely defined and not always used. For DHCP, it is defined as the number of seconds elapsed since a client began an attempt to acquire or renew a lease. This may be used by a busy DHCP server to prioritize replies when multiple client requests are outstanding.

Flags - Used by a client that does not know its IPv4 address when it sends a request. Only one of the 16 bits is used, which is the broadcast flag. A value of 1 in this field tells the DHCPv4 server or relay agent receiving the request that the reply should be sent as a broadcast.

Client IP Address: The client puts its own current IP address in this field if and only if it has a valid IP address while in the *BOUND*, *RENEWING* or *REBINDING* states; otherwise, it sets the field to 0. The client can only use this field when its address is actually valid and usable, not during the process of acquiring an address. Specifically, the client does not use this field to request a particular IP address in a lease; it uses the *Requested IP Address* DHCP option.

"Your" IP Address: The IP address that the server is assigning to the client.

Server IP Address: The meaning of this field is slightly changed in DHCP. In BOOTP, it is the IP address of the BOOTP server sending a *BOOTREPLY* message. In DHCP, it is the address of the server that the client should use for the next step in the bootstrap process, which may or may not be the server sending this reply.

The sending server always includes its own IP address in the *Server Identifier* DHCP option.

Gateway IP Address: This field is used just as it is in BOOTP, to route BOOTP messages when BOOTP relay agents are involved to facilitate the communication of BOOTP requests and replies between a client and a server on different subnets or networks. See the topic on DHCP relaying. As with BOOTP, this field is not used by clients and does not represent the server giving the client the address of a default router (that's done using the *Router* DHCP option).

Client Hardware Address: The hardware (layer two) address of the client, which is used for identification and communication.

Server Name: The server sending a *DHCPOFFER* or *DHCPACK* message may optionally put its name in this field. This can be a simple text "nickname" or a fully-qualified DNS domain name (such as "myserver.organization.org").

This field may also be used to carry DHCP options, using the “option overload” feature, indicated by the value of the DHCP *Option Overload* option.

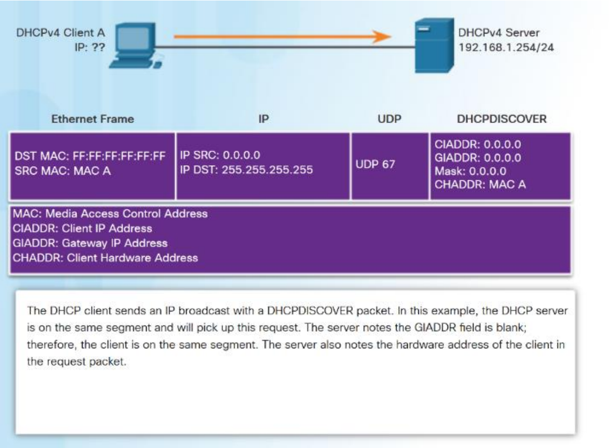
Boot Filename: Optionally used by a client to request a particular type of boot file in a *DHCPDISCOVER* message. Used by a server in a *DHCPOFFER* to fully specify a boot file directory path and filename.

This field may also be used to carry DHCP options, using the “option overload” feature, indicated by the value of the DHCP *Option Overload* option.

Options: Holds DHCP options, including several parameters required for basic DHCP operation. Note that this field was fixed at 64 bytes in length in BOOTP but is variable in length in DHCP. See the next two topics for more information. This field may be used by both client and server.

DHCPv4 Operation

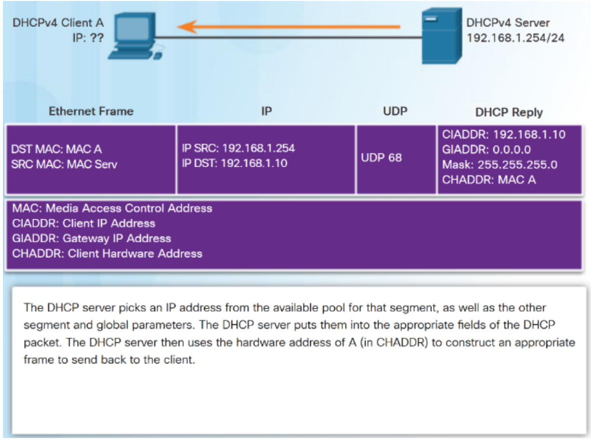
DHCPv4 Discover and Offer Messages



Ethernet Frame	IP	UDP	DHCPDISCOVER
DST MAC: FF:FF:FF:FF:FF:FF SRC MAC: MAC A	IP SRC: 0.0.0.0 IP DST: 255.255.255.255	UDP 67	CIADDR: 0.0.0.0 GIADDR: 0.0.0.0 Mask: 0.0.0.0 CHADDR: MAC A

MAC: Media Access Control Address
CIADDR: Client IP Address
GIADDR: Gateway IP Address
CHADDR: Client Hardware Address

The DHCP client sends an IP broadcast with a DHCPDISCOVER packet. In this example, the DHCP server is on the same segment and will pick up this request. The server notes the GIADDR field is blank; therefore, the client is on the same segment. The server also notes the hardware address of the client in the request packet.



Ethernet Frame	IP	UDP	DHCP Reply
DST MAC: MAC A SRC MAC: MAC Serv	IP SRC: 192.168.1.254 IP DST: 192.168.1.10	UDP 68	CIADDR: 192.168.1.10 GIADDR: 0.0.0.0 Mask: 255.255.255.0 CHADDR: MAC A

MAC: Media Access Control Address
CIADDR: Client IP Address
GIADDR: Gateway IP Address
CHADDR: Client Hardware Address

The DHCP server picks an IP address from the available pool for that segment, as well as the other segment and global parameters. The DHCP server puts them into the appropriate fields of the DHCP packet. The DHCP server then uses the hardware address of A (in CHADDR) to construct an appropriate frame to send back to the client.

If a client is configured to receive its IPv4 settings dynamically and wants to join the network, it requests addressing values from the DHCPv4 server. The client transmits a DHCPDISCOVER message on its local network when it boots or senses an active network connection. Because the client has no way of knowing the subnet to which it belongs, the DHCPDISCOVER message is an IPv4 broadcast (destination IPv4 address of 255.255.255.255). The client does not have a configured IPv4 address yet, so the source IPv4 address of 0.0.0.0 is used.

As shown in figure, the client IPv4 address (CIADDR), default gateway address (GIADDR), and subnet mask are all marked to indicate that the address 0.0.0.0 is used.

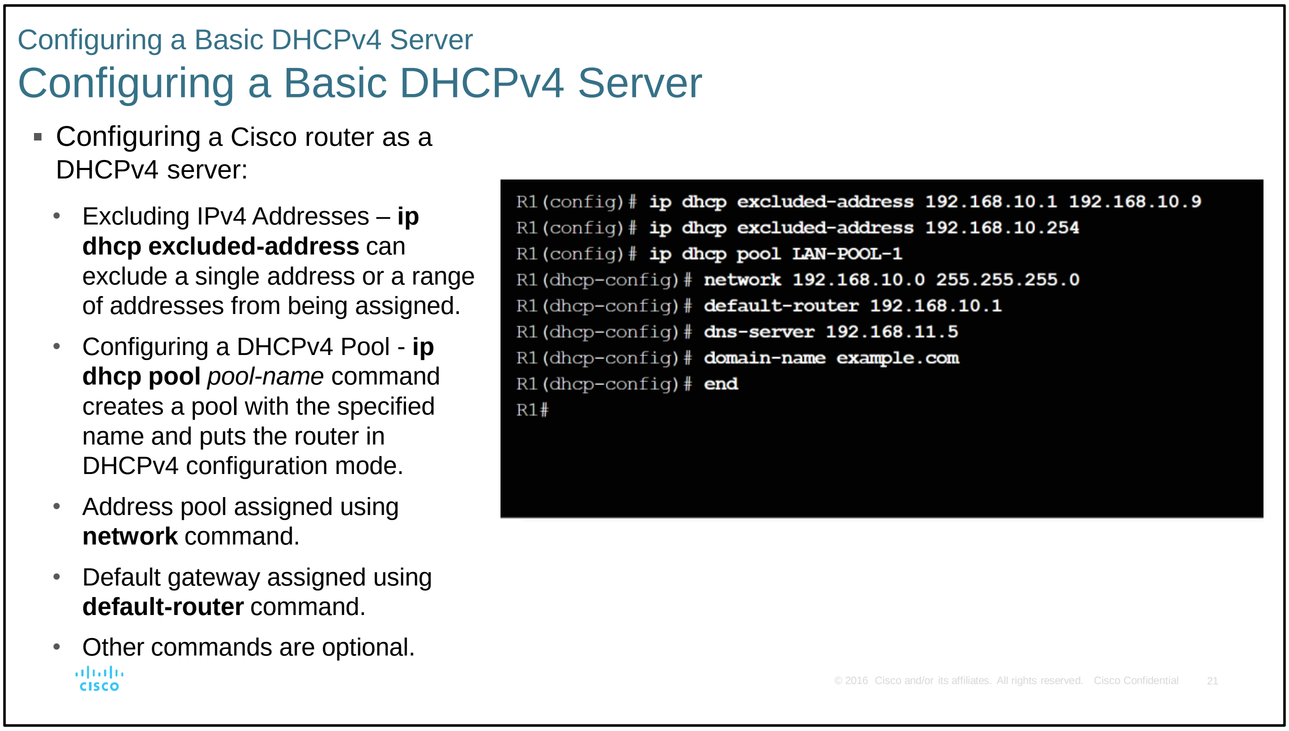
When the DHCPv4 server receives the DHCPDISCOVER message, it responds with a DHCPOFFER message. This message contains initial configuration information for the client, including the IPv4 address that the server offers, the subnet mask, the lease duration, and the IPv4 address of the DHCPv4 server making the offer.

The DHCPOFFER message can be configured to include other information, such as the lease renewal time and DNS address.

As shown in figure, the DHCP server responds to the DHCPDISCOVER by assigning values to the CIADDR and subnet mask. The frame is constructed using the client hardware address (CHADDR) and sent to the requesting client.

The client and server send acknowledgment messages, and the process is complete.

Note: Unknown information is sent as 0.0.0.0.



Configuring a Basic DHCPv4 Server

Configuring a Basic DHCPv4 Server

- Configuring a Cisco router as a DHCPv4 server:
  - Excluding IPv4 Addresses – **ip dhcp excluded-address** can exclude a single address or a range of addresses from being assigned.
  - Configuring a DHCPv4 Pool - **ip dhcp pool** *pool-name* command creates a pool with the specified name and puts the router in DHCPv4 configuration mode.
  - Address pool assigned using **network** command.
  - Default gateway assigned using **default-router** command.
  - Other commands are optional.

```
R1(config)# ip dhcp excluded-address 192.168.10.1 192.168.10.9
R1(config)# ip dhcp excluded-address 192.168.10.254
R1(config)# ip dhcp pool LAN-POOL-1
R1(dhcp-config)# network 192.168.10.0 255.255.255.0
R1(dhcp-config)# default-router 192.168.10.1
R1(dhcp-config)# dns-server 192.168.11.5
R1(dhcp-config)# domain-name example.com
R1(dhcp-config)# end
R1#
```

Step 1. Excluding IPv4 Addresses

The router functioning as the DHCPv4 server assigns all IPv4 addresses in a DHCPv4 address pool unless configured to exclude specific addresses. Typically, some IPv4 addresses in a pool are assigned to network devices that require static address assignments. Therefore, these IPv4 addresses should not be assigned to other devices. To exclude specific addresses, use the **ip dhcp excluded-address** command. A single address or a range of addresses can be excluded by specifying the low-address and high-address of the range. Excluded addresses should include the addresses assigned to routers, servers, printers, and other devices that have been manually configured.

Step 2. Configuring a DHCPv4 Pool

Configuring a DHCPv4 server involves defining a pool of addresses to assign. The **ip dhcp pool** *pool-name* command creates a pool with the specified name and puts the router in DHCPv4 configuration mode, which is identified by this prompt Router(dhcp-config)#.

Step 3. Configuring Specific Tasks

The address pool and default gateway router must be configured. Use the **network** statement to define the range of available addresses.

Use the **default-router** command to define the default gateway router. Typically, the gateway is the LAN interface of the router closest to the client devices. One gateway is required, but you can list up to eight addresses if there are multiple gateways.

Other DHCPv4 pool commands are optional. For example, the IPv4 address of the

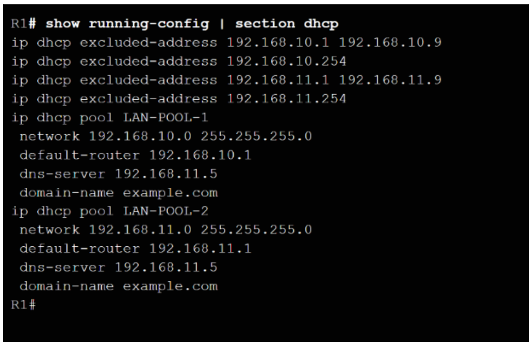
DNS server that is available to a DHCPv4 client is configured using the **dns-server** command. The **domain-name** *domain* command is used to define the domain name. The duration of the DHCPv4 lease can be changed using the **lease** command. The default lease value is one day. The **netbios-name-server** command is used to define the NetBIOS WINS server.

DHCPv4 Example
A sample configuration with basic DHCPv4 parameters configured on router R1, a DHCPv4 server for the 192.168.10.0/24 LAN is shown in figure using the example topology.

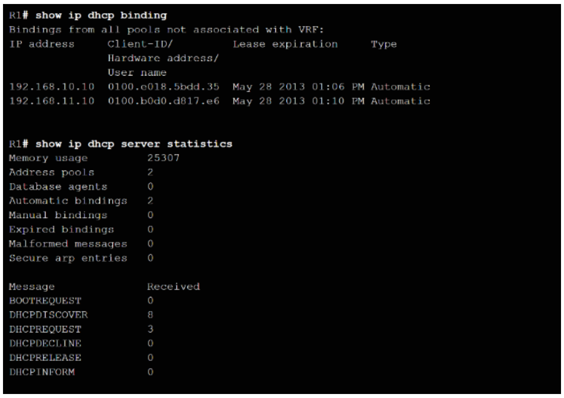
Disabling DHCPv4
The DHCPv4 service is enabled, by default, on versions of Cisco IOS software that support it. To disable the service, use the **no service dhcp** global configuration mode command. Use the **service dhcp** global configuration mode command to re-enable the DHCPv4 server process. Enabling the service has no effect if the parameters are not configured.

Configuring a Basic DHCPv4 Server

Verifying DHCPv4



```
R1# show running-config | section dhcp
ip dhcp excluded-address 192.168.10.1 192.168.10.9
ip dhcp excluded-address 192.168.10.254
ip dhcp excluded-address 192.168.11.1 192.168.11.9
ip dhcp excluded-address 192.168.11.254
ip dhcp pool LAN-POOL-1
 network 192.168.10.0 255.255.255.0
 default-router 192.168.10.1
 dns-server 192.168.11.5
 domain-name example.com
ip dhcp pool LAN-POOL-2
 network 192.168.11.0 255.255.255.0
 default-router 192.168.11.1
 dns-server 192.168.11.5
 domain-name example.com
R1#
```



```
R1# show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address      Client-ID/          Lease expiration      Type
                Hardware address/
                User name
192.168.10.10   0100.e018.5bdd.35   May 28 2013 01:06 PM Automatic
192.168.11.10   0100.b0d0.d817.e6   May 28 2013 01:10 PM Automatic


R1# show ip dhcp server statistics
Memory usage          25307
Address pools         2
Database agents       0
Automatic bindings    2
Manual bindings       0
Expired bindings      0
Malformed messages    0
Secure arp entries    0

Message               Received
BOOTREQUEST           0
DHCPDISCOVER          8
DHCPREQUEST           3
DHCPDECLINE           0
DHCPRELEASE           0
DHCPINFORM            0
```

- Verify DHCPv4 configuration using the **show running-config |section dhcp** command.
- Verify the operation of DHCPv4 using the **show ip dhcp binding** command.
- Verify that messages are being received or sent by the router using the **show ip dhcp server statistics** command.

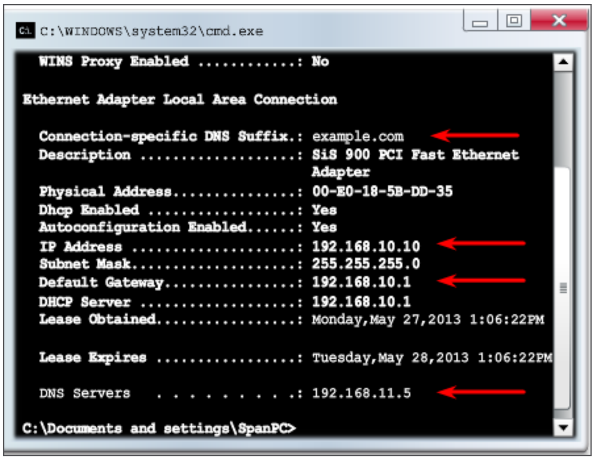
The **show running-config | section dhcp** command output displays the DHCPv4 commands configured on R1. The **| section** parameter displays only the commands associated with DHCPv4 configuration.

The operation of DHCPv4 can be verified using the **show ip dhcp binding** command. This command displays a list of all IPv4 address to MAC address bindings that have been provided by the DHCPv4 service. The command **show ip dhcp server statistics**, is used to verify that messages are being received or sent by the router. This command displays count information regarding the number of DHCPv4 messages that have been sent and received.

DHCPv4 Operation

Verifying a DHCPv4 Client

- Commands to verify DHCP:
- On the PC, issue the **`ipconfig /all`** command.



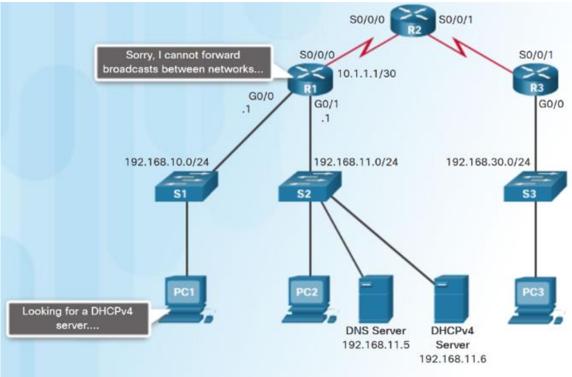
C:\WINDOWS\system32\cmd.exe

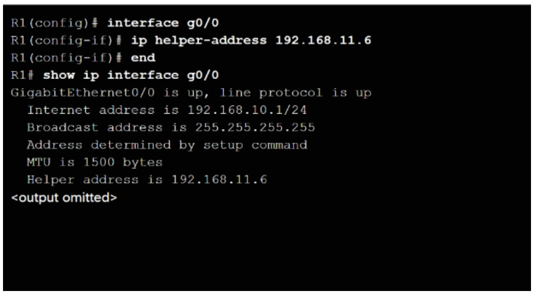
```
  WINS Proxy Enabled ...........: No

Ethernet Adapter Local Area Connection

  Connection-specific DNS Suffix.: example.com
  Description ..................: SiS 900 PCI Fast Ethernet
                                  Adapter
  Physical Address..............: 00-E0-18-5B-DD-35
  Dhcp Enabled .................: Yes
  Autoconfiguration Enabled.....: Yes
  IP Address ...................: 192.168.10.10
  Subnet Mask...................: 255.255.255.0
  Default Gateway...............: 192.168.10.1
  DHCP Server ..................: 192.168.10.1
  Lease Obtained................: Monday,May 27,2013 1:06:22PM

  Lease Expires ................: Tuesday,May 28,2013 1:06:22PM

  DNS Servers   . . . . . . . . .: 192.168.11.5

C:\Documents and settings\SpanPC>
```

As shown in figure, the **ipconfig /all** command, when issued on PC1, displays the TCP/IP parameters. Because PC1 was connected to the network segment 192.168.10.0/24, it automatically received a DNS suffix, IPv4 address, subnet mask, default gateway, and DNS server address from that pool. No router interface configuration is required. If a PC is connected to a network segment that has a DHCPv4 pool available, the PC can obtain an IPv4 address from the appropriate pool automatically.

Configuring a Basic DHCPv4 Server

DHCPv4 Relay





```
R1(config)# interface g0/0
R1(config-if)# ip helper-address 192.168.11.6
R1(config-if)# end
R1# show ip interface g0/0
GigabitEthernet0/0 is up, line protocol is up
  Internet address is 192.168.10.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is 192.168.11.6
<output omitted>
```

- DHCPDISCOVER messages are sent as broadcast messages.
- Routers do not forward broadcasts.
- A Cisco IOS helper address is configured so that the router acts as a relay agent forwarding the message to the DHCPv4 server.

What is DHCP Relay?
In a complex hierarchical network, enterprise servers are usually located in a server farm. These servers may provide DHCP, DNS, TFTP, and FTP services for the network. Network clients are not typically on the same subnet as those servers. In order to locate the servers and receive services, clients often use broadcast messages.
In Figure, PC1 is attempting to acquire an IPv4 address from a DHCP server using a broadcast message. In this scenario, router R1 is not configured as a DHCPv4 server and does not forward the broadcast. Because the DHCPv4 server is located on a different network, PC1 cannot receive an IP address using DHCP.
PC1 is attempting to renew its IPv4 address. To do so, the **ipconfig /release** command is issued. Notice that the IPv4 address is released and the address is shown to be 0.0.0.0. Next, the **ipconfig /renew** command is issued. This command causes PC1 to broadcast a DHCPDISCOVER message. The output shows that PC1 is unable to locate the DHCPv4 server. Because routers do not forward broadcasts, the request is not successful.

As a solution to this problem, an administrator can add DHCPv4 servers on all the subnets. However, running these services on several computers creates additional cost and administrative overhead.

A better solution is to configure a Cisco IOS helper address. This solution enables a router to forward DHCPv4 broadcasts to the DHCPv4 server. When a router forwards address assignment/parameter requests, it is acting as a DHCPv4 relay agent.

In the example topology, PC1 would broadcast a request to locate a DHCPv4 server. If R1 was configured as a DHCPv4 relay agent, it would forward the request to the DHCPv4 server located on subnet 192.168.11.0.

As shown in figure, the interface on R1 receiving the broadcast is configured with the **ip helper-address** interface configuration mode command. The address of the DHCPv4 server is configured as the only parameter.

When R1 has been configured as a DHCPv4 relay agent, it accepts broadcast requests for the DHCPv4 service and then forwards those requests as a unicast to the IPv4 address 192.168.11.6. The **show ip interface** command is used to verify the configuration.

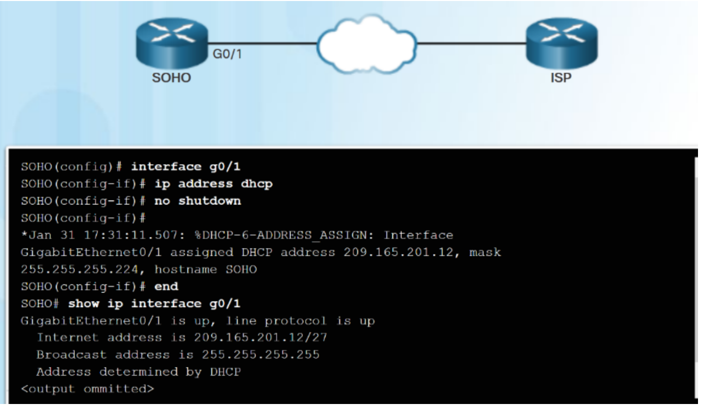
PC1 is now able to acquire an IPv4 address from the DHCPv4 server.
DHCPv4 is not the only service that the router can be configured to relay. By default, the **ip helper-address** command forwards the following eight UDP services:

- Port 37: Time
- Port 49: TACACS
- Port 53: DNS
- Port 67: DHCP/BOOTP client
- Port 68: DHCP/BOOTP server
- Port 69: TFTP
- Port 137: NetBIOS name service
- Port 138: NetBIOS datagram service

Configuring DHCPv4 Client

Configuring a Router as DHCPv4 Client

- Small office/home office (SOHO) and branch sites often have to be configured as DHCPv4 clients.
- Use the **ip address dhcp** interface configuration mode command.



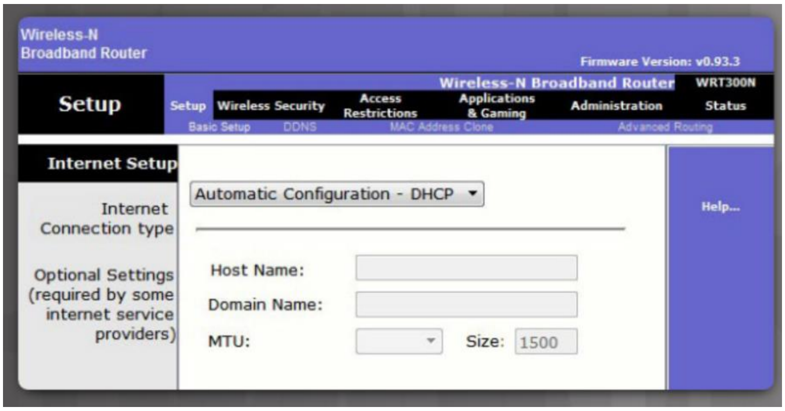
```
SOHO(config)# interface g0/1
SOHO(config-if)# ip address dhcp
SOHO(config-if)# no shutdown
SOHO(config-if)#
*Jan 31 17:31:11.507: %DHCP-6-ADDRESS_ASSIGN: Interface
GigabitEthernet0/1 assigned DHCP address 209.165.201.12, mask
255.255.255.224, hostname SOHO
SOHO(config-if)# end
SOHO# show ip interface g0/1
GigabitEthernet0/1 is up, line protocol is up
  Internet address is 209.165.201.12/27
  Broadcast address is 255.255.255.255
  Address determined by DHCP
<output ommitted>
```

Sometimes, Cisco routers in small office/home office (SOHO) and branch sites have to be configured as DHCPv4 clients in a similar manner to client computers. The method used depends on the ISP. However, in its simplest configuration, the Ethernet interface is used to connect to a cable or DSL modem.

To configure an Ethernet interface as a DHCP client, use the **ip address dhcp** interface configuration mode command.
In the figure, assume that an ISP has been configured to provide select customers with IP addresses from the 209.165.201.0/27 network range. After the G0/1 interface is configured with the **ip address dhcp** command, the **show ip interface g0/1** command confirms that the interface is up and that the address was allocated by a DHCPv4 server.

Configuring DHCPv4 Client

Configuring a Wireless Router as a DHCPv4 Client



Internet Setup

Internet Connection type: Automatic Configuration - DHCP

Optional Settings (required by some internet service providers)

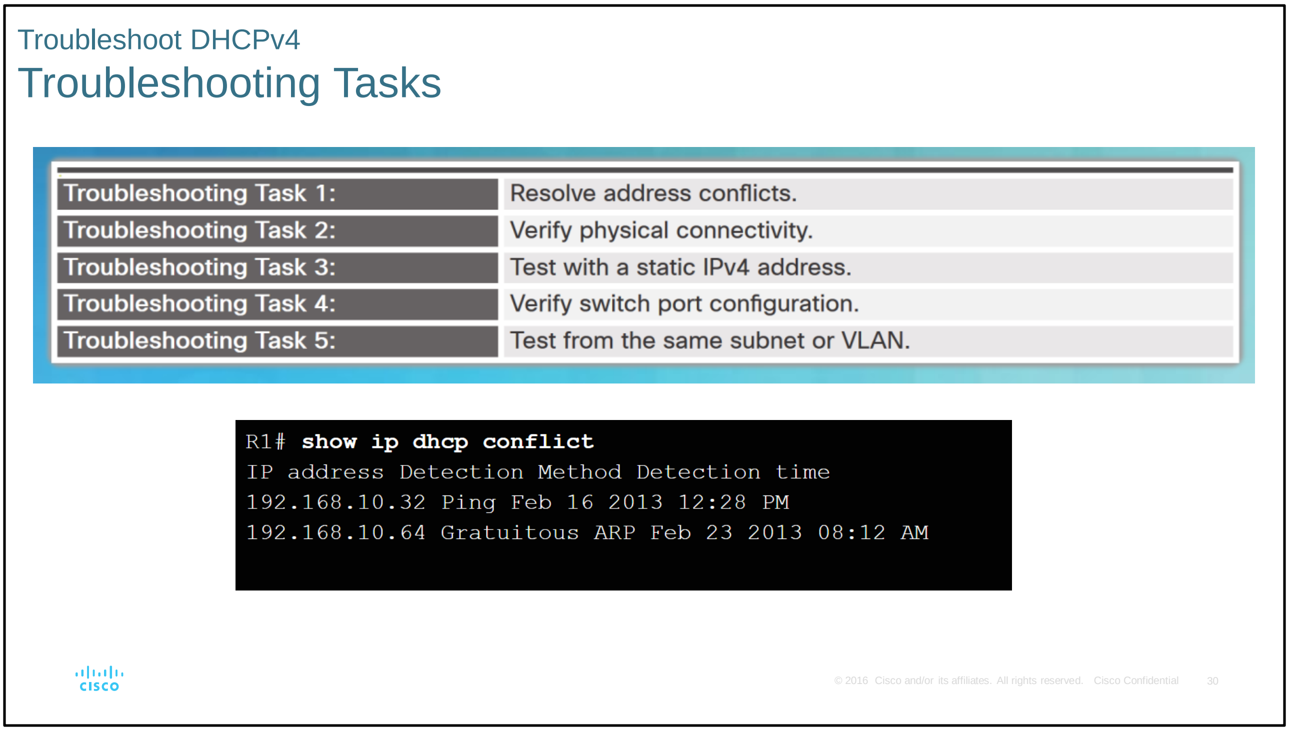
Host Name:

Domain Name:

MTU: Size: 1500

- Wireless routers are set to receive IPv4 addressing information automatically from the ISP.

8.1 – DHCPv4
8.1.3 – Configure DHCPv4 Client
8.1.3.2 – Configuring a Wireless Router as a DHCPv4 Client



Troubleshoot DHCPv4

Troubleshooting Tasks

Troubleshooting Task 1:	Resolve address conflicts.
Troubleshooting Task 2:	Verify physical connectivity.
Troubleshooting Task 3:	Test with a static IPv4 address.
Troubleshooting Task 4:	Verify switch port configuration.
Troubleshooting Task 5:	Test from the same subnet or VLAN.

```
R1# show ip dhcp conflict
IP address Detection Method Detection time
192.168.10.32 Ping Feb 16 2013 12:28 PM
192.168.10.64 Gratuitous ARP Feb 23 2013 08:12 AM
```

DHCPv4 problems can arise for a multitude of reasons, such as software defects in operating systems, NIC drivers, or DHCP relay agents, but the most common are configuration issues. Because of the number of potentially problematic areas, a systematic approach to troubleshooting is required, as shown in the figure.

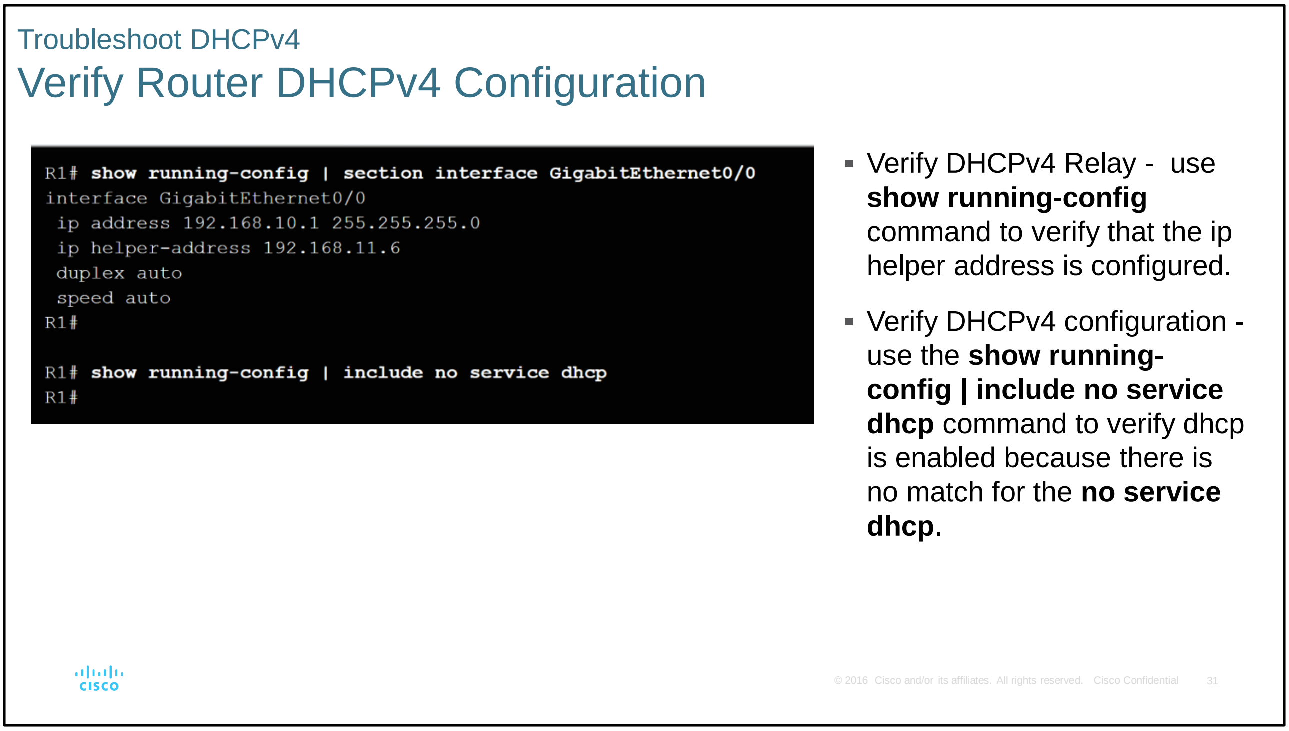
Troubleshooting Task 1: Resolve IPv4 Address Conflicts
An IPv4 address lease can expire on a client still connected to a network. If the client does not renew the lease, the DHCPv4 server can reassign that IPv4 address to another client. When the client reboots, it requests an IPv4 address. If the DHCPv4 server does not respond quickly, the client uses the last IPv4 address. The situation then arises where two clients are using the same IPv4 address, creating a conflict. The **show ip dhcp conflict** command displays all address conflicts recorded by the DHCPv4 server. The server uses the **ping** command to detect clients. The client uses Address Resolution Protocol (ARP) to detect conflicts. If an address conflict is detected, the address is removed from the pool and not assigned until an administrator resolves the conflict.

Troubleshooting Task 2: Verify Physical Connectivity
First, use the **show interface** *interface* command to confirm that the router interface acting as the default gateway for the client is operational. If the state of the interface is anything other than up, the port does not pass traffic, including DHCP client requests.

Troubleshooting Task 3: Test Connectivity using a Static IP Address
When troubleshooting any DHCPv4 issue, verify network connectivity by configuring static IPv4 address information on a client workstation. If the workstation is unable to reach network resources with a statically configured IPv4 address, the root cause of the problem is not DHCPv4. At this point, network connectivity troubleshooting is required.

Troubleshooting Task 4: Verify Switch Port Configuration
If the DHCPv4 client is unable to obtain an IPv4 address from the DHCPv4 server on startup, attempt to obtain an IPv4 address from the DHCPv4 server by manually forcing the client to send a DHCPv4 request.
Note: If there is a switch between the client and the DHCPv4 server, and the client is unable to obtain the DHCP configuration, switch port configuration issues may be the cause. These causes may include issues from trunking and channeling, STP, and RSTP. PortFast configuration and edge port configurations resolve the most common DHCPv4 client issues that occur with an initial installation of a Cisco switch.

Troubleshooting Task 5: Test DHCPv4 Operation on the Same Subnet or VLAN
It is important to distinguish whether DHCPv4 is functioning correctly when the client is on the same subnet or VLAN as the DHCPv4 server. If DHCPv4 is working correctly when the client is on the same subnet or VLAN, the problem may be the DHCP relay agent. If the problem persists even with testing DHCPv4 on the same subnet or VLAN as the DHCPv4 server, the problem may actually be with the DHCPv4 server.



Troubleshoot DHCPv4

Verify Router DHCPv4 Configuration

```
R1# show running-config | section interface GigabitEthernet0/0
interface GigabitEthernet0/0
 ip address 192.168.10.1 255.255.255.0
 ip helper-address 192.168.11.6
 duplex auto
 speed auto
R1#

R1# show running-config | include no service dhcp
R1#
```

- Verify DHCPv4 Relay - use **show running-config** command to verify that the ip helper address is configured.
- Verify DHCPv4 configuration - use the **show running-config | include no service dhcp** command to verify dhcp is enabled because there is no match for the **no service dhcp**.

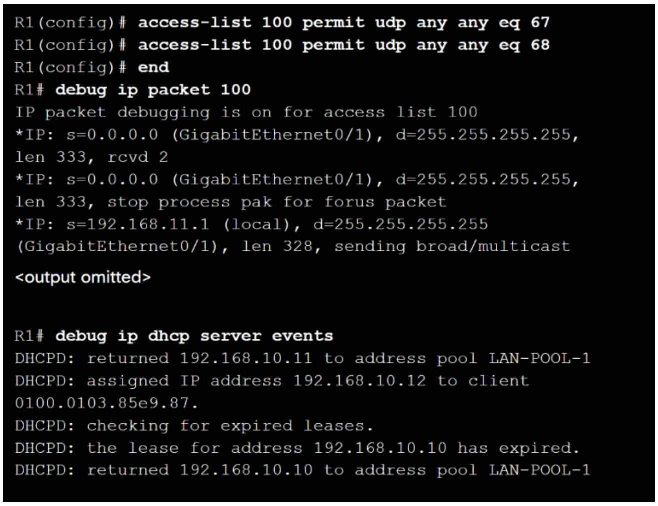
When the DHCPv4 server is located on a separate LAN from the client, the router interface facing the client must be configured to relay DHCPv4 requests by configuring the IPv4 helper address. If the IPv4 helper address is not configured properly, client DHCPv4 requests are not forwarded to the DHCPv4 server.
Follow these steps to verify the router configuration:

- **Step 1.** Verify that the **ip helper-address** command is configured on the correct interface. It must be present on the inbound interface of the LAN containing the DHCPv4 client workstations and must be directed to the correct DHCPv4 server. In the figure, the output of the **show running-config** command verifies that the DHCPv4 relay IPv4 address is referencing the DHCPv4 server address at 192.168.11.6. The **show ip interface** command can also be used to verify the DHCPv4 relay on an interface.
- **Step 2.** Verify that the global configuration command **no service dhcp** has not been configured. This command disables all DHCP server and relay functionality on the router. The command **service dhcp** does not appear in the running-config, because it is the default configuration. In the figure, the **show running-config | include no service dhcp** command verifies that the DHCPv4 service is enabled since there is no match for the **show running-config | include no service dhcp** command. If the service had been disabled, the **no service dhcp** command would be displayed in the output.

Troubleshoot DHCPv4

Debugging DHCPv4

- The extended ACL is used with the **debug ip packet** command to display only DHCPv4 messages.
- Another troubleshooting command is the **debug ip dhcp server events**.



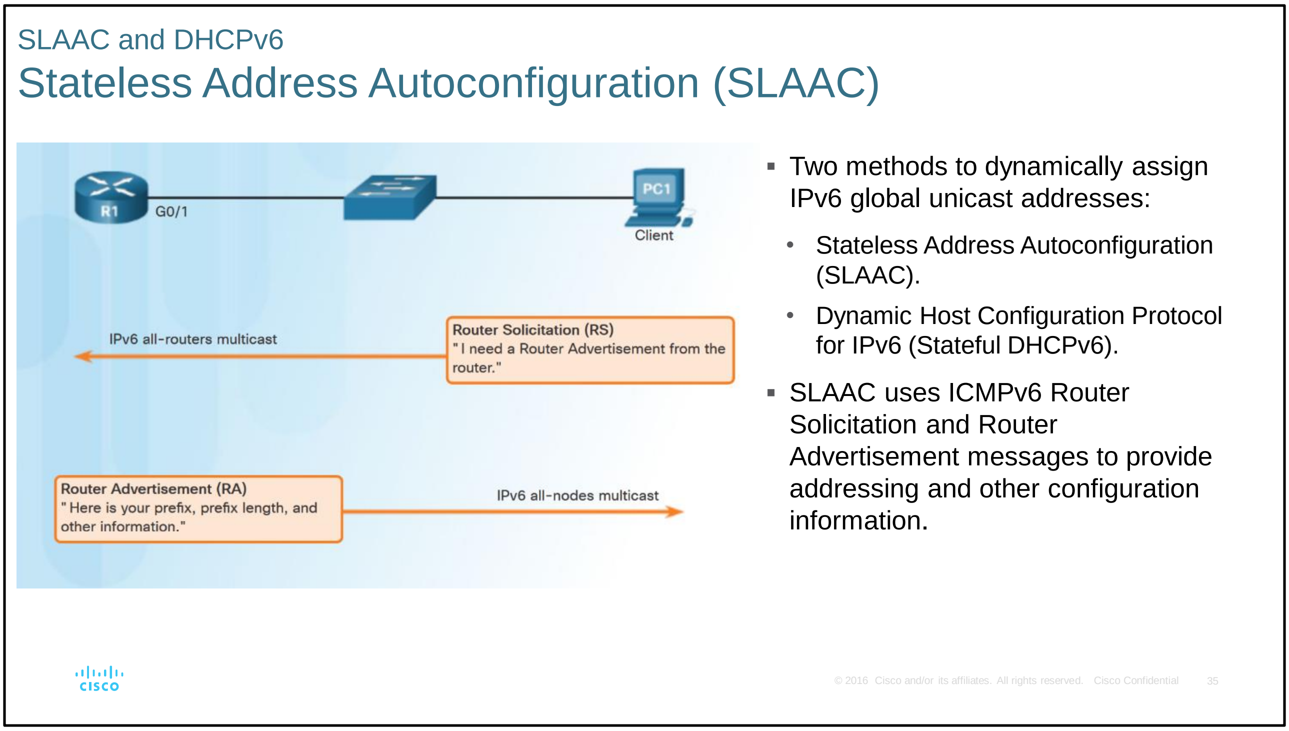
```
R1(config)# access-list 100 permit udp any any eq 67
R1(config)# access-list 100 permit udp any any eq 68
R1(config)# end
R1# debug ip packet 100
IP packet debugging is on for access list 100
*IP: s=0.0.0.0 (GigabitEthernet0/1), d=255.255.255.255,
len 333, rcvd 2
*IP: s=0.0.0.0 (GigabitEthernet0/1), d=255.255.255.255,
len 333, stop process pak for forus packet
*IP: s=192.168.11.1 (local), d=255.255.255.255
(GigabitEthernet0/1), len 328, sending broad/multicast
<output omitted>

R1# debug ip dhcp server events
DHCPD: returned 192.168.10.11 to address pool LAN-POOL-1
DHCPD: assigned IP address 192.168.10.12 to client
0100.0103.85e9.87.
DHCPD: checking for expired leases.
DHCPD: the lease for address 192.168.10.10 has expired.
DHCPD: returned 192.168.10.10 to address pool LAN-POOL-1
```

On routers configured as DHCPv4 servers, the DHCPv4 process fails if the router is not receiving requests from the client. As a troubleshooting task, verify that the router is receiving the DHCPv4 request from the client. This troubleshooting step involves configuring an ACL for debugging output.

The figure shows an extended ACL permitting only packets with UDP destination ports of 67 or 68. These are the typical ports used by DHCPv4 clients and servers when sending DHCPv4 messages. The extended ACL is used with the **debug ip packet** command to display only DHCPv4 messages.
The output in the figure shows that the router is receiving DHCP requests from the client. The source IP address is 0.0.0.0 because the client does not yet have an IP address. The destination is 255.255.255.255 because the DHCP discovery message from the client is sent as a broadcast. This output only shows a summary of the packet and not the DHCPv4 message itself. Nevertheless, the router did receive a broadcast packet with the source and destination IP and UDP ports that are correct for DHCPv4. The complete debug output shows all the packets in the DHCPv4 communications between the DHCPv4 server and client.
Another useful command for troubleshooting DHCPv4 operation is the **debug ip dhcp server events** command. This command reports server events, like address assignments and database updates. It is also used for decoding DHCPv4 receptions and transmissions.

DHCPv6

8 - DHCP
8.2 – DHCPv6



SLAAC and DHCPv6

Stateless Address Autoconfiguration (SLAAC)

R1
G0/1
PC1
Client
IPv6 all-routers multicast
Router Solicitation (RS)
" I need a Router Advertisement from the router."
Router Advertisement (RA)
" Here is your prefix, prefix length, and other information."
IPv6 all-nodes multicast

- Two methods to dynamically assign IPv6 global unicast addresses:
  - Stateless Address Autoconfiguration (SLAAC).
  - Dynamic Host Configuration Protocol for IPv6 (Stateful DHCPv6).
- SLAAC uses ICMPv6 Router Solicitation and Router Advertisement messages to provide addressing and other configuration information.

35

Similar to IPv4, IPv6 global unicast addresses can be configured manually or dynamically. However, there are two methods in which IPv6 global unicast addresses can be assigned dynamically:

- Stateless Address Autoconfiguration (SLAAC), as shown in the figure
- Dynamic Host Configuration Protocol for IPv6 (Stateful DHCPv6)

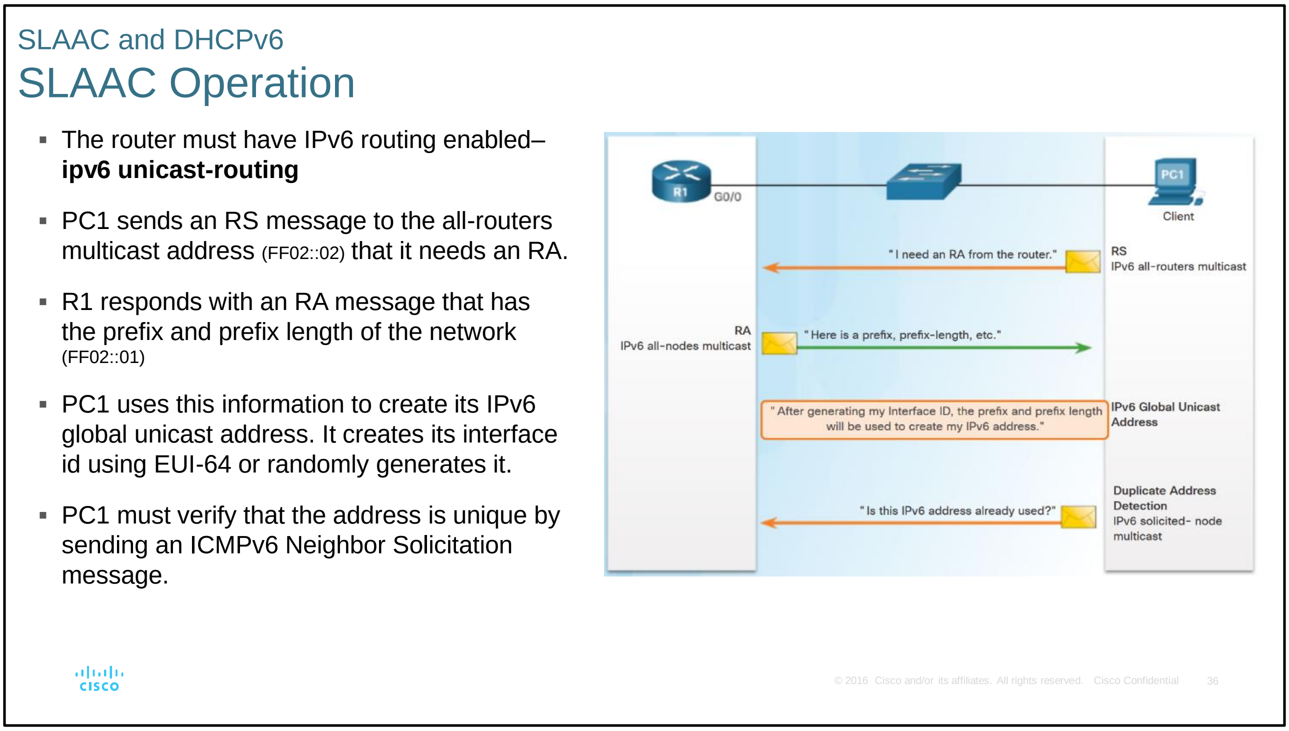
Introducing SLAAC

SLAAC is a method in which a device can obtain an IPv6 global unicast address without the services of a DHCPv6 server. At the core of SLAAC is ICMPv6. ICMPv6 is similar to ICMPv4 but includes additional functionality and is a much more robust protocol. SLAAC uses ICMPv6 Router Solicitation and Router Advertisement messages to provide addressing and other configuration information that would normally be provided by a DHCP server:

- **Router Solicitation (RS) message** - When a client is configured to obtain its addressing information automatically using SLAAC, the client sends an RS message to the router. The RS message is sent to the IPv6 all-routers multicast address FF02::2.
- **Router Advertisement (RA) message** - RA messages are sent by routers to provide addressing information to clients configured to obtain their IPv6 addresses automatically. The RA message includes the prefix and prefix length of the local segment. A client uses this information to create its own IPv6 global unicast

address. A router sends an RA message periodically, or in response to an RS message. By default, Cisco routers send RA messages every 200 seconds. RA messages are always sent to the IPv6 all-nodes multicast address FF02::1.

As the name indicates, SLAAC is stateless. A stateless service means there is no server that maintains network address information. Unlike DHCP, there is no SLAAC server that knows which IPv6 addresses are being used and which ones are available.



SLAAC and DHCPv6

SLAAC Operation

- The router must have IPv6 routing enabled– **ipv6 unicast-routing**
- PC1 sends an RS message to the all-routers multicast address (FF02::02) that it needs an RA.
- R1 responds with an RA message that has the prefix and prefix length of the network (FF02::01)
- PC1 uses this information to create its IPv6 global unicast address. It creates its interface id using EUI-64 or randomly generates it.
- PC1 must verify that the address is unique by sending an ICMPv6 Neighbor Solicitation message.

R1
G0/0
PC1
Client
"I need an RA from the router."
RS
IPv6 all-routers multicast
RA
IPv6 all-nodes multicast
"Here is a prefix, prefix-length, etc."
"After generating my Interface ID, the prefix and prefix length will be used to create my IPv6 address."
IPv6 Global Unicast Address
"Is this IPv6 address already used?"
Duplicate Address Detection
IPv6 solicited- node multicast

A router must be enabled as an IPv6 router before it can send RA messages. To enable IPv6 routing, a router is configured with the following command:
Router(config)# **ipv6 unicast-routing**

1. In the example topology shown in figure, PC1 is configured to obtain IPv6 addressing automatically. Since booting, PC1 has not received an RA message, so it sends an RS message to the all-routers multicast address to inform the local IPv6 router that it needs an RA.

2. R1 receives the RS message and responds with an RA message. Included in the RA message are the prefix and prefix length of the network. The RA message is sent to the IPv6 all-nodes multicast address FF02::1, with the link-local address of the router as the IPv6 source address.

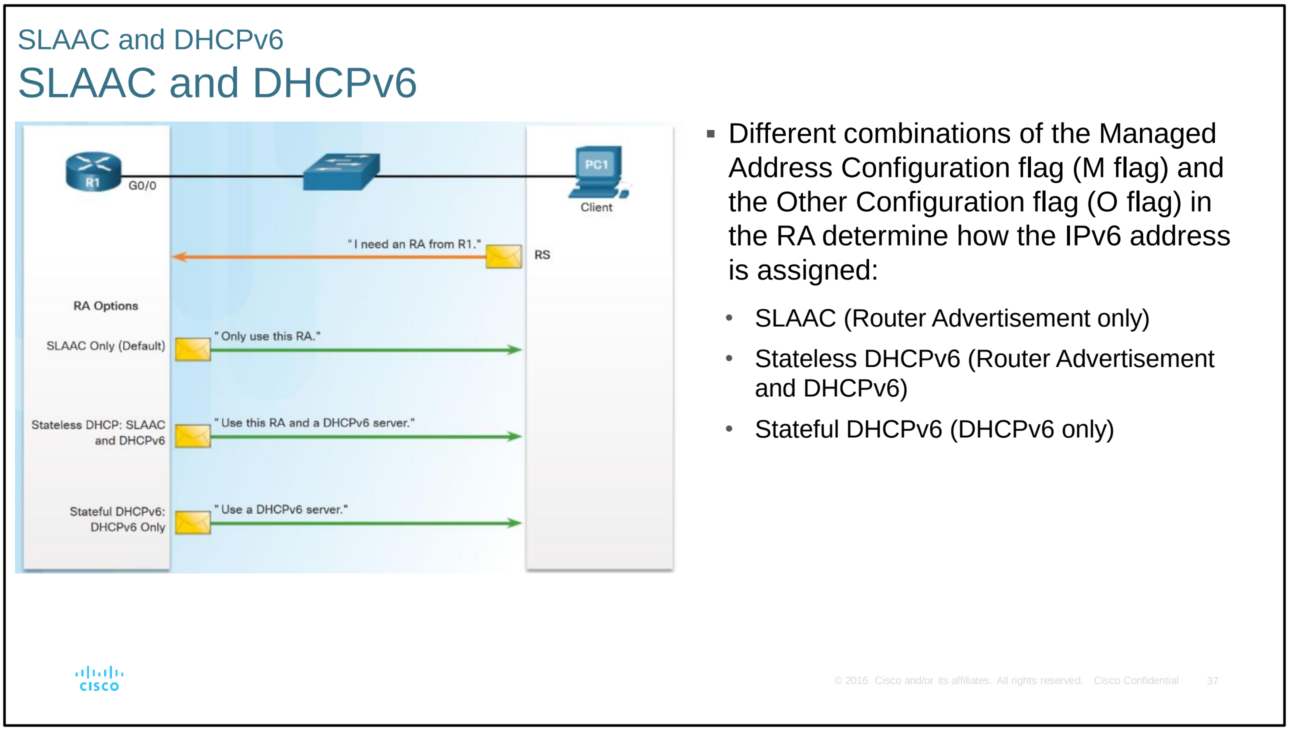
3. PC1 receives the RA message containing the prefix and prefix length for the local network. PC1 will use this information to create its own IPv6 global unicast address. PC1 now has a 64-bit network prefix but needs a 64-bit Interface ID (IID) to create a global unicast address.
There are two ways PC1 can create its own unique IID:

- **EUI-64** - Using the EUI-64 process, PC1 will create an IID using its 48-bit MAC address.
- **Randomly generated** - The 64-bit IID can be a random number generated by the

client operating system.

As shown in figure, PC1 can create a 128-bit IPv6 global unicast address by combining the 64-bit prefix with the 64-bit IID. PC1 will use the link-local address of the router as its IPv6 default gateway address.

4. Because SLAAC is a stateless process, before PC1 can use this newly created IPv6 address it must verify that it is unique. As shown in figure, PC1 sends an ICMPv6 Neighbor Solicitation message with its own address as the target IPv6 address. If no other devices respond with a Neighbor Advertisement message, then the address is unique and can be used by PC1. If a Neighbor Advertisement is received by PC1 then the address is not unique, and the operating system must determine a new Interface ID to use.
This process is part of ICMPv6 Neighbor Discovery and is known as Duplicate Address Detection (DAD).



SLAAC and DHCPv6

SLAAC and DHCPv6

R1 G0/0

PC1 Client

"I need an RA from R1."

RS

RA Options

SLAAC Only (Default) "Only use this RA."

Stateless DHCP: SLAAC and DHCPv6 "Use this RA and a DHCPv6 server."

Stateful DHCPv6: DHCPv6 Only "Use a DHCPv6 server."

- Different combinations of the Managed Address Configuration flag (M flag) and the Other Configuration flag (O flag) in the RA determine how the IPv6 address is assigned:
  - SLAAC (Router Advertisement only)
  - Stateless DHCPv6 (Router Advertisement and DHCPv6)
  - Stateful DHCPv6 (DHCPv6 only)

The decision of whether a client is configured to obtain its IPv6 addressing information automatically using SLAAC, DHCPv6, or a combination of both depends on the settings within the RA message. ICMPv6 RA messages contain two flags to indicate which option the client should use.

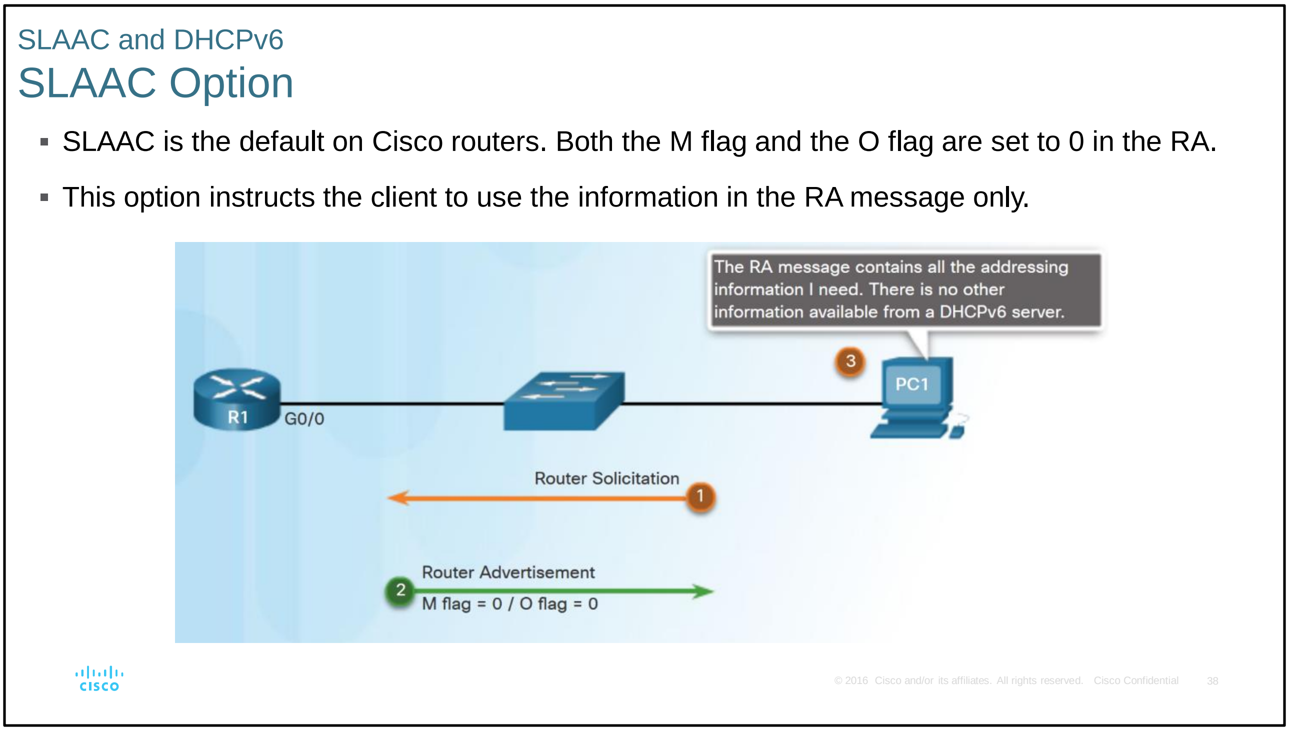
The two flags are the Managed Address Configuration flag (M flag) and the Other Configuration flag (O flag).

Using different combinations of the M and O flags, RA messages have one of three addressing options for the IPv6 device, as shown in the figure:

- SLAAC (Router Advertisement only)
- Stateless DHCPv6 (Router Advertisement and DHCPv6)
- Stateful DHCPv6 (DHCPv6 only)

Regardless of the option used, it is recommended by RFC 4861 that all IPv6 devices perform Duplicate Address Detection (DAD) on any unicast address, including addresses configured using SLAAC or DHCPv6.

Note: Although the RA message specifies the process the client should use in obtaining an IPv6 address dynamically, the client operating system may choose to ignore the RA message and use the services of a DHCPv6 server exclusively.



SLAAC and DHCPv6

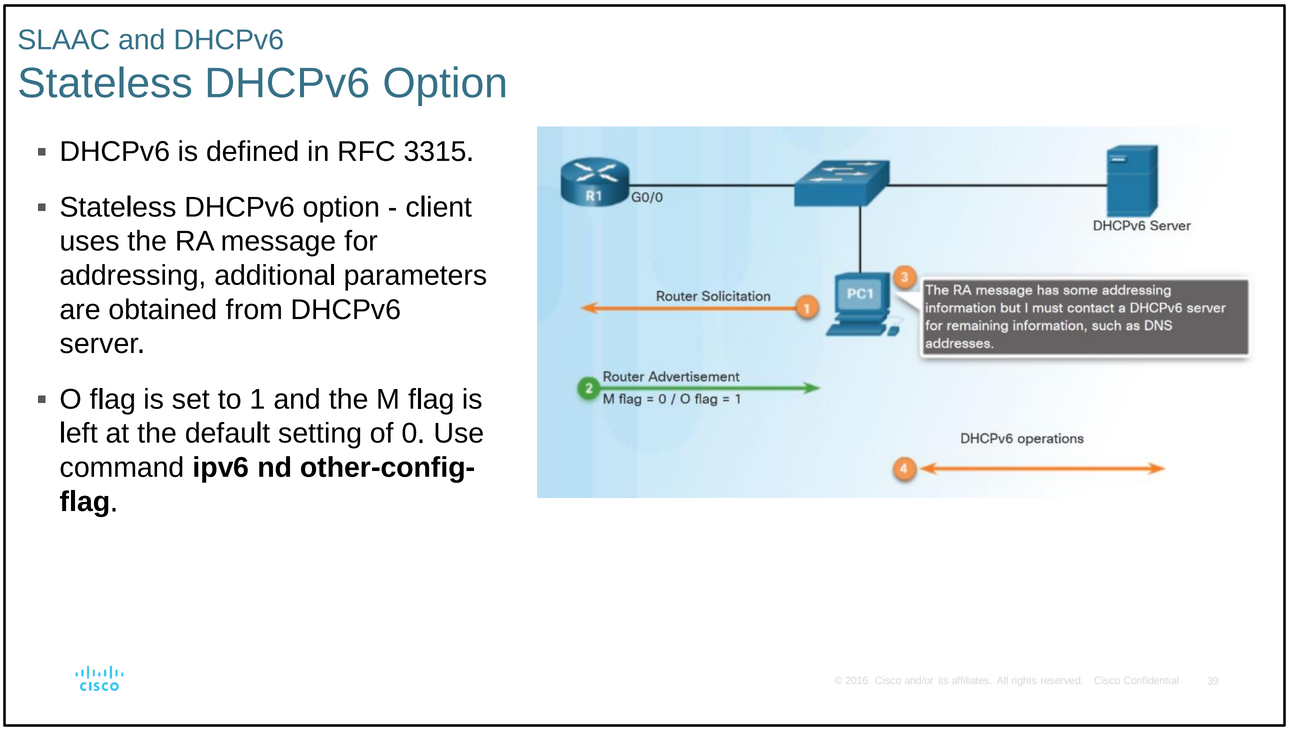
SLAAC Option

- SLAAC is the default on Cisco routers. Both the M flag and the O flag are set to 0 in the RA.
- This option instructs the client to use the information in the RA message only.

The RA message contains all the addressing information I need. There is no other information available from a DHCPv6 server.

SLAAC Option (Router Advertisement only)
SLAAC is the default option on Cisco routers. Both the M flag and the O flag are set to 0 in the RA, as shown in the figure.
This option instructs the client to use the information in the RA message exclusively. This includes prefix, prefix-length, DNS server, MTU, and default gateway information. There is no further information available from a DHCPv6 server. The IPv6 global unicast address is created by combining the prefix from RA and an Interface ID using either EUI-64 or a randomly generated value.
RA messages are configured on an individual interface of a router. To re-enable an interface for SLAAC that might have been set to another option, the M and O flags need to be reset to their initial values of 0. This is done using the following interface configuration mode commands:

```
Router(config-if)# no ipv6 nd managed-config-flag

Router(config-if)# no ipv6 nd other-config-flag
```



SLAAC and DHCPv6

Stateless DHCPv6 Option

- DHCPv6 is defined in RFC 3315.
- Stateless DHCPv6 option - client uses the RA message for addressing, additional parameters are obtained from DHCPv6 server.
- O flag is set to 1 and the M flag is left at the default setting of 0. Use command **ipv6 nd other-config-flag**.

The RA message has some addressing information but I must contact a DHCPv6 server for remaining information, such as DNS addresses.

Although DHCPv6 is similar to DHCPv4 in what it provides, the two protocols are independent of each other. DHCPv6 is defined in RFC 3315. There has been a lot of work done on this specification over the years as indicated by the fact that DHCPv6 RFC has the highest revision number of any Internet draft.

Stateless DHCPv6 Option (Router Advertisement and DHCPv6)
The stateless DHCPv6 option informs the client to use the information in the RA message for addressing, but additional configuration parameters are available from a DHCPv6 server.
Using the prefix and prefix length in the RA message, along with EUI-64 or a randomly generated IID, the client creates its IPv6 global unicast address.
The client will then communicate with a stateless DHCPv6 server to obtain additional information not provided in the RA message. This may be a list of DNS server IPv6 addresses, for example. This process is known as stateless DHCPv6 because the server is not maintaining any client state information (i.e., a list of available and allocated IPv6 addresses). The stateless DHCPv6 server is only providing configuration parameters for clients, not IPv6 addresses.

For stateless DHCPv6, the O flag is set to 1 and the M flag is left at the default setting of 0. The O flag value of 1 is used to inform the client that additional configuration information is available from a stateless DHCPv6 server.
To modify the RA message sent on the interface of a router to indicate stateless

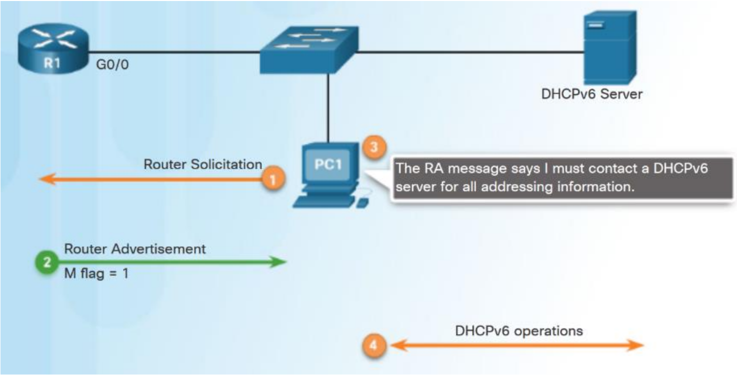
DHCPv6, use the following command:

```
Router(config-if)# ipv6 nd other-config-flag
```

SLAAC and DHCPv6

Stateful DHCPv6 Option

- RA message informs the client not to use the information in the RA message.
- All addressing and configuration information must be obtained from a stateful DHCPv6 server.
- M flag is set to 1. Use the command **ipv6 nd managed-config-flag**.



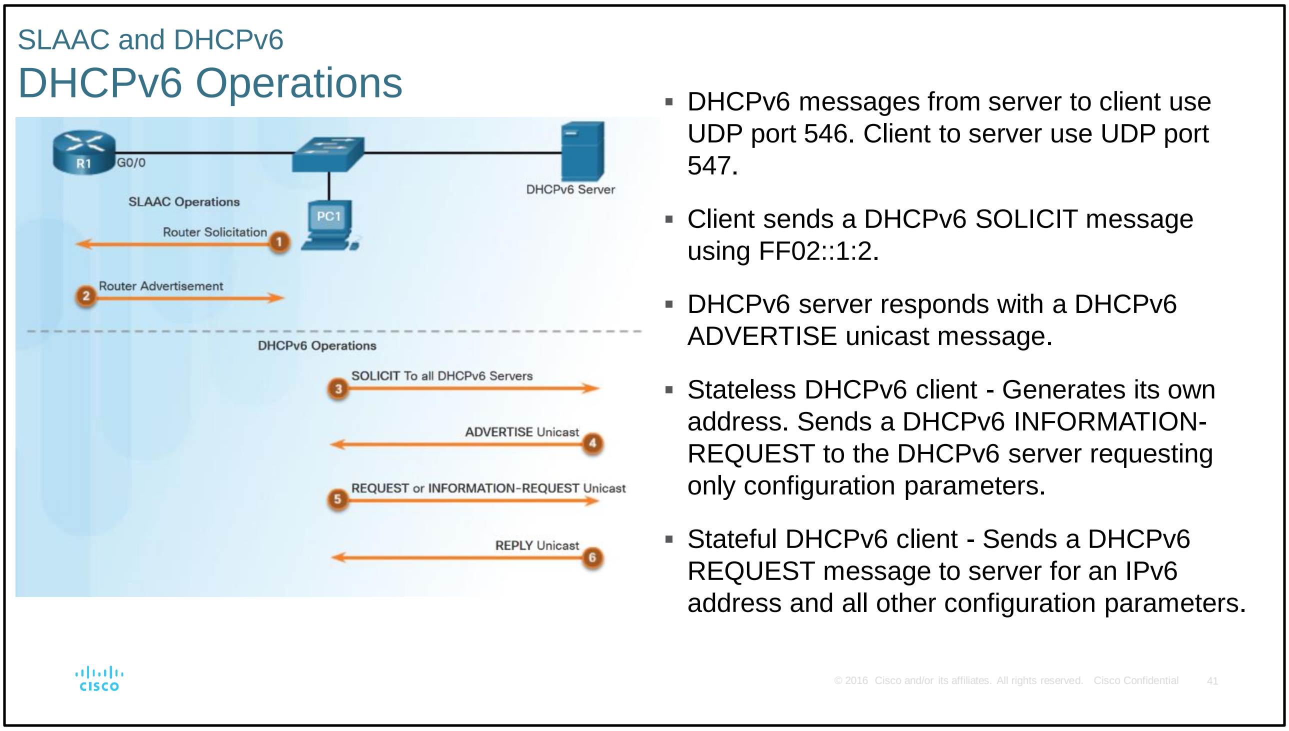
The RA message says I must contact a DHCPv6 server for all addressing information.

Stateful DHCPv6 (DHCPv6 only)

This option is the most similar to DHCPv4. In this case, the RA message informs the client not to use the information in the RA message. All addressing information and configuration information must be obtained from a stateful DHCPv6 server. This is known as stateful DHCPv6 because the DHCPv6 server maintains IPv6 state information. This is similar to a DHCPv4 server allocating addresses for IPv4.

The M flag indicates whether or not to use stateful DHCPv6. The O flag is not involved. The following command is used to change the M flag from 0 to 1 to signify stateful DHCPv6:

Router(config-if)# **ipv6 nd managed-config-flag**



SLAAC and DHCPv6

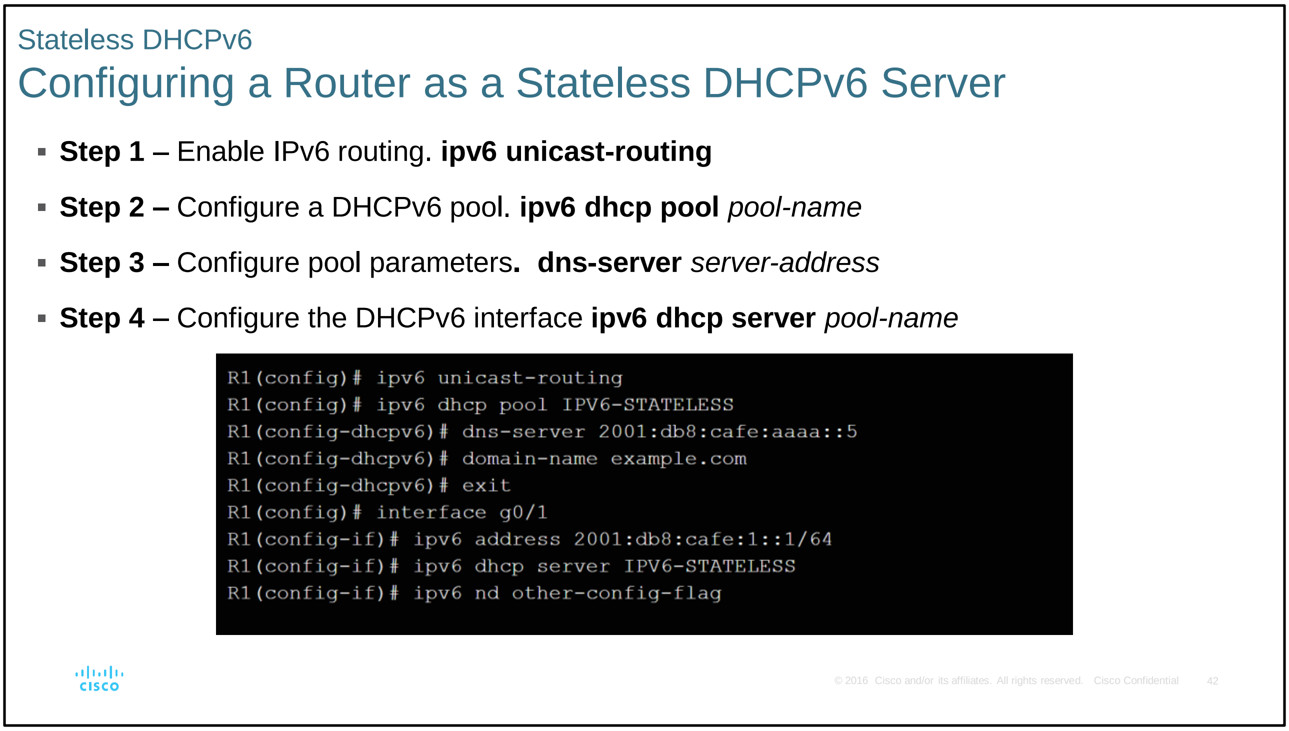
DHCPv6 Operations

- DHCPv6 messages from server to client use UDP port 546. Client to server use UDP port 547.
- Client sends a DHCPv6 SOLICIT message using FF02::1:2.
- DHCPv6 server responds with a DHCPv6 ADVERTISE unicast message.
- Stateless DHCPv6 client - Generates its own address. Sends a DHCPv6 INFORMATION-REQUEST to the DHCPv6 server requesting only configuration parameters.
- Stateful DHCPv6 client - Sends a DHCPv6 REQUEST message to server for an IPv6 address and all other configuration parameters.

As shown in figure, stateless or stateful DHCPv6, or both begin with an ICMPv6 RA message from the router. The RA message might have been a periodic message or solicited by the device using an RS message.
If stateless or stateful DHCPv6 is indicated in the RA message, then the device begins DHCPv6 client/server communications.

DHCPv6 Communications
When stateless DHCPv6 or stateful DHCPv6 is indicated by the RA, DHCPv6 operation is invoked. DHCPv6 messages are sent over UDP. DHCPv6 messages from the server to the client use UDP destination port **546**. The client sends DHCPv6 messages to the server using UDP destination port **547**.
The client, now a DHCPv6 client, needs to locate a DHCPv6 server. The client sends a DHCPv6 SOLICIT message to the reserved IPv6 multicast all-DHCPv6-servers address **FF02::1:2**. This multicast address has link-local scope, which means routers do not forward the messages to other networks.
One or more DHCPv6 servers respond with a DHCPv6 ADVERTISE message. The ADVERTISE message informs the DHCPv6 client that the server is available for DHCPv6 service.
The client responds with a DHCPv6 REQUEST or INFORMATION-REQUEST message to the server, depending on whether it is using stateful or stateless DHCPv6.
Stateless DHCPv6 client - The client sends a DHCPv6 INFORMATION-REQUEST message to the DHCPv6 server requesting only configuration parameters, such as

DNS server address. The client generated its own IPv6 address using the prefix from the RA message and a self-generated Interface ID.
Stateful DHCPv6 client - The client sends a DHCPv6 REQUEST message to the server to obtain an IPv6 address and all other configuration parameters from the server.
The server sends a DHCPv6 REPLY to the client containing the information requested in the REQUEST or INFORMATION-REQUEST message.



Stateless DHCPv6

Configuring a Router as a Stateless DHCPv6 Server

- **Step 1 –** Enable IPv6 routing. **ipv6 unicast-routing**
- **Step 2 –** Configure a DHCPv6 pool. **ipv6 dhcp pool** *pool-name*
- **Step 3 –** Configure pool parameters**. dns-server** *server-address*
- **Step 4 –** Configure the DHCPv6 interface **ipv6 dhcp server** *pool-name*

```
R1(config)# ipv6 unicast-routing
R1(config)# ipv6 dhcp pool IPV6-STATELESS
R1(config-dhcpv6)# dns-server 2001:db8:cafe:aaaa::5
R1(config-dhcpv6)# domain-name example.com
R1(config-dhcpv6)# exit
R1(config)# interface g0/1
R1(config-if)# ipv6 address 2001:db8:cafe:1::1/64
R1(config-if)# ipv6 dhcp server IPV6-STATELESS
R1(config-if)# ipv6 nd other-config-flag
```

There are four steps to configure a router as a DHCPv6 server:

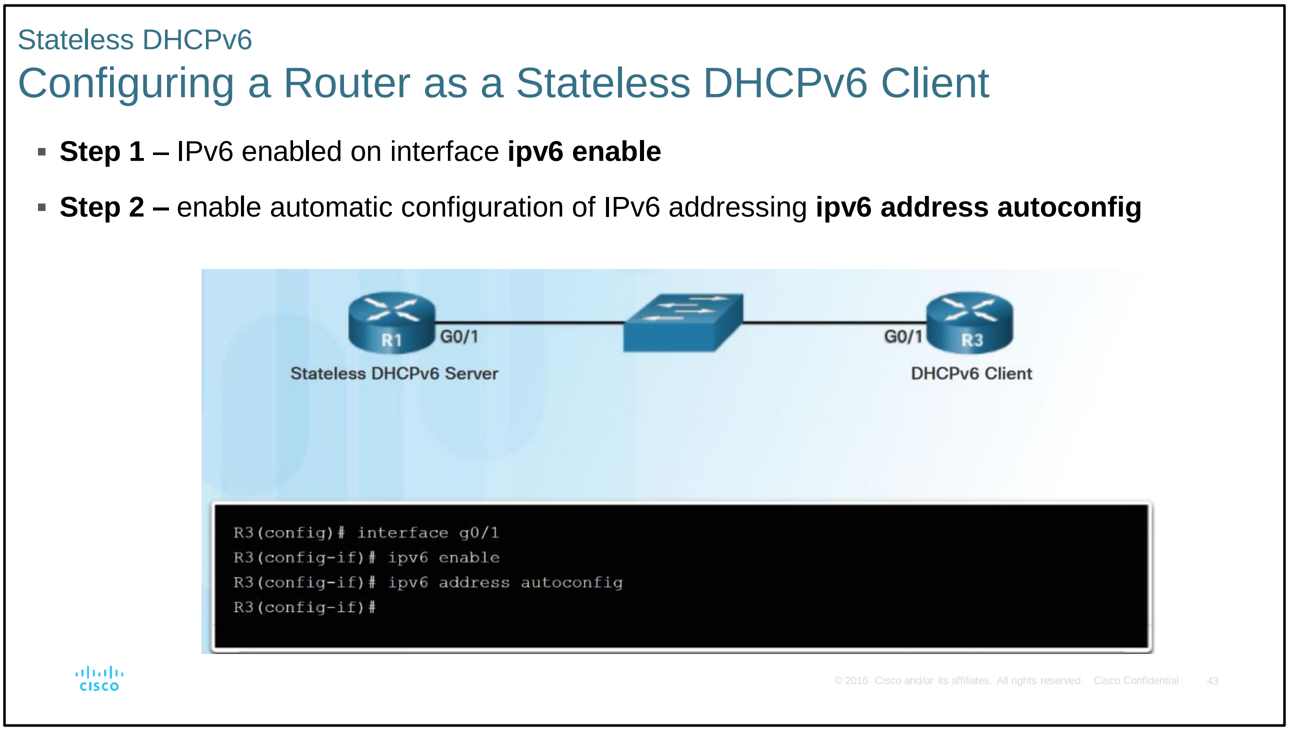
Step 1. Enable IPv6 Routing
Use the **ipv6 unicast-routing** command is required to enable IPv6 routing. This command is not necessary for the router to be a stateless DHCPv6 server, but is required for sending ICMPv6 RA messages.

Step 2. Configure a DHCPv6 Pool
The **ipv6 dhcp pool** *pool-name* command creates a pool and enters the router in DHCPv6 configuration mode, which is identified by the Router(config-dhcpv6)# prompt.

Step 3. Configure Pool Parameters
During the SLAAC process the client received the information it needed to create an IPv6 global unicast address. The client also received the default gateway information using the source IPv6 address from the RA message, which is the link-local address of the router. However, the stateless DHCPv6 server can be configured to provide other information that might not have been included in the RA message such as DNS server address and the domain name.

Step 4. Configure the DHCPv6 Interface
The **ipv6 dhcp server** *pool-name* interface configuration mode command binds the

DHCPv6 pool to the interface. The router responds to stateless DHCPv6 requests on this interface with the information contained in the pool. The O flag needs to be changed from 0 to 1 using the interface command **ipv6 nd other-config-flag**. RA messages sent on this interface indicate that additional information is available from a stateless DHCPv6 server.



Stateless DHCPv6

Configuring a Router as a Stateless DHCPv6 Client

- **Step 1 –** IPv6 enabled on interface **ipv6 enable**
- **Step 2 –** enable automatic configuration of IPv6 addressing **ipv6 address autoconfig**

```
R3(config)# interface g0/1
R3(config-if)# ipv6 enable
R3(config-if)# ipv6 address autoconfig
R3(config-if)#
```

In this figure's example, a Cisco router is used as the stateless DHCPv6 client. This is not a typical scenario and is used for demonstration purposes only. Typically, a stateless DHCPv6 client is a device, such as a computer, tablet, mobile device, or webcam.

The client router needs an IPv6 link-local address on the interface to send and receive IPv6 messages, such as RS messages and DHCPv6 messages. The link-local address of a router is created automatically when IPv6 is enabled on the interface. This can happen when a global unicast address is configured on the interface or by using the **ipv6 enable** command. After the router receives a link-local address, it can send RS messages and participate in DHCPv6.

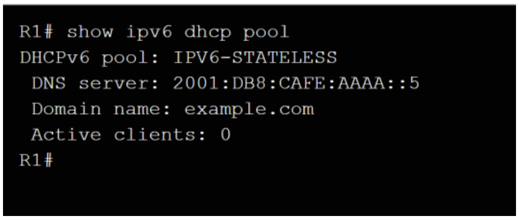
In this example, the **ipv6 enable** command is used because the router does not yet have a global unicast address.

The **ipv6 address autoconfig** command enables automatic configuration of IPv6 addressing using SLAAC. An RA message is then used to inform the client router to use stateless DHCPv6.

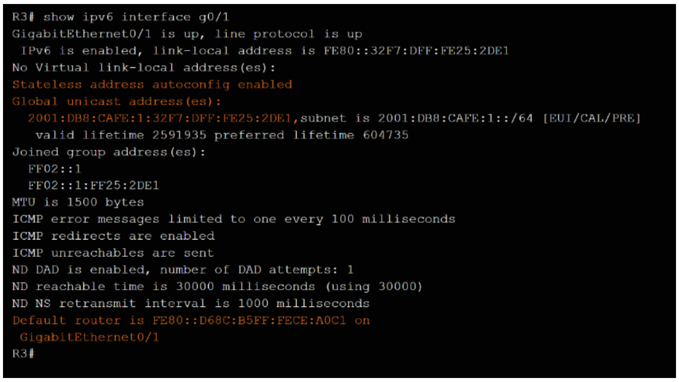
Stateless DHCPv6

Verifying Stateless DHCPv6

- Commands to verify Stateless DHCPv6:
  - **show ipv6 dhcp pool**
  - **show running-config**
  - **show ipv6 interface**
  - **debug ipv6 dhcp detail**



```
R1# show ipv6 dhcp pool
DHCPv6 pool: IPV6-STATELESS
 DNS server: 2001:DB8:CAFE:AAAA::5
 Domain name: example.com
 Active clients: 0
R1#
```



```
R3# show ipv6 interface g0/1
GigabitEthernet0/1 is up, line protocol is up
 IPv6 is enabled, link-local address is FE80::32F7:DFF:FE25:2DE1
No Virtual link-local address(es):
Stateless address autoconfig enabled
Global unicast address(es):
  2001:DB8:CAFE:1:32F7:DFF:FE25:2DE1,subnet is 2001:DB8:CAFE:1::/64 [EUI/CAL/PRE]
   valid lifetime 2591935 preferred lifetime 604735
Joined group address(es):
  FF02::1
  FF02::1:FF25:2DE1
MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ICMP unreachables are sent
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds (using 30000)
ND NS retransmit interval is 1000 milliseconds
Default router is FE80::D68C:B5FF:FECE:A0C1 on
 GigabitEthernet0/1
R3#
```

Verifying the Stateless DHCPv6 Server
In Figure, the **show ipv6 dhcp pool** command verifies the name of the DHCPv6 pool and its parameters. The number of active clients is 0, because there is no state being maintained by the server.

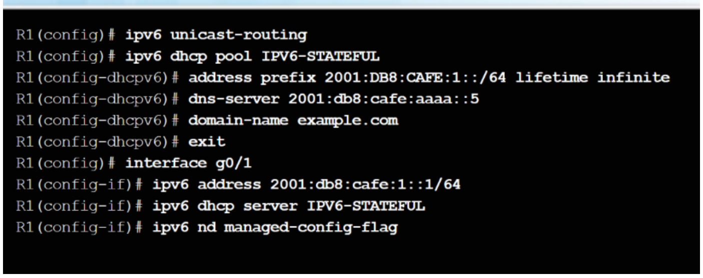
The **show running-config** command can also be used to verify all the commands that were previously configured.

Verifying the Stateless DHCPv6 Client
In this example, a router is used as a stateless DHCPv6 client.
show ipv6 interface command shows that the router has ”Stateless address autoconfig enabled“ and has an IPv6 global unicast address. The IPv6 global unicast address was created using SLAAC, which includes the prefix contained in the RA message. The IID was generated using EUI-64. DHCPv6 was not used to assign the IPv6 address.
The default router information is also from the RA message. This was the source IPv6 address of the packet that contained the RA message and the link-local address of the router.
debug ipv6 dhcp detail command shows the DHCPv6 messages exchanged between the client and the server. Notice that the client, router R3, is sending the DHCPv6 messages from its link-local address to the All_DHCPv6_Relay_Agents_and_Servers address FF02::1:2.

Stateful DHCPv6 Server

Configuring a Router as a Stateful DHCPv6 Server

- **Step 1** – Enable IPv6 Routing.
  - **ipv6 unicast routing**
- **Step 2** – Configure a DHCPv6 pool.
  - **ipv6 dhcp pool** *pool-name*
- **Step 3** – Configure pool parameters:
  - **address prefix** *prefix/length*
  - **dns-server** *dns-server-address*
  - **domain-name** *domain-name*
- **Step 4** - Configure DHCPv6 interface:
  - **ipv6 dhcp server** *pool-name*
  - **ipv6 nd managed-config-flag**



```
R1(config)# ipv6 unicast-routing
R1(config)# ipv6 dhcp pool IPV6-STATEFUL
R1(config-dhcpv6)# address prefix 2001:DB8:CAFE:1::/64 lifetime infinite
R1(config-dhcpv6)# dns-server 2001:db8:cafe:aaaa::5
R1(config-dhcpv6)# domain-name example.com
R1(config-dhcpv6)# exit
R1(config)# interface g0/1
R1(config-if)# ipv6 address 2001:db8:cafe:1::1/64
R1(config-if)# ipv6 dhcp server IPV6-STATEFUL
R1(config-if)# ipv6 nd managed-config-flag
```

Configuring a stateful DHCPv6 server is similar to configuring a stateless server. The most significant difference is that a stateful server also includes IPv6 addressing information similar to a DHCPv4 server.

Step 1. Enable IPv6 Routing
As shown in the figure, use the **ipv6 unicast-routing** command is required to enable IPv6 routing. This command is not necessary for the router to be a stateful DHCPv6 server, but is required for sending ICMPv6 RA messages.

Step 2. Configure a DHCPv6 Pool
The **ipv6 dhcp pool** *pool-name* command creates a pool and enters the router in DHCPv6 configuration mode, which is identified by the Router(config-dhcpv6)# prompt.

Step 3. Configure Pool Parameters
With stateful DHCPv6 all addressing and other configuration parameters must be assigned by the DHCPv6 server. The **address** *prefix/length* command is used to indicate the pool of addresses to be allocated by the server. The **lifetime** option indicates the valid and preferred lease times in seconds. As with stateless DHCPv6, the client uses the source IPv6 address from the packet that contained the RA message.
Other information provided by the stateful DHCPv6 server typically includes DNS

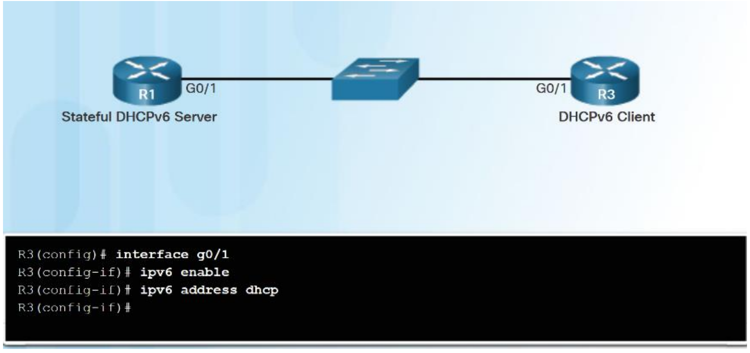
server address and the domain name.

Step 4. Interface Commands
The **ipv6 dhcp server** *pool-name* interface command binds the DHCPv6 pool to the interface. The router responds to stateless DHCPv6 requests on this interface with the information contained in the pool. The M flag needs to be changed from 0 to 1 using the interface command **ipv6 nd managed-config-flag**. This informs the device not to use SLAAC but to obtain IPv6 addressing and all configuration parameters from a stateful DHCPv6 server.
DHCPv6 Stateful Server Example

Figure shows an example of stateful DHCPv6 server commands for a router configured on R1. Notice that a default gateway is not specified because the router will automatically send its own link-local address as the default gateway. Router R3 is configured as a client to help verify the stateful DHCPv6 operations.

Stateful DHCPv6 Server

Configuring a Router as a Stateful DHCPv6 Client



```
R3(config)# interface g0/1
R3(config-if)# ipv6 enable
R3(config-if)# ipv6 address dhcp
R3(config-if)#
```

- **Step 1 –** Allow the router to send RS messages and participate in DHCPv6.
  - **ipv6 enable**
- **Step 2 –** Make the router a DHCPv6 client.
  - **ipv6 address dhcp**

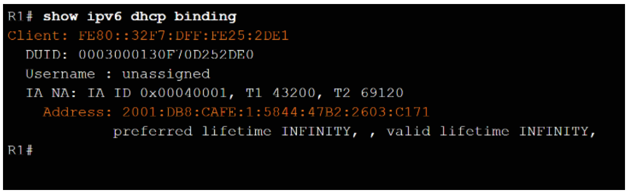
As shown in the figure, use the **ipv6 enable** interface configuration mode command to allow the router to receive a link-local address to send RS messages and participate in DHCPv6.

The **ipv6 address dhcp** interface configuration mode command enables the router to behave as a DHCPv6 client on this interface.

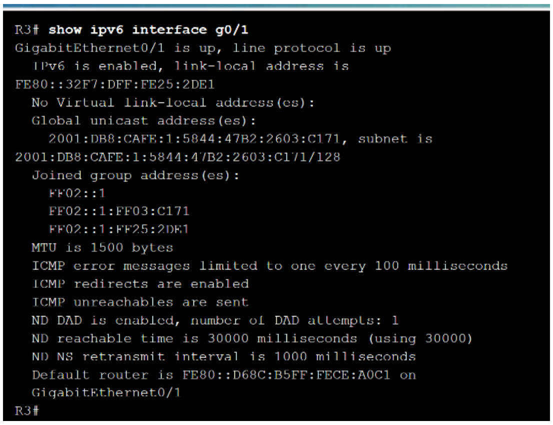
Stateful DHCPv6 Server

Verifying Stateful DHCPv6

- Use the following commands to verify Stateful DHCPv6:
  - **show ipv6 dhcp pool**
  - **show ipv6 dhcp binding**
  - **show ipv6 interface**



```
R1# show ipv6 dhcp binding
Client: FE80::32F7:DFF:FE25:2DE1
  DUID: 0003000130F70D252DE0
  Username : unassigned
  IA NA: IA ID 0x00040001, T1 43200, T2 69120
    Address: 2001:DB8:CAFE:1:5844:47B2:2603:C171
            preferred lifetime INFINITY, , valid lifetime INFINITY,
R1#
```



```
R3# show ipv6 interface g0/1
GigabitEthernet0/1 is up, line protocol is up
  IPv6 is enabled, link-local address is
FE80::32F7:DFF:FE25:2DE1
  No Virtual link-local address(es):
  Global unicast address(es):
    2001:DB8:CAFE:1:5844:47B2:2603:C171, subnet is
2001:DB8:CAFE:1:5844:47B2:2603:C171/128
  Joined group address(es):
    FF02::1
    FF02::1:FF03:C171
    FF02::1:FF25:2DE1
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds (using 30000)
  ND NS retransmit interval is 1000 milliseconds
  Default router is FE80::D68C:B5FF:FECE:A0C1 on
  GigabitEthernet0/1
R3#
```

Verifying the Stateful DHCPv6 Server

The **show ipv6 dhcp pool** command verifies the name of the DHCPv6 pool and its parameters.

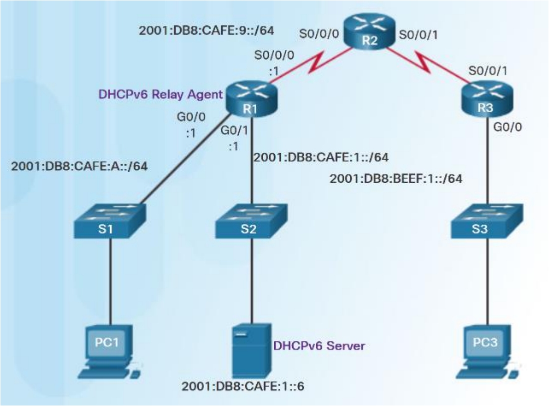
The **show ipv6 dhcp binding** command displays the automatic binding between the link-local address of the client and the address assigned by the server. FE80::32F7:DFF:FE25:2DE1 is the link-local address of the client. In this example, this is the G0/1 interface of R3. This address is bound to the IPv6 global unicast address, 2001:DB8:CAFE:1:5844:47B2:2603:C171, which was assigned by R1, the DHCPv6 server. This information is maintained by a stateful DHCPv6 server and not by a stateless DHCPv6 server.

Verifying the Stateful DHCPv6 Client

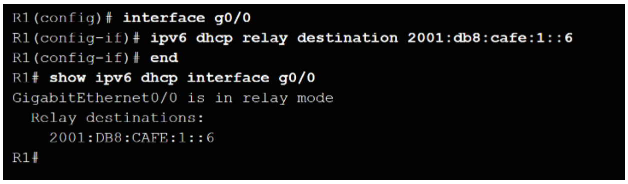
The output from the **show ipv6 interface** command shown in figure verifies the IPv6 global unicast address on DHCPv6 client R3 that was assigned by the DHCPv6 server. The default router information is not from the DHCPv6 server, but was determined by using the source IPv6 address from the RA message. Although the client does not use the information contained in the RA message, it is able to use the source IPv6 address for its default gateway information.

Stateful DHCPv6 Server

Configuring a Router as a DHCPv6 Relay Agent



- If the DHCPv6 server is located on a different network than the client, the router can be configured as a DHCPv6 relay agent.
  - **ipv6 dhcp relay destination** *destination-address*



```
R1(config)# interface g0/0
R1(config-if)# ipv6 dhcp relay destination 2001:db8:cafe:1::6
R1(config-if)# end
R1# show ipv6 dhcp interface g0/0
GigabitEthernet0/0 is in relay mode
  Relay destinations:
    2001:DB8:CAFE:1::6
R1#
```

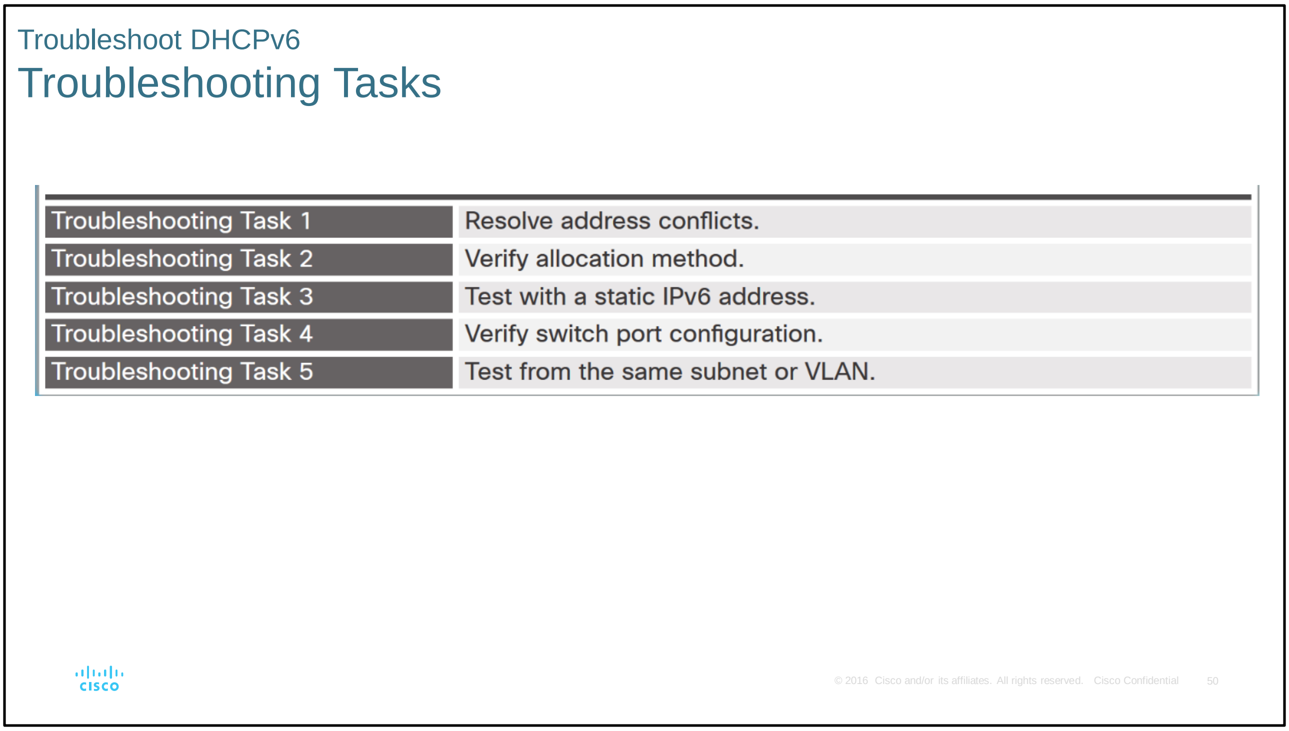
If the DHCPv6 server is located on a different network than the client, then the IPv6 router can be configured as a DHCPv6 relay agent. The configuration of a DHCPv6 relay agent is similar to the configuration of an IPv4 router as a DHCPv4 relay.

Note: Although the configuration of a DHCPv6 relay agent is similar to DHCPv4, IPv6 router or relay agents forward DHCPv6 messages slightly differently than DHCPv4 relays. The messages and the process are beyond the scope of this class.

Figure shows an example topology where a DHCPv6 server is located on the 2001:DB8:CAFE:1::/64 network. The network administrator wants to use this DHCPv6 server as a central, stateful DHCPv6 server to allocate IPv6 addresses to all clients. Therefore, clients on other networks such as PC1 on the 2001:DB8:CAFE:A::/64 network, must communicate with the DHCPv6 server.
DHCPv6 messages from clients are sent to the IPv6 multicast address FF02::1:2. All_DHCPv6_Relay_Agents_and_Servers address. This address has link-local scope which means routers do not forward these messages. The router must be configured as a DHCPv6 relay agent to enable the DHCPv6 client and server to communicate.

Configuring the DHCPv6 Relay Agent
As shown in the second part of the figure, a DHCPv6 relay agent is configured using the **ipv6 dhcp relay destination** command. This command is configured on the interface facing the DHCPv6 client using the address of the DHCPv6 server as the

destination.
The **show ipv6 dhcp interface** command verifies the G0/0 interface is in relay mode with 2001:DB8:CAFE:1::6 configured as the DHCPv6 server.



Troubleshoot DHCPv6

Troubleshooting Tasks

Troubleshooting Task 1	Resolve address conflicts.
Troubleshooting Task 2	Verify allocation method.
Troubleshooting Task 3	Test with a static IPv6 address.
Troubleshooting Task 4	Verify switch port configuration.
Troubleshooting Task 5	Test from the same subnet or VLAN.

Troubleshooting DHCPv6 is similar to troubleshooting DHCPv4.

Troubleshooting Task 1. Resolve Conflicts
Similar to IPv4 addresses, an IPv6 address lease can expire on a client that still needs to connect to the network. The **show ipv6 dhcp conflict** command displays any address conflicts logged by the stateful DHCPv6 server. If an IPv6 address conflict is detected, the client typically removes the address and generates a new address using either SLAAC or stateful DHCPv6.

Troubleshooting Task 2. Verify Allocation Method
The **show ipv6 interface** *interface* command can be used to verify the method of address allocation indicated in the RA message as indicated by the settings of the M and O flags. This information is displayed in the last lines of the output. If a client is not receiving its IPv6 address information from a stateful DHCPv6 server, it could be due to incorrect M and O flags in the RA message.

Troubleshooting Task 3. Test with a Static IPv6 Address
When troubleshooting any DHCP issue, whether it is DHCPv4 or DHCPv6, network connectivity can be verified by configuring a static IP address on a client workstation. In the case of IPv6, if the workstation is unable to reach network resources with a statically configured IPv6 address, the root cause of the problem is not SLAAC or DHCPv6. At this point, network connectivity troubleshooting is required.

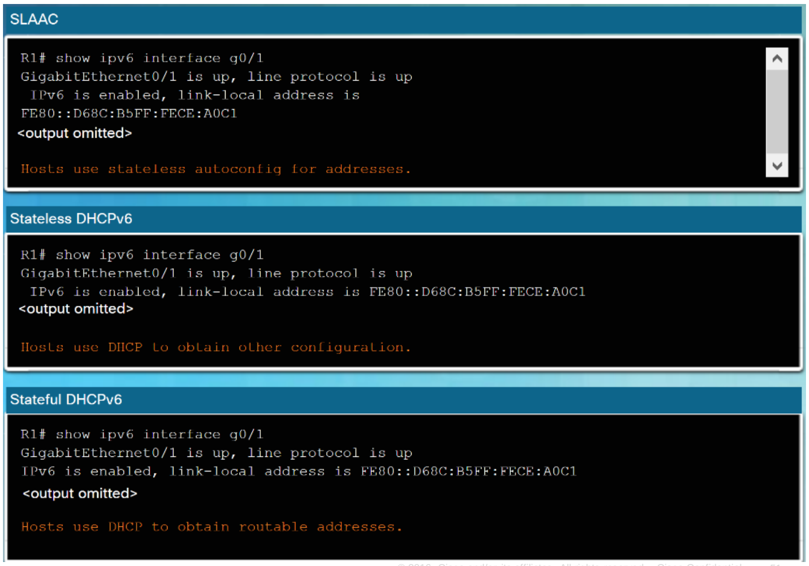
Troubleshooting Task 4. Verify Switch Port Configuration
If the DHCPv6 client is unable to obtain information from a DHCPv6 server, verify that the switch port is enabled and is operating correctly.
Note: If there is a switch between the client and the DHCPv6 server, and the client is unable to obtain the DHCP configuration, switch port configuration issues may be the cause. These causes may include issues from trunking and channeling, STP, and RSTP. PortFast and edge port configurations resolve the most common DHCPv6 client issues that occur with an initial installation of a Cisco switch.

Troubleshooting Task 5. Test DHCPv6 Operation on the Same Subnet or VLAN
If the stateless or stateful DHCPv6 server is functioning correctly, but is on a different IPv6 network or VLAN than the client, the problem may be with the DHCPv6 relay agent. The client facing interface on the router must be configured with the **ipv6 dhcp relay destination** command.

Troubleshoot DHCPv6

Verify Router DHCPv6 Configuration

- Use the **show ipv6 interface** command to verify DHCPv6 configuration.



SLAAC

```
R1# show ipv6 interface g0/1
GigabitEthernet0/1 is up, line protocol is up
 IPv6 is enabled, link-local address is
FE80::D68C:B5FF:FECE:A0C1
<output omitted>

Hosts use stateless autoconfig for addresses.
```

Stateless DHCPv6

```
R1# show ipv6 interface g0/1
GigabitEthernet0/1 is up, line protocol is up
 IPv6 is enabled, link-local address is FE80::D68C:B5FF:FECE:A0C1
<output omitted>

Hosts use DHCP to obtain other configuration.
```

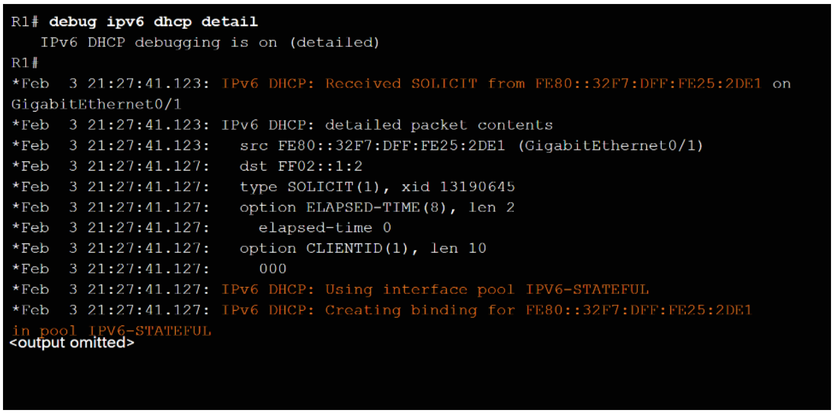
Stateful DHCPv6

```
R1# show ipv6 interface g0/1
GigabitEthernet0/1 is up, line protocol is up
IPv6 is enabled, link-local address is FE80::D68C:B5FF:FECE:A0C1
<output omitted>

Hosts use DHCP to obtain routable addresses.
```

The **show ipv6 interface** command can be used to view the current configuration for allocation method.

Troubleshoot DHCPv6

Debugging DHCPv6



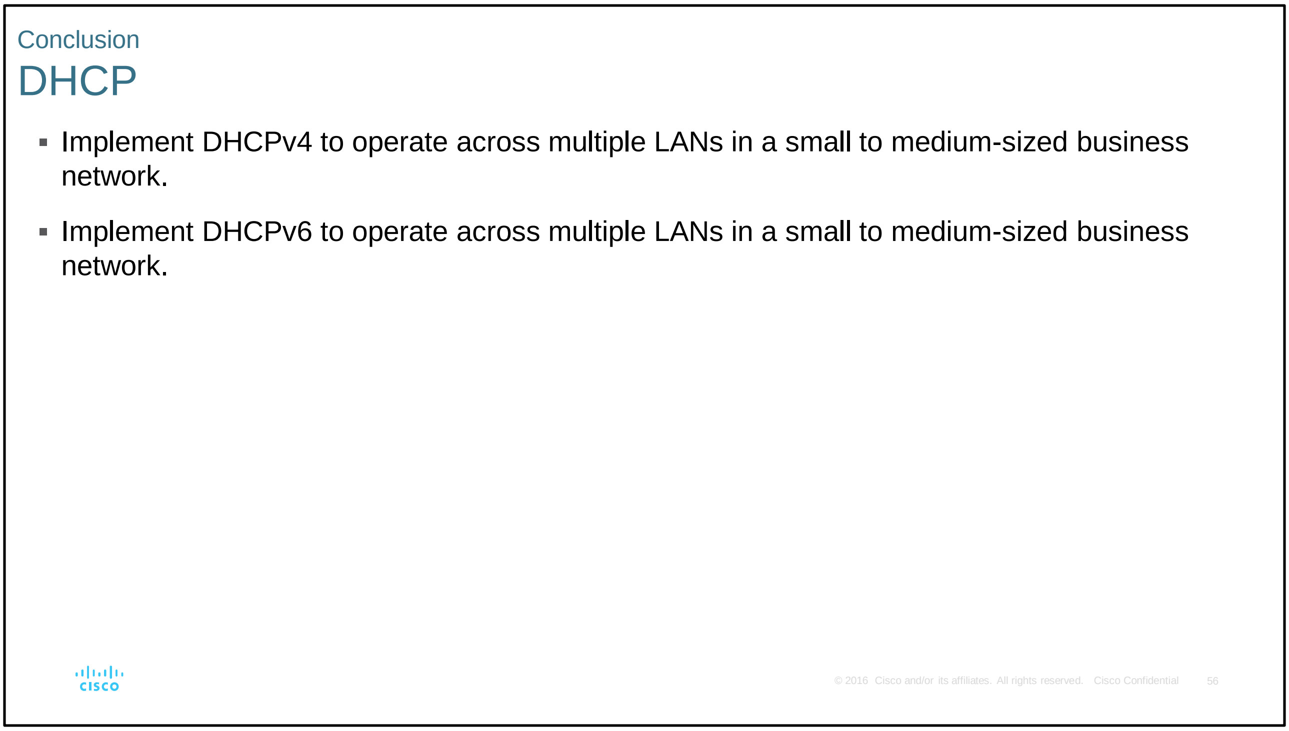
```
R1# debug ipv6 dhcp detail
   IPv6 DHCP debugging is on (detailed)
R1#
*Feb  3 21:27:41.123: IPv6 DHCP: Received SOLICIT from FE80::32F7:DFF:FE25:2DE1 on
GigabitEthernet0/1
*Feb  3 21:27:41.123: IPv6 DHCP: detailed packet contents
*Feb  3 21:27:41.123:   src FE80::32F7:DFF:FE25:2DE1 (GigabitEthernet0/1)
*Feb  3 21:27:41.127:   dst FF02::1:2
*Feb  3 21:27:41.127:   type SOLICIT(1), xid 13190645
*Feb  3 21:27:41.127:   option ELAPSED-TIME(8), len 2
*Feb  3 21:27:41.127:     elapsed-time 0
*Feb  3 21:27:41.127:   option CLIENTID(1), len 10
*Feb  3 21:27:41.127:     000
*Feb  3 21:27:41.127: IPv6 DHCP: Using interface pool IPV6-STATEFUL
*Feb  3 21:27:41.127: IPv6 DHCP: Creating binding for FE80::32F7:DFF:FE25:2DE1
in pool IPV6-STATEFUL
<output omitted>
```

- To verify the receipt and transmission of DHCPv6 messages:
  - **debug ipv6 dhcp detail**

When the router is configured as a stateless or stateful DHCPv6 server, the **debug ipv6 dhcp detail** command is useful to verify the receipt and transmission of DHCPv6 messages. As shown in the figure, a stateful DHCPv6 router has received a SOLICIT message from a client. The router is using the addressing information in its IPV6-STATEFUL pool for binding information.

Chapter Summary

8 - DHCP
8.3 – Chapter Summary



Conclusion

DHCP

- Implement DHCPv4 to operate across multiple LANs in a small to medium-sized business network.
- Implement DHCPv6 to operate across multiple LANs in a small to medium-sized business network.

8.3 – Summary

8.3.1 – Conclusion
8.3.1.3 – Chapter 8: DHCP

cisco