**SLAAC AND DHCPV6**

8.0.1

Welcome

Welcome to SLAAC and DHCPv6!

SLAAC and DHCPv6 are dynamic addressing protocols for an IPv6 network. So, a little bit of configuring will make your day as a network administrator lot easier. In this module, you will learn how to use SLAAC to allow hosts to create their own IPv6 global unicast address, as well as configure a Cisco IOS router to be a DHCPv6 server, a DHCPv6 client, or a DHCPv6 relay agent. This module includes a lab where you will configure DHCPv6 on real equipment!

8.0.2

What will I learn to do in this module?

**Module Title**: SLAAC and DHCPv6

**Module Objective**: Configure dynamic address allocation in IPv6 networks.

| Table caption | |
| --- | --- |
| **Topic Title** | **Topic Objective** |
| **IPv6 Global Unicast Address Assignment** | Explain how an IPv6 host can acquire its IPv6 configuration. |
| **SLAAC** | Explain the operation of SLAAC. |
| **DHCPv6** | Explain the operation of DHCPv6. |
| **Configure DHCPv6 Server** | Configure a stateful and stateless DHCPv6 server |

**IPV6 GUA ASSIGNMENT**

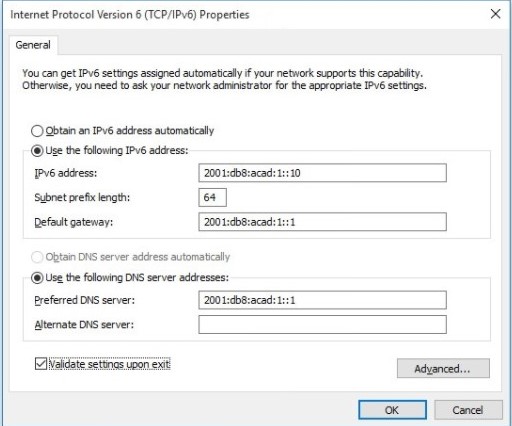
8.1.1

IPv6 Host Configuration

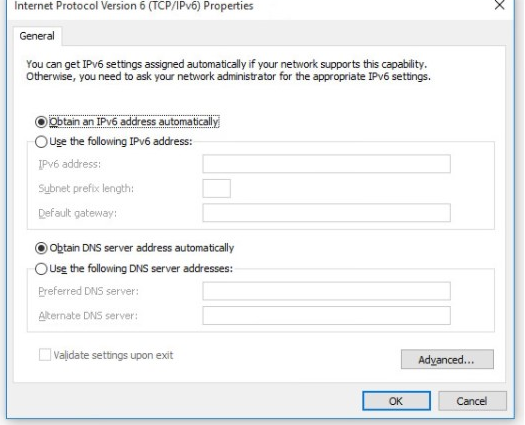
First things first. To use either stateless address autoconfiguration (SLAAC) or DHCPv6, you should review global unicast addresses (GUAs) and link-local addresses (LLAs). This topic covers both.

On a router, an IPv6 global unicast address (GUA) is manually configured using the **ipv6 address** *ipv6-address****/****prefix-length* interface configuration command.

A Windows host can also be manually configured with an IPv6 GUA address configuration, as shown in the figure.

****

Manually entering an IPv6 GUA can be time consuming and somewhat error prone. Therefore, most Windows host are enabled to dynamically acquire an IPv6 GUA configuration, as shown in the figure

****

8.1.2

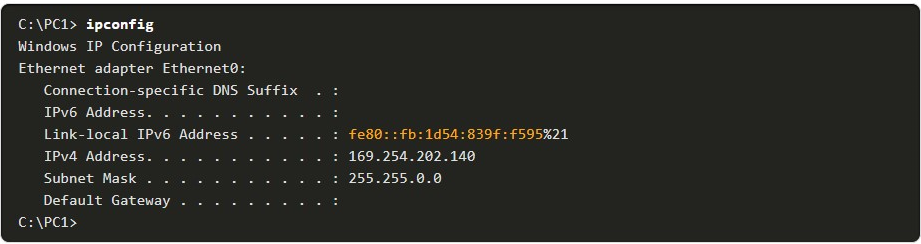
IPv6 Host Link-Local Address

When automatic IPv6 addressing is selected, the host will attempt to automatically obtain and configure IPv6 address information on the interface.

The host will use one of three methods defined by the Internet Control Message Protocol version 6 (ICMPv6) Router Advertisement (RA) message received on the interface.

An IPv6 router that is on the same link as the host sends out RA messages that suggest to the hosts how to obtain their IPv6 addressing information. The IPv6 link-local address is automatically created by the host when it boots and the Ethernet interface is active. The example **ipconfig** output shows an automatically generated link-local address (LLA) on an interface.

In the figure, notice that the interface does not have an IPv6 GUA. The reason is because, in this example, the network segment does not have a router to provide network configuration instructions for the host or the host has not been configured with at static IPv6 address.



**Note:** Host operating systems will at times show a link-local address appended with a "%" and a number. This is known as a ***Zone ID or Scope ID***. It is used by the OS to associate the LLA with a specific interface.

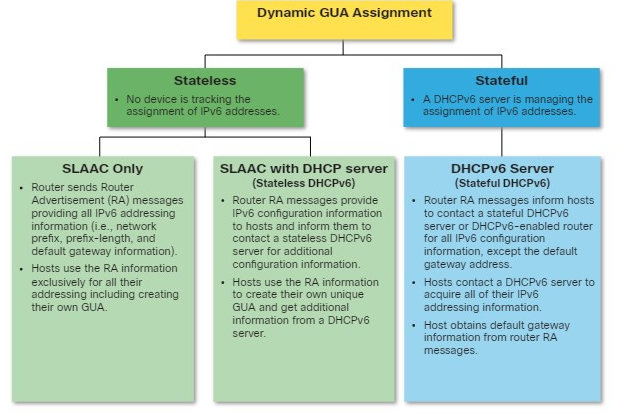
8.1.3

IPv6 GUA Assignment

IPv6 was designed to simplify how a host can acquire its IPv6 configuration. By default, an IPv6-enabled router advertises its IPv6 information. This allows a host to dynamically create or acquire its IPv6 configuration.

The IPv6 GUA can be assigned dynamically using stateless and stateful services, as shown in the figure.

All stateless and stateful methods in this module use ICMPv6 RA messages to suggest to the host how to create or acquire its IPv6 configuration. Although host operating systems follow the suggestion of the RA, the actual decision is ultimately up to the host.

****

8.1.4

## Three RA Message Flags

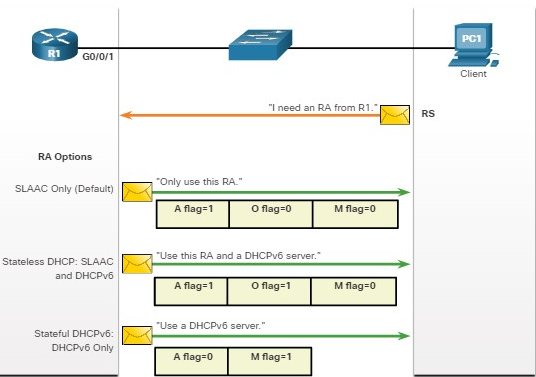
The decision of how a client will obtain an IPv6 GUA depends on the settings within the RA message.

An ICMPv6 RA message includes three flags to identify the dynamic options available to a host, as follows:

* **A flag** - This is the Address Auto configuration flag. Use Stateless Address Autoconfiguration (SLAAC) to create an IPv6 GUA.
* **O flag** - This is the Other Configuration flag. Other information is available from a stateless DHCPv6 server.
* **M flag** - This is the Managed Address Configuration flag. Use a stateful DHCPv6 server to obtain an IPv6 GUA.

Using different combinations of the A, O and M flags, RA messages inform the host about the dynamic options available.

The figure illustrates these three methods.



1. Which address type is automatically created by default on a host interface when no RAs are received?



global unicast address



link-local address



MAC address

**ANS: A link-local IPv6 address is immediately created on a Windows 10 host.**

1. Which method best describes stateless DHCP?



SLAAC only



SLAAC with stateless DHCPv6 Server



Stateful DHCPv6 Server

**ANS: SLAAC with a DHCP server is a stateless method of IPv6 address allocation.**

**SLAAC**

**SLAAC OVERVIEW**

8.2.1

## SLAAC Overview

Not every network has or needs access to a DHCPv6 server. But every device in an IPv6 network needs a GUA.

The SLAAC method enables hosts to create their own unique IPv6 global unicast address without the services of a DHCPv6 server.

SLAAC is a stateless service. This means there is no server that maintains network address information to know which IPv6 addresses are being used and which ones are available.

SLAAC uses ICMPv6 RA messages to provide addressing and other configuration information that would normally be provided by a DHCP server. A host configures its IPv6 address based on the information that is sent in the RA. RA messages are sent by an IPv6 router every ***200 seconds.***

A host can also send a Router Solicitation (RS) message requesting that an IPv6-enabled router send the host an RA.

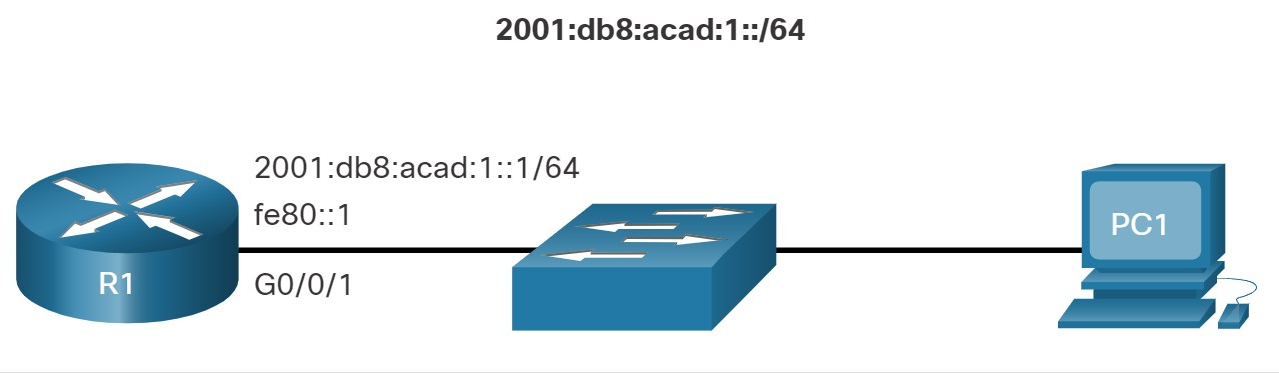
SLAAC can be deployed as SLAAC only, or SLAAC with DHCPv6.

8.2.2

## Enabling SLAAC

Refer to the following topology to see how SLAAC is enabled to provide stateless dynamic GUA allocation.

shows a topology with a router connected to a switch connected to a host PC

****

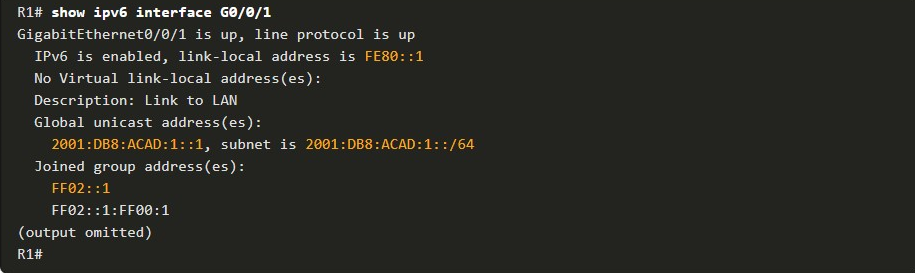
Assume R1 GigabitEthernet 0/0/1 has been configured with the indicated IPv6 GUA and link-local addresses. Click each button for an explanation of how R1 is enabled for SLAAC.

1. **Verify ipv6 addresses**

The output of the **show ipv6 interface** command displays the current settings on the G0/0/1 interface.

As highlighted, R1 has been assigned the following IPv6 addresses:

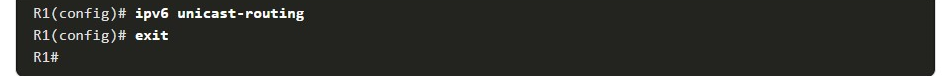
* **Link-local IPv6 address** - fe80::1
* **GUA and subnet** - 2001:db8:acad:1::1 and 2001:db8:acad:1::/64
* **IPv6 all-nodes group** - ff02::1

****

**2. Enable ipv6 routing**

Although the router interface has an IPv6 configuration, it is still not yet enabled to send RAs containing address configuration information to hosts using SLAAC.

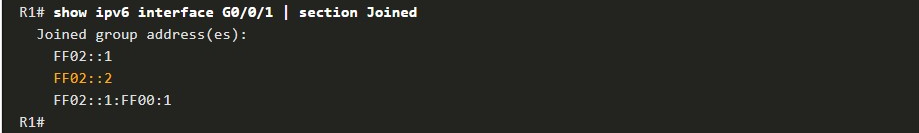
To enable the sending of RA messages, a router must join the IPv6 all-routers group using the **ipv6 unicast-routing** global config command, as show in the output.

****

**3. Verify SLAAC Is enabled**

The IPv6 all-routers group responds to the IPv6 multicast address ff02::2. You can use the **show ipv6 interface** command to verify if a router is enabled as shown, in the output.

An IPv6-enabled Cisco router sends RA messages to the IPv6 all-nodes multicast address ff02::1 every 200 seconds.

****

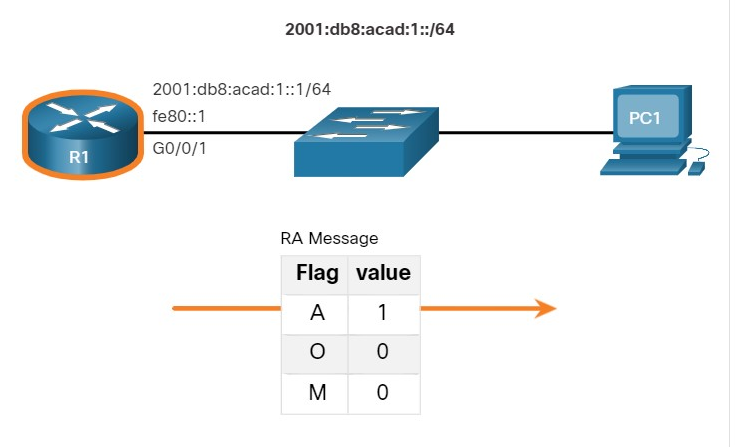
8.2.3

## SLAAC Only Method

The SLAAC only method is enabled **by default** when the **ipv6 unicast-routing** command is configured. All enabled Ethernet interfaces with an IPv6 GUA configured will start sending RA messages with the A flag set to 1, and the O and M flags set to 0, as shown in the figure.

The **A = 1** flag suggests to the client that it create its own IPv6 GUA using the prefix advertised in the RA. The client can create its own Interface ID using either Extended Unique Identifier method (EUI-64) or have it randomly generated.

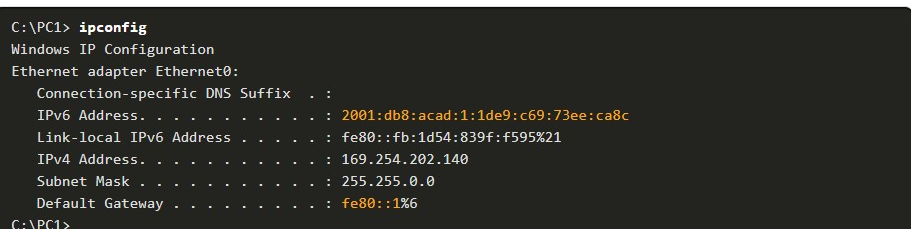
The **O =0** and **M=0** flags instruct the client to use the information in the RA message exclusively. The RA includes the prefix, prefix-length, DNS server, MTU, and default gateway information. There is no further information available from a DHCPv6 server.

****

In the example, PC1 is enabled to obtain its IPv6 addressing information automatically. Because of the settings of the A, O and M flags, PC1 performs SLAAC only, using the information contained in the RA message sent by R1.

The ***default gateway*** address is the ***source IPv6 address*** of the ***RA message***, which is the LLA for R1. The default gateway can only be obtained automatically from the RA message.

**NB:** A DHCPv6 server does not provide this information.

****

8.2.4

## ICMPv6 RS Messages

A router sends RA messages every 200 seconds. However, it will also send an RA message if it receives an RS message from a host.

When a client is configured to obtain its addressing information automatically, it sends an RS message to the IPv6 all-routers multicast address of ff02::2.

The figure illustrates how a host initiates the SLAAC method.

****

PC1 has just booted and has not yet received an RA message. Therefore, it sends an RS message to the IPv6 all-routers multicast address of ff02::2 requesting an RA.

1. R1 is part of the IPv6 all-routers group and received the RS message. It generates an RA containing the local network prefix and prefix length (e.g., 2001:db8:acad:1::/64). It then sends the RA message to the IPv6 all-nodes multicast address of ff02::1. PC1 uses this information to create a unique IPv6 GUA.

8.2.5

## Host Process to Generate Interface ID

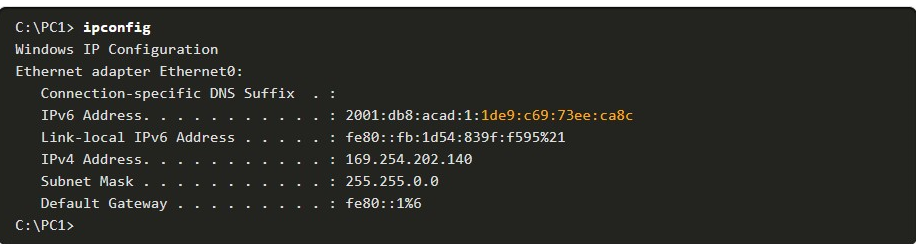
Using SLAAC, a host typically acquires its 64-bit IPv6 subnet information from the router RA. However, it must generate the remainder 64-bit interface identifier (ID) using one of two methods:

* **Randomly generated** - The 64-bit interface ID is randomly generated by the client operating system. This is the method now used by Windows 10 hosts.
* **EUI-64** - The host creates an interface ID using its 48-bit MAC address. The host inserts the hex value of fffe in the middle of the address, and flips the seventh bit of the interface ID.

This changes the value of the second hexadecimal digit of the interface ID. Some operating systems default to the randomly generated interface ID instead of the EUI-64 method, due to privacy concerns. This is because the Ethernet MAC address of the host is used by EUI-64 to create the interface ID.

**Note**: Windows, Linux, and Mac OS allow for the user to modify the generation of the interface ID to be either randomly generated or to use EUI-64.

For instance, in the following **ipconfig** output, the Windows 10 PC1 host used the IPv6 subnet information contained in the R1 RA and randomly generated a 64-bit interface ID as highlighted in the output.

****

8.2.6

## Duplicate Address Detection

The process enables the host to create an IPv6 address. However, there is no guarantee that the address is unique on the network.

SLAAC is a stateless process; therefore, a host has the option to verify that a newly created IPv6 address is unique before it can be used. The Duplicate Address Detection (DAD) process is used by a host to ensure that the IPv6 GUA is unique.

DAD is implemented using ICMPv6. To perform DAD, the host sends an ICMPv6 ***Neighbor Solicitation (NS) message*** with a specially constructed multicast address, called a ***solicited-node multicast address***. This address duplicates the last 24 bits of IPv6 address of the host.

If no other devices respond with a NA message, then the address is virtually guaranteed to be unique and can be used by the host. If an NA is received by the host, then the address is not unique, and the operating system has to determine a new interface ID to use.

The Internet Engineering Task Force (IETF) recommends that DAD is used on all IPv6 unicast addresses regardless of whether it is created using SLAAC only, obtained using stateful DHCPv6, or manually configured. DAD is not mandatory because a 64-bit interface ID provides 18 quintillion possibilities and the chance that there is a duplication is remote. However, most operating systems perform DAD on all IPv6 unicast addresses, regardless of how the address is configured.

Yo

1. Which two ICMPv6 messages are used in the SLAAC process? (Choose two.)



Neighbor Advertisements (NA)



Neighbor Solicitation (NS)



Router Solicitation (RS)



Router Advertisements (RA)

**ANS: The SLAAC process uses RA messages and can also respond to RS messages from a host.**

1. Which command must be configured on a router to enable it to join the IPv6 all-routers multicast address ff02::2?



**ip routing**



**ipv6 unicast-routing**



**ipv6 address** *ipv6-address/prefix-length*



**ipv6 address** *ipv6-address* **link-local**

**ANS:** **The ipv6 unicast-routing global config command is required for a router to join the IPv6 all-routers group.**

1. What are the flag settings when a host should use the SLAAC only option?



A=1, M=0, O=0



A=1, M=1, O=0



A=1, M=0, O=1



A=0, M=1, O=1

**ANS: SLAAC sets the flags to A=1. M=0, O=0.**

1. Which ICMPv6 message is sent by a host in an attempt to locate an online IPv6enabled router to obtain IPv6 addressing information?



Neighbor Advertisements (NA)



Neighbor Solicitation (NS)



Router Solicitation (RS)



Router Advertisements (RA)

**ANS: A host sends a Router Solicitation (RS) message to the IPv6 all-routers group to locate an online router.**

1. What method is used by a host to verify an IPv6 address is unique on the local network before assigning that address to an interface?



ARP



DAD



PING



SLAAC

**ANS: A host uses DAD to ensure an IPv6 address is unique on the local network.**

**DHCPV6**

8.3.1

DHCPv6 Operation Steps

This topic explains stateless and stateful DHCPv6. Stateless DHCPv6 uses parts of SLAAC to ensure that all the necessary information is supplied to the host. Stateful DHCPv6 does not require SLAAC.

Although DHCPv6 is similar to DHCPv4 in what it provides, the two protocols are independent of each other.

**Note**: DHCPv6 is defined in RFC 3315.

The host begins the DHCPv6 client/server communications after stateless DHCPv6 or stateful DHCPv6 is indicated in the RA.

***Server to client DHCPv6 messages*** use UDP destination **port 546** while ***client to server DHCPv6 messages*** use UDP destination ***port 547***.

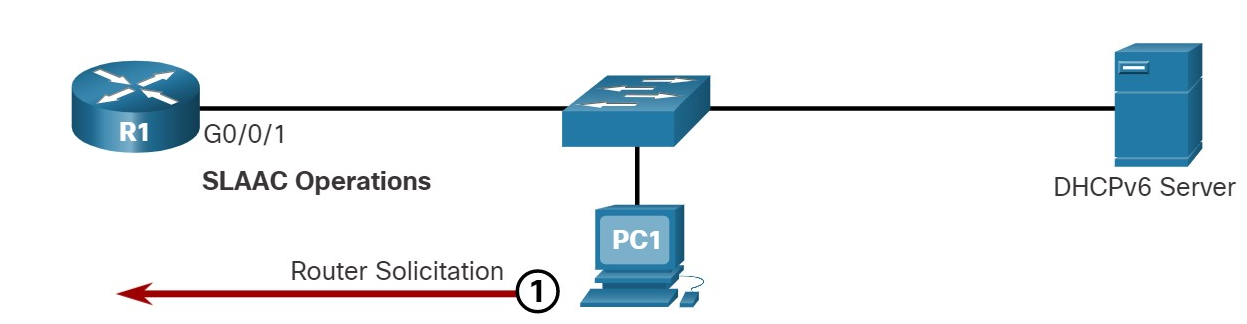
The steps for DHCPv6 operations are as follows:

1. The host sends an RS message.
2. The router responds with an RA message.
3. The host sends a DHCPv6 SOLICIT message.
4. The DHCPv6 server responds with an ADVERTISE message.
5. The host responds to the DHCPv6 server.
6. The DHCPv6 server sends a REPLY message.

Click each button for an explanation and illustration of these DHCPv6 operation steps.

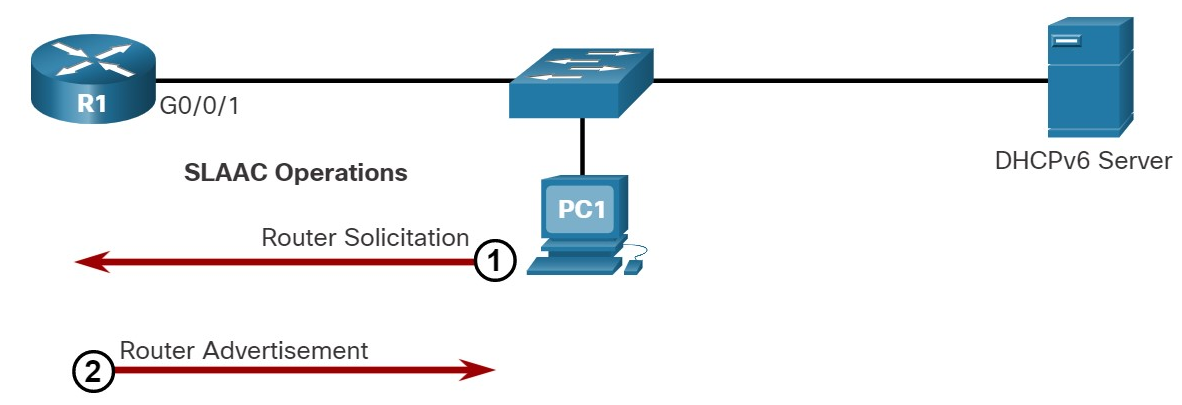
**Step 1. Host sends an RS message.**

PC1 sends an RS message to all IPv6-enabled routers.

****

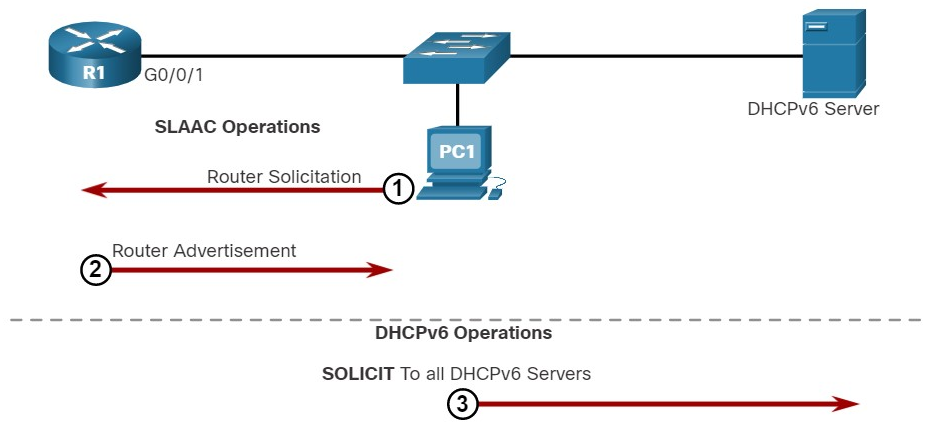
**Step 2. Router responds with an RA message.**

R1 receives the RS and responds with an RA indicating that the client is to initiate communication with a DHCPv6 server.



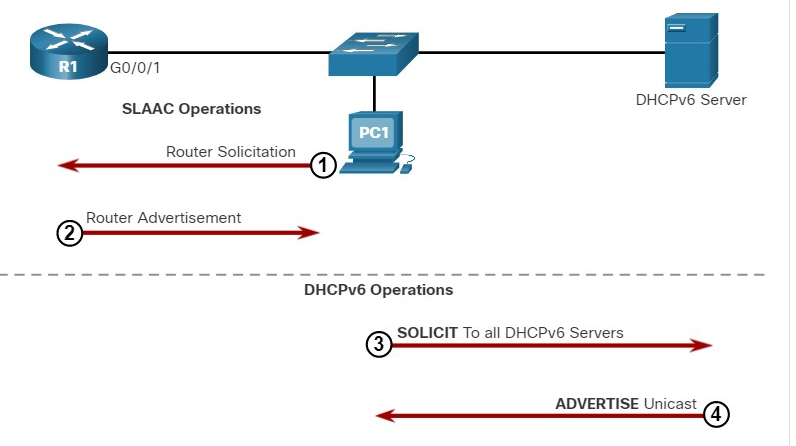
**Step 3. Host sends a DHCPv6 SOLICIT message.**

The client, now a DHCPv6 client, needs to locate a DHCPv6 server and sends a DHCPv6 SOLICIT message to the reserved IPv6 multicast all-DHCPv6-servers address of ff02::1:2. This multicast address has link-local scope, which means routers do not forward the messages to other networks.



**Step 4. DHCPv6 server responds with an ADVERTISE message.**

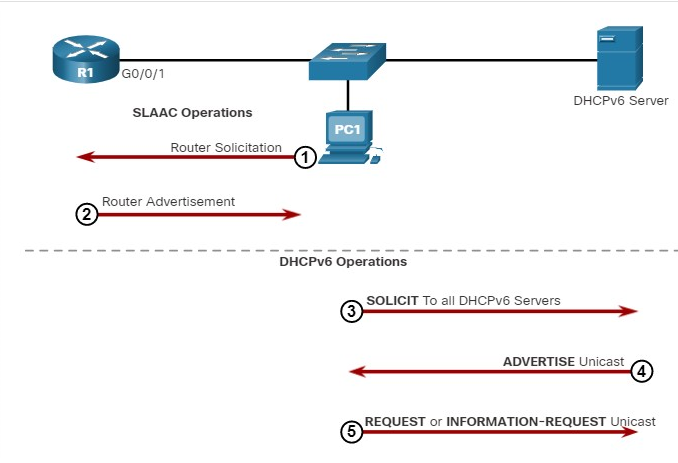
One or more DHCPv6 servers respond with a DHCPv6 ADVERTISE unicast message. The ADVERTISE message informs the DHCPv6 client that the server is available for DHCPv6 service.



**Step 5. Host responds to DHCPv6 server.**

The PC1 response depends on whether it is using stateful or stateless DHCPv6:

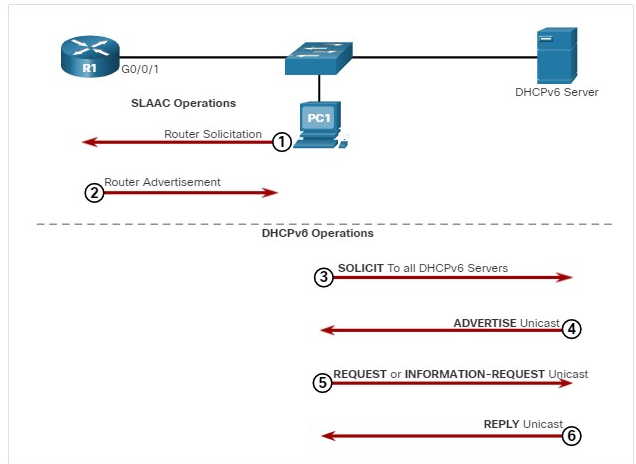
* **Stateless DHCPv6 client** - The client creates an IPv6 address using the prefix in the RA message and a self-generated Interface ID. The client then sends a DHCPv6 INFORMATION-REQUEST message to the DHCPv6 server requesting additional configuration parameters (e.g., DNS server address).
* **Stateful DHCPv6 client** - The client sends a DHCPv6 REQUEST message to the DHCPv6 server to obtain all necessary IPv6 configuration parameters.



**Step 6. DHCPv6 sends a REPLY message.**

The server sends a DHCPv6 REPLY unicast message to the client. The content of the message varies depending on if it is replying to a REQUEST or INFORMATION-REQUEST message.

**Note**: The client will use the source IPv6 Link-local address of the RA as its default gateway address. A DHCPv6 server does not provide this information.



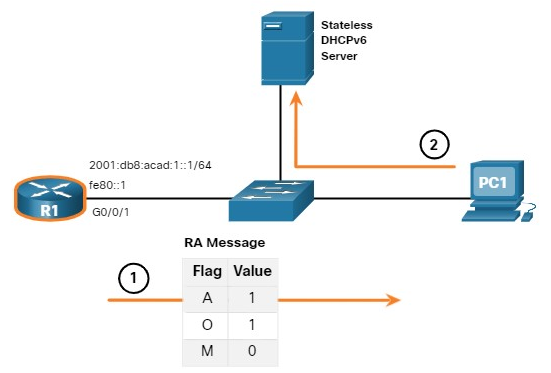
8.3.2

Stateless DHCPv6 Operation

The stateless DHCPv6 server is only providing information that is identical for all devices on the network such as the IPv6 address of a DNS server.

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.

The figure illustrates stateless DHCPv6 operation.

****

1. PC1 receives a stateless DHCP RA message. The RA message contains the network prefix and prefix length. The M flag for stateful DHCP is set to the default value 0. The A=1 flag tells the client to use SLAAC. The O=1 flag informs the client that additional configuration information is available from a stateless DHCPv6 server.
2. The client sends a DHCPv6 SOLICIT message looking for a stateless DHCPv6 server to obtain additional information (e.g., DNS server addresses).

8.3.3

## Enable Stateless DHCPv6 on an Interface

Stateless DHCPv6 is enabled on a router interface using the **ipv6 nd other-config-flag** interface configuration command. This sets the O flag to 1.

The highlighted output confirms the RA will tell receiving hosts to use stateless autoconfigure (A flag = 1) and contact a DHCPv6 server to obtain another configuration information (O flag = 1).

**Note:** You can use the **no ipv6 nd other-config-flag** to reset the interface to the default SLAAC only option (O flag = 0).

****

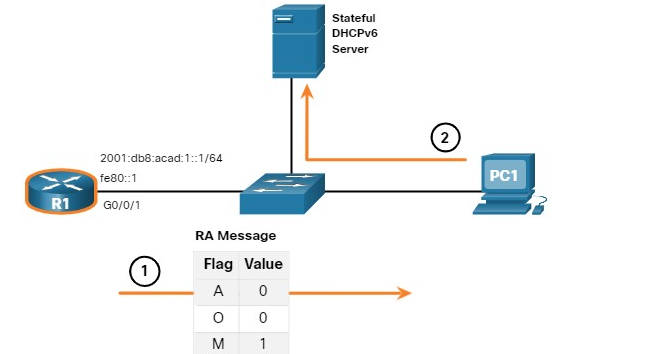
8.3.4

Stateful DHCPv6 Operation

This option is most similar to DHCPv4. In this case, the RA message tells the client to obtain all addressing information from a stateful DHCPv6 server, except the ***default gateway address*** which is the source IPv6 link-local address of the RA.

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 figure illustrates stateful DHCPv6 operation.

****

PC1 receives a DHCPv6 RA message with the O flag set to 0 and the M flag set to 1, indicating to PC1 that it will receive all its IPv6 addressing information from a stateful DHCPv6 server.

1. PC1 sends a DHCPv6 SOLICIT message looking for a stateful DHCPv6 server.

**Note**: If A=1 and M=1, some operating systems such as Windows will create an IPv6 address using SLAAC and obtain a different address from the stateful DHCPv6 server. In most cases it is recommended to manually set the A flag to 0

8.3.5

Enable Stateful DHCPv6 on an Interface

Stateful DHCPv6 is enabled on a router interface using the **ipv6 nd managed-config-flag** interface configuration command. This sets the M flag to 1. The **ipv6 nd prefix default no-autoconfig** interface command disables SLAAC by setting the A flag to 0.

The highlighted output in the example confirms that the RA will tell the host to obtain all IPv6 configuration information from a DHCPv6 server (M flag = 1).

****

1. What UDP port do DHCPv6 clients use to send DHCPv6 messages?



67



68



546



547

**ANS: DHCPv6 clients use UDP port 547 to send DHCPv6 messages. DHCPv6 servers use UDP port 546.**

1. What DHCPv6 message does a host send to look for a DHCPv6 server?



ADVERTISE



SOLICIT



INFORMATION-REQUEST



REQUEST

**ANS: A DHCPv6 client sends a DHCPv6 SOLICIT message to the reserved IPv6 multicast all-DHCPv6-servers address of ff02::1:2.**

1. What DHCPv6 message does a host send to the DHCPv6 server if it is using stateful DHCPv6?



ADVERTISE



SOLICIT



INFORMATION-REQUEST



REQUEST

**ANS: A DHCPv6 client will send a DHCPv6 REQUEST message if it is using stateful DHCPv6 and a DHCPv6 INFORMATION-REQUEST message if it is using stateless DHCPv6**.

1. What flag settings combination is used for stateless DHCP?



A=1, M=0, O=0



A=0, M=1, O=0



A=1, M=0, O=1



A=0, M=1, O=1

**ANS: Stateless DHCPv6 sets the flags to A=1, M=0, O=1.**

1. What M flag setting indicates that stateful DHCPv6 is used?



M=0



M=1

**ANS: Stateful DHCPv6 sets the flags to A=1, M=1.**

**CONFIGURE A DHCPV6 SERVER**

8.4.1

## DHCPv6 Router Roles

Cisco IOS routers are powerful devices. In smaller networks, you do not have to have separate devices to have a DHCPv6 server, client, or relay agent. A Cisco IOS router can be configured to provide DHCPv6 server services.

Specifically, it can be configured to be one of the following:

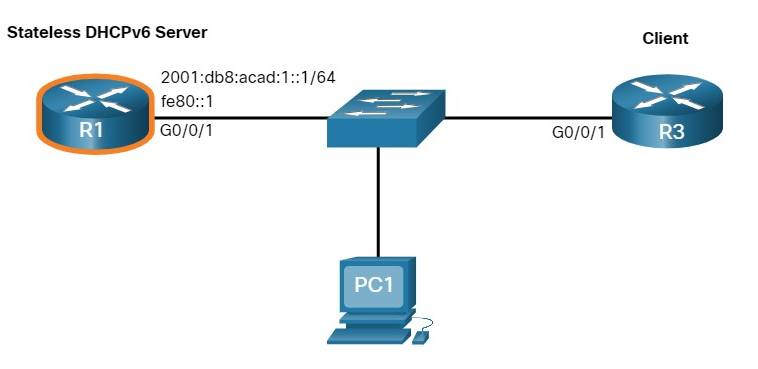
* **DHCPv6 Server** - Router provides stateless or stateful DHCPv6 services.
* **DHCPv6 Client** - Router interface acquires an IPv6 IP configuration from a DHCPv6 server.
* **DHCPv6 Relay Agent** - Router provides DHCPv6 forwarding services when the client and the server are located on different networks.

8.4.2

## Configure a Stateless DHCPv6 Server

The stateless DHCPv6 server option requires that the router advertise the IPv6 network addressing information in RA messages. However, the client must contact a DHCPv6 server for more information.

Refer to the sample topology to learn how to configure the stateless DHCPv6 server method.

****

In this example, R1 will provide SLAAC services for the host IPv6 configuration and DHCPv6 services.

There are five steps to configure and verify a router as a **stateless DHCPv6 server:**

**Step 1**. Enable IPv6 routing.  
**Step 2**. Define a DHCPv6 pool name.  
**Step 3**. Configure the DHCPv6 pool.  
**Step 4**. Bind the DHCPv6 pool to an interface.  
**Step 5**. Verify that the hosts have received IPv6 addressing information.

**Step 1. Enable IPv6 routing.**

The **ipv6 unicast-routing** command is required to enable IPv6 routing. Although it is not necessary for the router to be a stateless DHCPv6 server, it is required for the router to source ICMPv6 RA messages.



**Step 2. Define a DHCPv6 pool name.**

Create the DHCPv6 pool using the **ipv6 dhcp pool** POOL-NAME global config command. This enters DHCPv6 pool sub-configuration mode as identified by the **Router(config-dhcpv6)#** prompt.

**Note:** The pool name does not have to be uppercase. However, using an uppercase name makes it easier to see in a configuration.



**Step 3. Configure the DHCPv6 pool.**

R1 will be configured to provide additional DHCP information including DNS server address and domain name, as shown in the command output.

****

**Step 4. Bind the DHCPv6 pool to an interface.**

The DHCPv6 pool has to be bound to the interface using the **ipv6 dhcp server** POOL-NAME interface config command as shown in the output.

The router responds to stateless DHCPv6 requests on this interface with the information contained in the pool. The O flag needs to be manually 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. The A flag is 1 by default, telling clients to use SLAAC to create their own GUA.

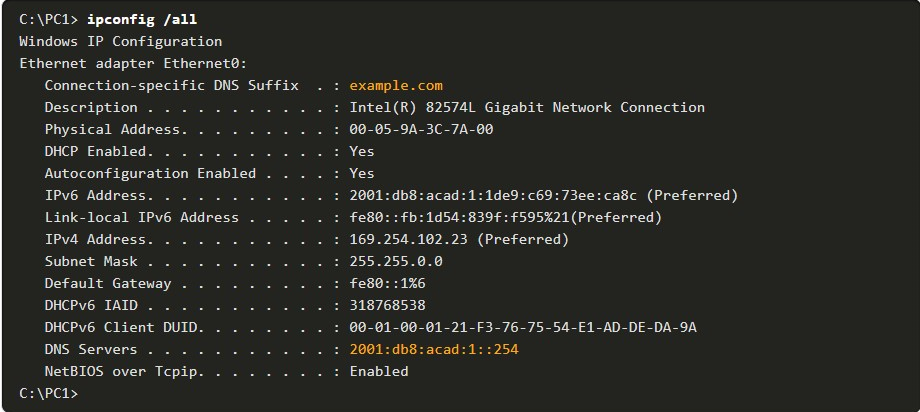
****

**Step 5. Verify hosts received IPv6 addressing information.**

To verify stateless DHCP on a Windows host, use the **ipconfig /all** command. The example output displays the settings on PC1.

Notice in the output that PC1 created its IPv6 GUA using the 2001:db8:acad:1::/64 prefix. Also notice that the default gateway is the IPv6 link-local address of R1. This confirms that PC1 derived its IPv6 configuration from the RA of R1.

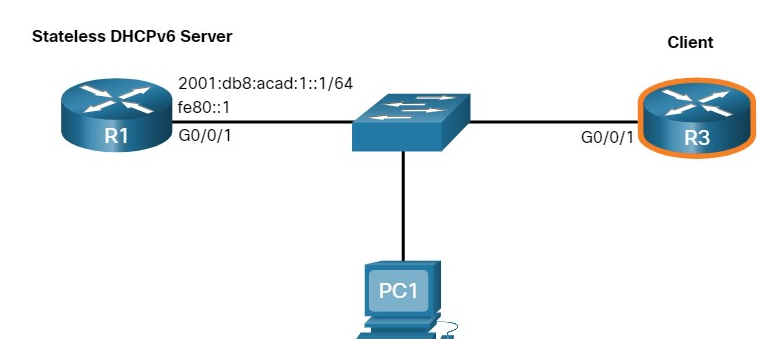
The highlighted output confirms that PC1 has learned the domain name and DNS server address information from the stateless DHCPv6 server.

****

8.4.3

Configure a Stateless DHCPv6 Client

A router can also be a DHCPv6 client and get an IPv6 configuration from a DHCPv6 server, such as a router functioning as a DHCPv6 server. In the figure, R1 is a stateless DHCPv6 server.

****

There are five steps to configure and verify a router as a stateless DHCPv6 server.

**Step 1**. Enable IPv6 routing.  
**Step 2**. Configure the client router to create an LLA.  
**Step 3**. Configure the client router to use SLAAC.  
**Step 4**. Verify that the client router is assigned a GUA.  
**Step 5**. Verify that the client router received other necessary DHCPv6 information.

**Step 1. Enable IPv6 routing.**

The DHCPv6 client router needs to have **ipv6 unicast-routing** enabled.

****

**Step 2. Configure client router to create an LLA.**

The client router needs to have a link-local address. An IPv6 link-local address is created on a router interface when a global unicast address is configured. It can also be created without a GUA using the **ipv6 enable** interface configuration command. Cisco IOS uses EUI-64 to create a randomized Interface ID.

In the output, the **ipv6 enable** command is configured on the Gigabit Ethernet 0/0/1 interface of the R3 client router.

****

**Step 3. Configure client router to use SLAAC.**

The client router needs to be configured to use SLAAC to create an IPv6 configuration. The **ipv6 address autoconfig** command enables the automatic configuration of IPv6 addressing using SLAAC.

****

**Step 4. Verify client router is assigned a GUA.**

Use the **show ipv6 interface brief** command to verify the host configuration as shown. The output confirms that the G0/0/1 interface on R3 was assigned a valid GUA.

**Note**: it may take the interface a few seconds to complete the process.

****

**Step 5. Verify client router received other DHCPv6 information.**

The **show ipv6 dhcp interface g0/0/1** command confirms that the DNS and domain names were also learned by R3.

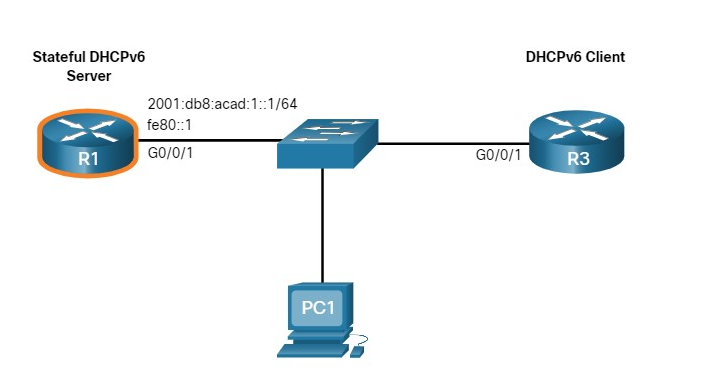
****

8.4.4

Configure a Stateful DHCPv6 Server

The stateful DHCP server option requires that the IPv6 enabled router tells the host to contact a DHCPv6 server to obtain all necessary IPv6 network addressing information.

In the figure, R1 will provide stateful DHCPv6 services to all hosts on the local network. Configuring a stateful DHCPv6 server is similar to configuring a stateless server. The most significant difference is that a stateful DHCPv6 server also includes IPv6 addressing information similar to a DHCPv4 server.

****

There are five steps to configure and verify a router as a stateless DHCPv6 server:

**Step 1**. Enable IPv6 routing.  
**Step 2**. Define a DHCPv6 pool name.  
**Step 3**. Configure the DHCPv6 pool.  
**Step 4**. Bind the DHCPv6 pool to an interface.  
**Step 5**. Verify that the hosts have received IPv6 addressing information.

**Step 1. Enable IPv6 routing.**

The **ipv6 unicast-routing** command is required to enable IPv6 routing.

****

**Step 2. Define a DHCPv6 pool name.**

Create the DHCPv6 pool using the **ipv6 dhcp pool** POOL-NAME global config command.

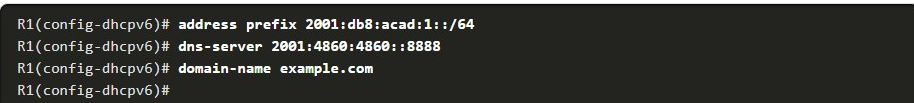
****

**Step 3. Configure the DHCPv6 pool.**

R1 will be configured to provide IPv6 addressing, DNS server address, and domain name, as shown in the command output.

With stateful DHCPv6, all addressing and other configuration parameters must be assigned by the DHCPv6 server. The **address prefix** command is used to indicate the pool of addresses to be allocated by the server. Other information provided by the stateful DHCPv6 server typically includes DNS server address and the domain name, as shown in the output.

**Note**: This example is setting the DNS server to Google's public DNS server.

****

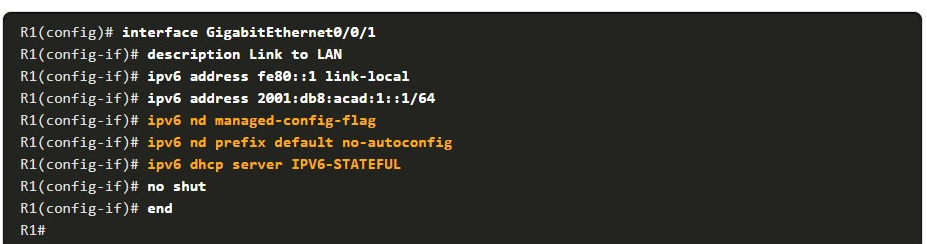
**Step 4. Bind the DHCPv6 pool to an interface.**

The example shows the full configuration of the GigabitEthernet 0/0/1 interface on R1.

The DHCPv6 pool has to be bound to the interface using the **ipv6 dhcp server** *POOL-NAME* interface config command.

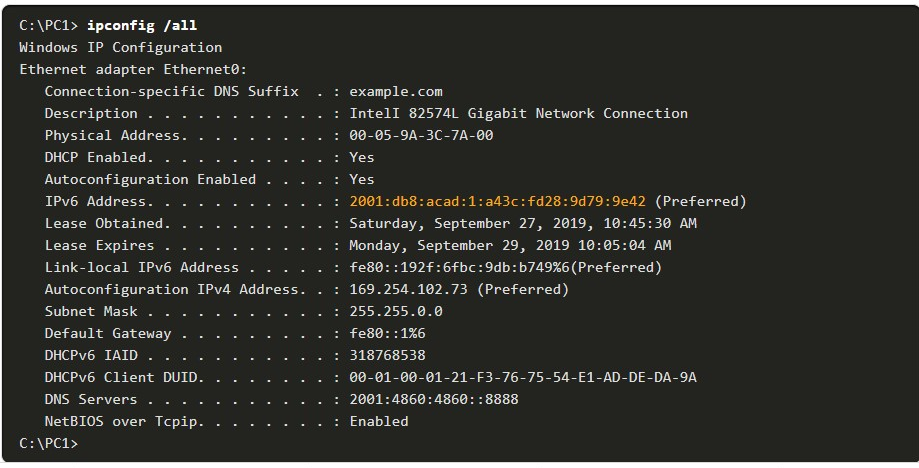
* The M flag is manually changed from 0 to 1 using the interface command **ipv6 nd managed-config-flag**.
* The A flag is manually changed from 1 to 0 using the interface command **ipv6 nd prefix default** **no-autoconfig**. The A flag can be left at 1, but some client operating systems such as Windows will create a GUA using SLAAC and get a GUA from the stateful DHCPv6 server. Setting the A flag to 0 tells the client not to use SLAAC to create a GUA.
* The **ipv6 dhcp server** command binds the DHCPv6 pool to the interface. R1 will now respond with the information contained in the pool when it receives stateful DHCPv6 requests on this interface.

**Note:** You can use the **no ipv6 nd managed-config-flag** command to set the M flag back to its default of 0. The **no ipv6 nd prefix default no-autoconfig** command sets the A flag back to its default of 1.

****

**Step 5. Verify hosts received IPv6 addressing information.**

To verify on a Windows host, use the **ipconfig /all** command to verify the stateless DHCP configuration method. The output displays the settings on PC1. The highlighted output shows that PC1 has received its IPv6 GUA from a stateful DHCPv6 server.

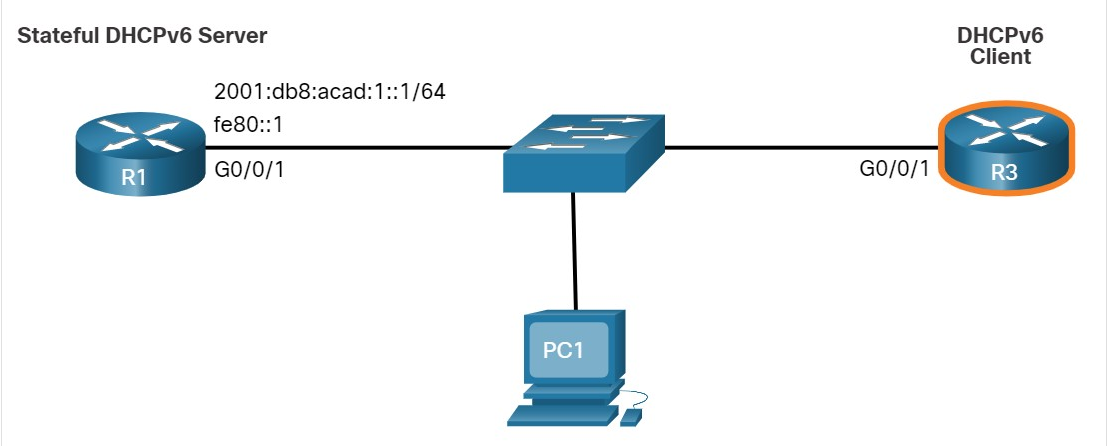
****

8.4.5

Configure a Stateful DHCPv6 Client

A router can also be a DHCPv6 client. The client router needs to have **ipv6 unicast-routing** enabled and an IPv6 link-local address to send and receive IPv6 messages.

Refer to the sample topology to learn how to configure the stateful DHCPv6 client

****

There are five steps to configure and verify a router as a stateful DHCPv6 server.

**Step 1**. Enable IPv6 routing.  
**Step 2**. Configure the client router to create an LLA.  
**Step 3**. Configure the client router to use DHCPv6.  
**Step 4**. Verify that the client router is assigned a GUA.  
**Step 5**. Verify that the client router received other necessary DHCPv6 information.

**Step 1. Enable IPv6 routing.**

The DHCPv6 client router needs to have **ipv6 unicast-routing** enabled.

****

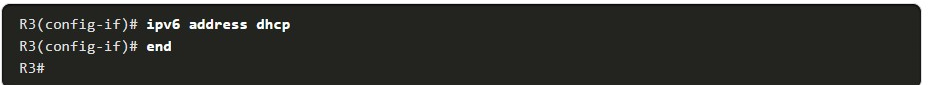
**Step 2. Configure client router to create an LLA.**

In the output, the **ipv6 enable** command is configured on the R3 Gigabit Ethernet 0/0/1 interface. This enables the router to create an IPv6 LLA without needing a GUA.

****

**Step 3. Configure client router to use DHCPv6.**

The **ipv6 address dhcp** command configures R3 to solicit its IPv6 addressing information from a DHCPv6 server.

****

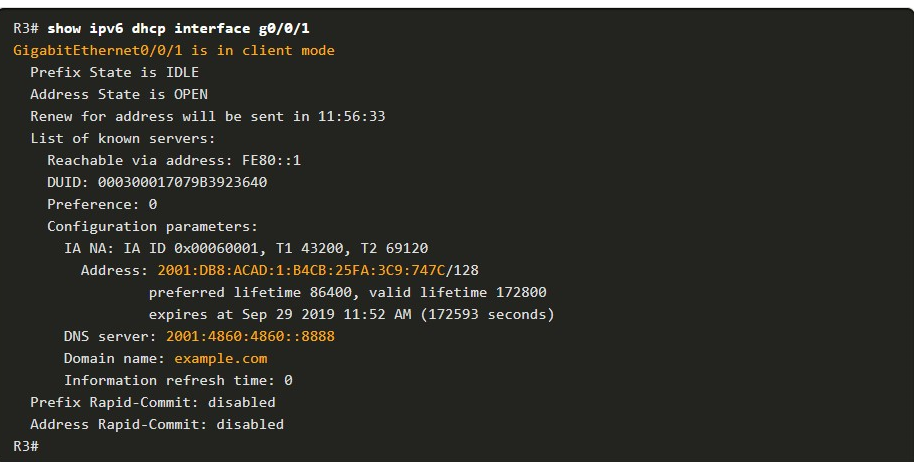
**Step 4. Verify client router is assigned a GUA.**

Use the **show ipv6 interface brief** command to verify the host configuration as shown.

****

**Step 5. Verify client router received other DHCPv6 information.**

The **show ipv6 dhcp interface g0/0/1** command confirms that the DNS and domain names were learned by R3.

****

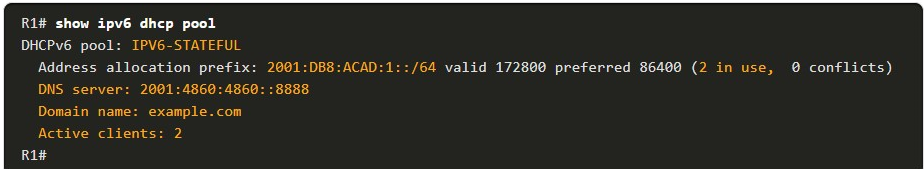
8.4.6

DHCPv6 Server Verification Commands

Use the **show ipv6 dhcp pool** and **show ipv6 dhcp binding** commands to verify DHCPv6 operation on a router.

The **show ipv6 dhcp pool** command verifies the name of the DHCPv6 pool and its parameters. The command also identifies the number of active clients. In this example, the IPV6-STATEFUL pool currently has 2 clients, which reflects PC1 and R3 receiving their IPv6 global unicast address from this server.

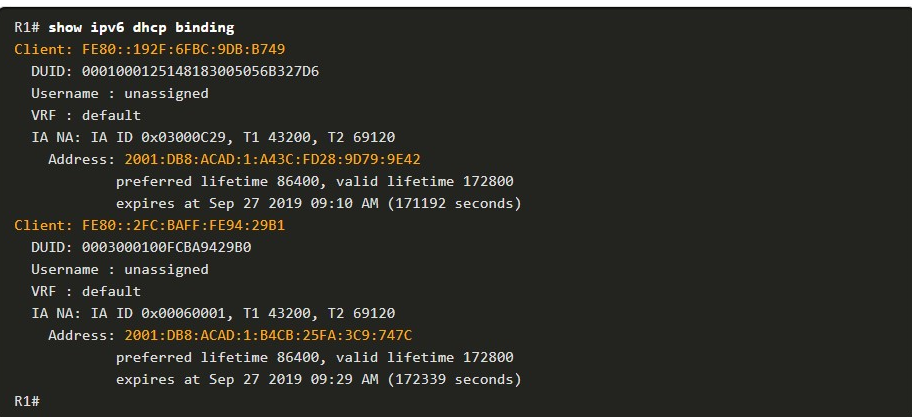
When a router is providing stateful DHCPv6 services, it also maintains a database of assigned IPv6 addresses

****

Use the **show ipv6 dhcp binding** command output to display the IPv6 link-local address of the client and the global unicast address assigned by the server.

The output displays the current stateful binding on R1. The first client in the output is PC1 and the second client is R3.

This information is maintained by a stateful DHCPv6 server. A stateless DHCPv6 server would not maintain this information.

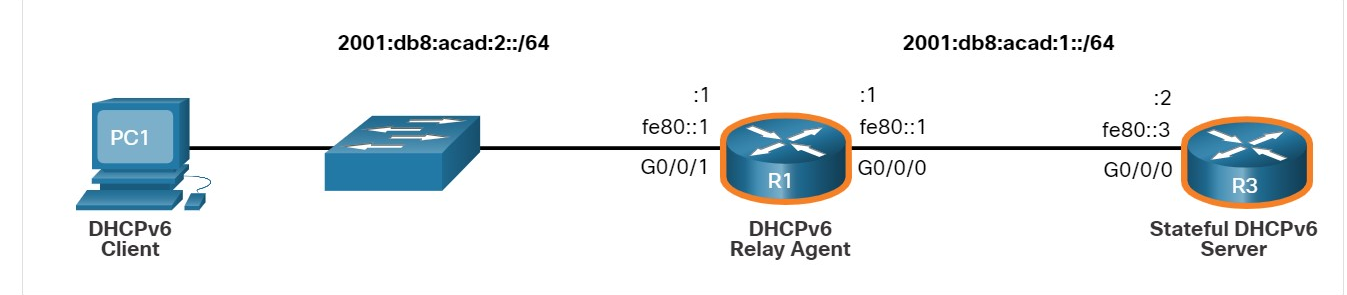
****

8.4.7

Configure a DHCPv6 Relay Agent

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.

In the figure, R3 is configured as a stateful DHCPv6 server. PC1 is on the 2001:db8:acad:2::/64 network and requires the services of a stateful DHCPv6 server to acquire its IPv6 configuration. R1 needs to be configured as the DHCPv6 Relay Agent.

****

The command syntax to configure a router as a DHCPv6 relay agent is as follows:

****

This command is configured on the interface facing the DHCPv6 clients and specifies the DHCPv6 server address and egress interface to reach the server, as shown in the output. The egress interface is only required when the next-hop address is an LLA.

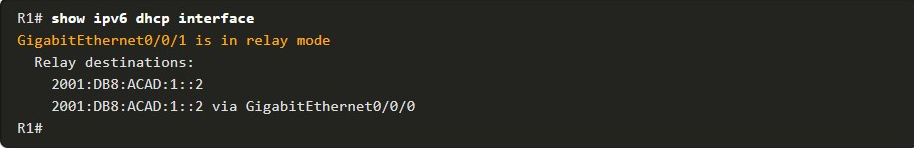
8.4.8

Verify the DHCPv6 Relay Agent

Verify that the DHCPv6 relay agent is operational with the **show ipv6 dhcp interface** and **show ipv6 dhcp binding** commands. Verify Windows hosts received IPv6 addressing information with the **ipconfig /all** command

1. **show ipv6 dhcp interface**

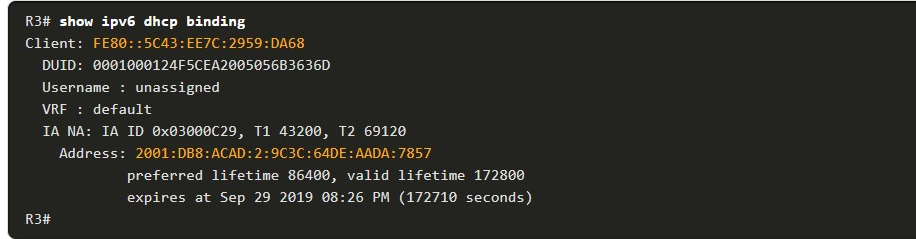
The DHCPv6 relay agent can be verified using the **show ipv6 dhcp interface** command. This will verify that the G0/0/1 interface is in relay mode.

****

**2.** **show ipv6 dhcp binding**

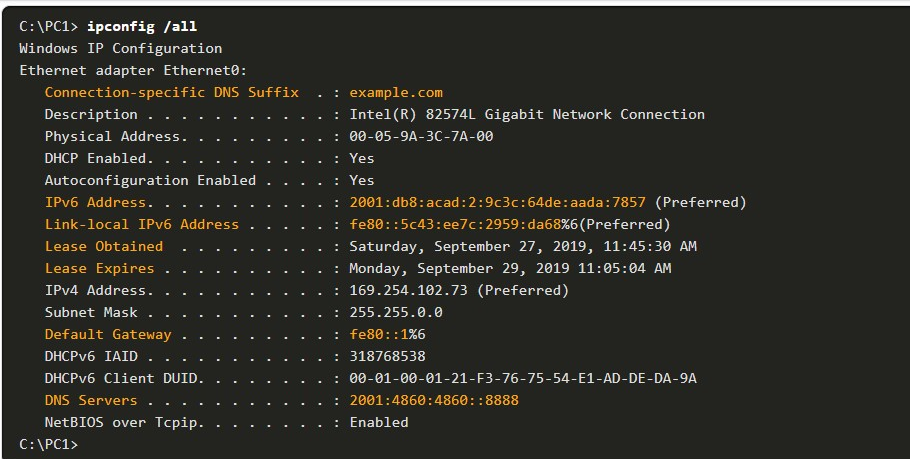
On R3, use the **show ipv6 dhcp binding command** to verify if any hosts have been assigned an IPv6 configuration.

Notice that a client link-local address has been assigned an IPv6 GUA. We can assume that this is PC1.



3. **ipconfig /all**

Finally, use **ipconfig /all** on PC1 to confirm that it has been assigned an IPv6 configuration. As you can see, PC1 has indeed received its IPv6 configuration from the DHCPv6 server.



You have successfully identified the correct answers.

1. .
2. Which three DHCPv6 roles can a router perform? (Choose all that apply.)



DHCPv6 client



DHCPv6 relay agent



DHCPv6 server

**ANS: A router can be a DHCPv6 client, server, or relay agent**

1. Which command is not configured in stateless DHCPv6?



**address prefix** *ipv6-address/prefix*



**domain-name** *name*



**dns-server** *server-address*



**ipv6 dhcp server** *pool-name*

**ANS: The address prefix *ipv6-address/prefix* command is used for stateful DHCPv6**.

1. An IPv6-enabled router is to acquire its IPv6 GUA from another IPv6 router using SLAAC. Which interface configuration command should be configured on the client router?



**ipv6 address autoconfig**



**ipv6 address auto config**



**ipv6 address dhcp**



**ipv6 address dhcpv6**

**ANS: The ipv6 address dhcp command configured a router interface to be a DHCPv6 client**.

1. A router is to provide DHCPv6 server services. Which command should be configured on the client facing interface?



**ipv6 enable**



**ipv6 dhcp pool** *POOL-NAME*



**ipv6 dhcp server** *POOL-NAME*



**ipv6 nd other-config-flag**

**ANS: The ipv6 dhcp server IPV6-STATEFUL command is issued on the router interface facing the DHCPv6 clients.**

1. An IPv6-enabled router is to acquire its IPv6 GUA from a DHCPv6 server. Which interface configuration command should be configured on client router?



**ipv6 address autoconfig**



**ipv6 address auto config**



**ipv6 address dhcp**



**ipv6 address dhcpv6**

**ANS: The ipv6 address dhcp command configured a router interface to be a DHCPv6 client.**

1. Which DHCPv6 verification command would display the link-local and GUA assigned address for each active client?



**show ip dhcp pool**



**show ipv6 dhcp binding**



**show ipv6 dhcp interface**



**show ipv6 dhcp pool**

**ANS: The show ipv6 dhcp binding command output will show active DHCPv6 leases to clients**.

1. Which command is configured on the client LAN interface of the DHCPv6 relay agent?



**ip helper-address**



**ipv6 dhcp relay destination**



**ipv6 enable**



**ipv6 helper-address**

**ANS: The ipv6 dhcp relay destination command is issued on the client facing interface of the DHCPv6 relay agent.**

8.5.1

## Lab - Configure DHCPv6(pending)

In this lab, you will complete the following objectives:

* Part 1: Build the Network and Configure Basic Device Settings
* Part 2: Verify SLAAC address assignment from R1
* Part 3: Configure and verify a Stateless DHCPv6 Server on R1
* Part 4: Configure and verify a Stateful DHCPv6 Server on R1
* Part 5: Configure and verify a DHCPv6 Relay on R2

8.5.2

## What did I learn in this module?

**IPv6 GUA Assignment**

On a router, an IPv6 global unicast addresses (GUA) is manually configured using the **ipv6 address** ipv6-address/prefix-length interface configuration command.

When automatic IPv6 addressing is selected, the host will attempt to automatically obtain and configure IPv6 address information on the interface.

The IPv6 link-local address is automatically created by the host when it boots and the Ethernet interface is active. By default, an IPv6-enabled router advertises its IPv6 information enabling a host to dynamically create or acquire its IPv6 configuration.

The IPv6 GUA can be assigned dynamically using stateless and stateful services. The decision of how a client will obtain an IPv6 GUA depends on the settings within the RA message. An ICMPv6 RA message includes three flags to identify the dynamic options available to a host:

* **A flag** – This is the Address Autoconfiguration flag. Use SLAAC to create an IPv6 GUA.
* **O flag** – This is the Other Configuration flag. Get Other information from a stateless DHCPv6 server.
* **M flag** – This is the Managed Address Configuration flag. Use a stateful DHCPv6 server to obtain an IPv6 GUA.

**SLAAC**

The SLAAC method enables hosts to create their own unique IPv6 global unicast address without the services of a DHCPv6 server.

SLAAC, which is stateless, uses ICMPv6 RA messages to provide addressing and other configuration information that would normally be provided by a DHCP server.

SLAAC can be deployed as SLAAC only, or SLAAC with DHCPv6. To enable the sending of RA messages, a router must join the IPv6 all-routers group using the **ipv6 unicast-routing** global config command.

Use the **show ipv6 interface** command to verify if a router is enabled. The SLAAC only method is enabled by default when the ipv6 unicast-routing command is configured. All enabled Ethernet interfaces with an IPv6 GUA configured will start sending RA messages with the A flag set to 1, and the O and M flags set to 0.

The A = 1 flag suggests to the client to create its own IPv6 GUA using the prefix advertised in the RA. The O =0 and M=0 flags instructs the client to use the information in the RA message exclusively.

A router sends RA messages every 200 seconds. However, it will also send an RA message if it receives an RS message from a host. Using SLAAC, a host typically acquires its 64-bit IPv6 subnet information from the router RA. However, it must generate the remainder 64-bit interface identifier (ID) using one of two methods: randomly generated, or EUI-64. The DAD process is used by a host to ensure that the IPv6 GUA is unique. DAD is implemented using ICMPv6. To perform DAD, the host sends an ICMPv6 NS message with a specially constructed multicast address, called a solicited-node multicast address. This address duplicates the last 24 bits of IPv6 address of the host.

**DHCPv6**

The host begins the DHCPv6 client/server communications after stateless DHCPv6 or stateful DHCPv6 is indicated in the RA.

Server to client DHCPv6 messages use UDP destination port 546, while client to server DHCPv6 messages use UDP destination port 547.

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. This is called stateless DHCPv6 because the server is not maintaining any client state information.

Stateless DHCPv6 is enabled on a router interface using the **ipv6 nd other-config-flag** interface configuration command. This sets the O flag to 1. In stateful DHCPv6, the RA message tells the client to obtain all addressing information from a stateful DHCPv6 server, except the default gateway address which is the source IPv6 link-local address of the RA. It is called stateful because the DHCPv6 server maintains IPv6 state information. Stateful DHCPv6 is enabled on a router interface using the **ipv6 nd managed-config-flag** interface configuration command. This sets the M flag to 1.

**Configure DHCPv6 Server**

A Cisco IOS router can be configured to provide DHCPv6 server services as one of the following three types: DHCPv6 server, DHCPv6 client, or DHCPv6 relay agent.

The stateless DHCPv6 server option requires that the router advertise the IPv6 network addressing information in RA messages. A router can also be a DHCPv6 client and get an IPv6 configuration from a DHCPv6 server.

The stateful DHCP server option requires that the IPv6-enabled router tells the host to contact a DHCPv6 server to acquire all required IPv6 network addressing information.

For a client router to be a DHCPv6 router, it needs to **have ipv6 unicast-routing** enabled and an IPv6 link-local address to send and receive IPv6 messages. Use the **show ipv6 dhcp pool** and **show ipv6 dhcp binding** commands to verify DHCPv6 operation on a router.

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 using the **ipv6 dhcp relay destination** ipv6-address [interface-type interface-number] command.

This command is configured on the interface facing the DHCPv6 clients and specifies the DHCPv6 server address and egress interface to reach the server. The egress interface is only required when the next-hop address is an LLA. Verify the DHCPv6 relay agent is operational with the **show ipv6 dhcp interface** and **show ipv6 dhcp binding** commands.

1. How does an IPv6 client ensure that it has a unique address after it configures its IPv6 address using the SLAAC allocation method?

Topic 8.2.0 - SLAAC is a stateless allocation method and does not use a DHCP server to manage the IPv6 addresses. When a host generates an IPv6 address, it must verify that it is unique. The host will send an ICMPv6 Neighbor Solicitation message with its own IPv6 address as the target. As long as no other device responds with a Neighbor Advertisement message, then the address is unique.



It sends an ICMPv6 Neighbor Solicitation message with the IPv6 address as the target IPv6 address.



It checks with the IPv6 address database that is hosted by the SLAAC server.



It sends an ARP message with the IPv6 address as the destination IPv6 address.



It contacts the DHCPv6 server via a special formed ICMPv6 message.

1. Which method would an IPv6-enabled host using SLAAC employ to learn the address of the default gateway?

Topic 8.2.0 - When using SLAAC, a host will learn from the router advertisement that is sent by the link router the address to use as a default gateway.



reply messages that are received from the DHCPv6 server



advertise messages that are received from the DHCPv6 server



neighbor advertisements that are eceived from link neighbors



router advertisements that are received from the link router

1. What two methods can be used to generate an interface ID by an IPv6 host that is using SLAAC? (Choose two.)

Topic 8.2.0 - A host that is using SLAAC has two means to configure an interface ID: EUI-64 and random generation by the host operating system.



stateful DHCPv6



random generation



DAD



ARP



EUI-64

1. A client is using SLAAC to obtain an IPv6 address for its interface. After an address has been generated and applied to the interface, what must the client do before it can begin to use this IPv6 address?

Topic 8.3.0 - Stateless DHCPv6 or stateful DHCPv6 uses a DHCP server, but Stateless Address Autoconfiguration (SLAAC) does not. A SLAAC client can automatically generate an address that is based on information from local routers via Router Advertisement (RA) messages. Once an address has been assigned to an interface via SLAAC, the client must ensure via Duplicate Address Detection (DAD) that the address is not already in use. It does this by sending out an ICMPv6 Neighbor Solicitation message and listening for a response. If a response is received, then it means that another device is already using this address.



It must send an ICMPv6 Router Solicitation message to determine what default gateway it should use.



It must send an ICMPv6 Neighbor Solicitation message to ensure that the address is not already in use on the network.



It must send a DHCPv6 REQUEST message to the DHCPv6 server to request permission to use this address.



It must send a DHCPv6 INFORMATION-REQUEST message to request the address of the DNS server.

1. Which command should be configured on a router interface to set the router as a stateful DHCPv6 client?

Topic 8.4.0 - When the **ipv6 address dhcp** command is configured on a router interface, it enables the router as a DHCPv6 client on this interface. The **ipv6 enable** command enables IPv6 on an interface and allows the router to configure its link-local address. The **ipv6 address autoconfigure** command tells the router to use either SLAAC or stateless DHCPv6 to configure its global unicast address. The **ipv6 dhcp server** command is used on a router that is running a DHCPv6 server to indicate what address information should be served to clients.



**ipv6 enable**



**ipv6 address autoconfigure**



**ipv6 dhcp server stateful**



**ipv6 address dhcp**

1. What message informs IPv6 enabled interfaces to use stateful DHCPv6 for obtaining an IPv6 address?

Topic 8.2.0 - Before an IPv6 enabled interface will use stateful DHCPv6 to obtain an IPv6 address, the interface must receive an ICMPv6 Router Advertisement with the managed configuration flag (M flag) set to 1.



the ICMPv6 Router Solicitation



the ICMPv6 Router Advertisement



the DHCPv6 Reply message



the DHCPv6 Advertise message

1. Which destination IP address is used when an IPv6 host sends a DHCPv6 SOLICIT message to locate a DHCPv6 server?

Topic 8.3.0 - DHCPv6 hosts will send a DHCP SOLICIT message to the all DHCP routers multicast address of FF02::1:2.



FF02::1



FF02::1:2



FE80::1



FF02::2

1. In which alternative to DHCPv6 does a router dynamically provide IPv6 configuration information to hosts?

Topic 8.2.0 - Stateless Address Autoconfiguration (SLAAC) can be used as an alternative to DHCPv6. In this approach, a router provides global routing prefix, prefix length, default gateway, and DNS server information to a host. The host is not provided with a global unicast address by SLAAC. Instead, SLAAC suggests that the host create its own global unicast address based on the supplied global routing prefix. ARP is not used in IPv6. ICMPv6 messages are used by SLAAC to provide addressing and other configuration information. EUI-64 is a process in which a host will create an Interface ID from its 48-bit MAC address.



ARP



EUI-64



SLAAC



ICMPv6

1. A company implements the stateless DHCPv6 method for configuring IPv6 addresses on employee workstations. After a workstation receives messages from multiple DHCPv6 servers to indicate their availability for DHCPv6 service, which message does it send to a server for configuration information?

Topic 8.3.0 - In stateless DHCPv6 configuration, a client configures its IPv6 address by using the prefix and prefix length in the RA message, combined with a self-generated interface ID. It then contacts a DHCPv6 server for additional configuration information via an INFORMATION-REQUEST message. The DHCPv6 SOLICIT message is used by a client to locate a DHCPv6 server. The DHCPv6 ADVERTISE message is used by DHCPv6 servers to indicate their availability for DHCPv6 service. The DHCPv6 REQUEST message is used by a client, in the stateful DHCPv6 configuration, to request ALL configuration information from a DHCPv6 server.



DHCPv6 REQUEST



DHCPv6 SOLICIT



DHCPv6 ADVERTISE



DHCPv6 INFORMATION-REQUEST

1. What process is used in ICMPv6 for a host to verify that an IPv6 address is unique before configuring it on an interface?

Topic 8.2.0 - Before an IPv6 host can enable and use an assigned IPv6 address, the host must verify that the address is unique on the network. To verify that no other hosts are using the IPv6 address, the host performs the duplicate address detection (DAD) process by sending a Neighbor Solicitation (NS) message to the IPv6 address.



EUI-64



SLAAC



DAD



ARP

1. What are two characteristics of the SLAAC method for IPv6 address configuration? (Choose two.)

Topic 8.2.0 - With SLAAC, the default gateway for IPv6 clients will be the link-local address of the router interface that is attached to the client LAN. The IPv6 addressing is dynamically assigned via the ICMPv6 protocol. SLAAC is a stateless method of acquiring an IPv6 address, a method that requires no servers. When a client is configured to obtain its addressing information automatically via SLAAC, the client sends a router solicitation message to the IPv6 all-routers multicast address FF02::2. The router advertisement messages are sent by routers to provide addressing information to clients.



Router solicitation messages are sent by the router to offer IPv6 addressing to clients.



IPv6 addressing is dynamically assigned to clients through the use of ICMPv6.



The default gateway of an IPv6 client on a LAN will be the link-local address of the router interface attached to the LAN.



Clients send router advertisement messages to routers to request IPv6 addressing.



This stateful method of acquiring an IPv6 address requires at least one DHCPv6 server.

1. After booting, a client receives an ICMPv6 RA message with the M flag set to 0 and the O flag set to 1. What does this indicate?

Topic 8.3.0 - The Managed Address Configuration (M) flag and the Other Configuration (O) flag in ICMPv6 RA messages are used to indicate to an IPv6 client how it should configure its IPv6 addresses. If the M flag is set to 0 it means that the host should automatically configure its own IPv6 interface address rather than asking for one from a DHCPv6 server. If the O flag is set to 1, it means that the client can find additional addressing information, such as a DNS server address, by contacting a DHCPv6 server after it has automatically configured its own address.



The client should automatically configure an IPv6 address and then contact a DHCPv6 server for more information.



The client should automatically configure an IPv6 address without contacting a DHCPv6 server.



The client should be statically configured with an IPv6 address because the local router does not support autoconfiguration.



The client should request an IPv6 address directly from a DHCPv6 server.

1. A network administrator is entering the command **ipv6 unicast-routing** to start configuring DHCPv6 operation on a router. Which statement describes the function of this command?

Topic 8.2.0 - The **ipv6 unicast-routing** command is required to enable IPv6 routing on a router. This command is not necessary for the router to be a stateless or stateful DHCPv6 server, but is required for sending ICMPv6 RA messages.



It is required for sending ICMPv6 RA messages.



It is required to configure stateful DHCPv6 server on the router.



It is required to configure stateless DHCPv6 server on the router.



It is required for enabling DNS service in DHCPv6 configurations.