



Configuring IPv6 Client IP Address Learning

- [Prerequisites for IPv6 Client Address Learning, on page 1](#)
- [Information About IPv6 Client Address Learning, on page 1](#)
- [Configuring IPv6 Unicast, on page 5](#)
- [Configuring RA Guard Policy, on page 6](#)
- [Applying RA Guard Policy, on page 7](#)
- [Configuring IPv6 Snooping, on page 8](#)
- [Configuring IPv6 ND Suppress Policy, on page 9](#)
- [Configuring IPv6 Snooping on VLAN/PortChannel, on page 10](#)
- [Configuring IPv6 on Interface, on page 11](#)
- [Configuring DHCP Pool , on page 12](#)
- [Configuring Stateless Auto Address Configuration Without DHCP \(CLI\), on page 14](#)
- [Configuring Stateless Auto Address Configuration With DHCP , on page 15](#)
- [Configuring Stateful DHCP Locally, on page 16](#)
- [Configuring Stateful DHCP Externally, on page 18](#)
- [Verifying IPv6 Address Learning Configuration, on page 20](#)
- [Additional References, on page 21](#)
- [Feature Information for IPv6 Client Address Learning, on page 22](#)

Prerequisites for IPv6 Client Address Learning

Before configuring IPv6 client address learning, configure the clients to support IPv6.

Information About IPv6 Client Address Learning

Client Address Learning is configured on device to learn the client's IPv4 and IPv6 address and clients transition state maintained by the device on an association, re-association, de-authentication and timeout.

There are three ways for IPv6 client to acquire IPv6 addresses:

- Stateless Address Auto-Configuration (SLACC)
- Stateful DHCPv6
- Static Configuration

For all of these methods, the IPv6 client always sends neighbor solicitation DAD (Duplicate Address Detection) request to ensure there is no duplicate IP address on the network. The device snoops the client's NDP and DHCPv6 packets to learn about its client IP addresses.

SLAAC Address Assignment

The most common method for IPv6 client address assignment is Stateless Address Auto-Configuration (SLAAC). SLAAC provides simple plug-and-play connectivity where clients self-assign an address based on the IPv6 prefix. This process is achieved

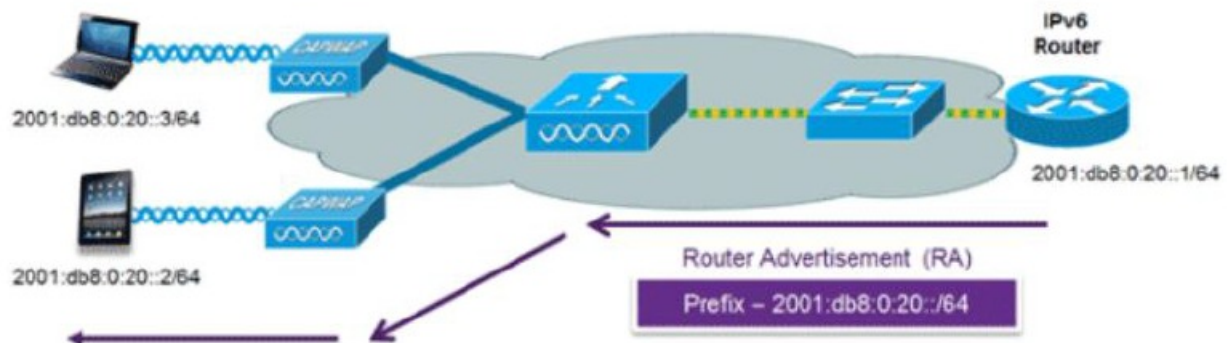
Stateless Address Auto-Configuration (SLAAC) is configured as follows:

- Host sends a router solicitation message.
- Hosts wait for a Router Advertisement message.
- Hosts take the first 64 bits of the IPv6 prefix from the Router Advertisement message and combine it with the 64 bit EUI-64 address (in the case of ethernet, this is created from the MAC Address) to create a global unicast message. The host also uses the source IP address, in the IP header, of the Router Advertisement message, as its default gateway.
- Duplicate Address Detection is performed by IPv6 clients in order to ensure that random addresses that are picked do not collide with other clients.
- The choice of algorithm is up to the client and is often configurable.

The last 64 bits of the IP v6 address can be learned based on the following 2 algorithms:

- EUI-64 which is based on the MAC address of the interface, or
- Private addresses that are randomly generated.

Figure 1: SLAAC Address Assignment



The following Cisco IOS configuration commands from a Cisco-capable IPv6 router are used to enable SLAAC addressing and router advertisements:

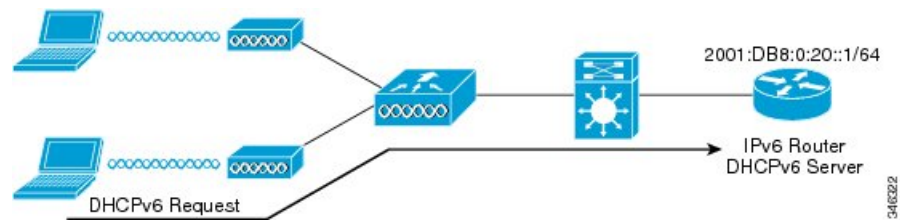
```

ipv6 unicast-routing
interface Vlan20
description IPv6-SLAAC
ip address 192.168.20.1 255.255.255.0
ipv6 address FE80:DB8:0:20::1 linklocal
ipv6 address 2001:DB8:0:20::1/64
ipv6 enable
end

```

Stateful DHCPv6 Address Assignment

Figure 2: Stateful DHCPv6 Address Assignment



The use of DHCPv6 is not required for IPv6 client connectivity if SLAAC is already deployed. There are two modes of operation for DHCPv6 called Stateless and Stateful.

The DHCPv6 Stateless mode is used to provide clients with additional network information that is not available in the router advertisement, but not an IPv6 address as this is already provided by SLAAC. This information can include the DNS domain name, DNS server(s), and other DHCP vendor-specific options. This interface configuration is for a Cisco IOS IPv6 router implementing stateless DHCPv6 with SLAAC enabled:

```
ipv6 unicast-routing
ipv6 dhcp pool IPV6_DHCPPPOOL
address prefix 2001:db8:5:10::/64
domain-name cisco.com
dns-server 2001:db8:6:6::1
interface Vlan20
description IPv6-DHCP-Stateless
ip address 192.168.20.1 255.255.255.0
ipv6 nd other-config-flag
ipv6 dhcp server IPV6_DHCPPPOOL
ipv6 address 2001:DB8:0:20::1/64
end
```

The DHCPv6 Stateful option, also known as managed mode, operates similarly to DHCPv4 in that it assigns unique addresses to each client instead of the client generating the last 64 bits of the address as in SLAAC. This interface configuration is for a Cisco IOS IPv6 router implementing stateful DHCPv6 on a local Device:

```
ipv6 unicast-routing
ipv6 dhcp pool IPV6_DHCPPPOOL
address prefix 2001:db8:5:10::/64
domain-name cisco.com
dns-server 2001:db8:6:6::1
interface Vlan20
description IPv6-DHCP-Stateful
ip address 192.168.20.1 255.255.255.0
ipv6 address 2001:DB8:0:20::1/64
ipv6 nd prefix 2001:DB8:0:20::/64 no-advertise
ipv6 nd managed-config-flag
ipv6 nd other-config-flag
ipv6 dhcp server IPV6_DHCPPPOOL
end
```

This interface configuration is for a Cisco IOS IPv6 router implementing stateful DHCPv6 on an external DHCP server:

```
ipv6 unicast-routing
domain-name cisco.com
dns-server 2001:db8:6:6::1
interface Vlan20
description IPv6-DHCP-Stateful
ip address 192.168.20.1 255.255.255.0
ipv6 address 2001:DB8:0:20::1/64
```

```

ipv6 nd prefix 2001:DB8:0:20::/64 no-advertise
ipv6 nd managed-config-flag
ipv6 nd other-config-flag
ipv6 dhcp_relay destination 2001:DB8:0:20::2
end

```

Static IP Address Assignment

Statically configured address on a client.

Router Solicitation

A Router Solicitation message is issued by a host to facilitate local routers to transmit Router Advertisement from which it can obtain information about local routing or perform Stateless Auto-configuration. Router Advertisements are transmitted periodically and the host prompts with an immediate Router Advertisement using a Router Solicitation such as - when it boots or following a restart operation.

Router Advertisement

A Router Advertisement message is issued periodically by a router or in response to a Router Solicitation message from a host. The information contained in these messages is used by hosts to perform Stateless Auto-configuration and to modify its routing table.

Neighbor Discovery

IPv6 Neighbor Discovery is a set of messages and processes that determine relationships between neighboring nodes. Neighbor Discovery replaces ARP, ICMP Router Discovery, and ICMP Redirect used in IPv4.

IPv6 Neighbor Discovery inspection analyzes neighbor discovery messages in order to build a trusted binding table database, and IPv6 neighbor discovery packets that do not comply are dropped. The neighbor binding table in the switch tracks each IPv6 address and its associated MAC address. Clients are expired from the table according to Neighbor Binding timers.

Neighbor Discovery Suppression

The IPv6 addresses of clients are cached by the device. When the device receives an NS multicast looking for an IPv6 address, and if the target address is known to the device and belongs to one of its clients, the device will reply with an NA message on behalf of the client. The result of this process generates the equivalent of the Address Resolution Protocol (ARP) table of IPv4 but is more efficient - uses generally fewer messages.



Note

The device acts like proxy and respond with NA, only when the **ipv6 nd suppress** command is configured

If the device does not have the IPv6 address of a client, the device will not respond with NA and forward the NS packet. To resolve this, an NS Multicast Forwarding knob is provided. If this knob is enabled, the device gets the NS packet for the IPv6 address that it does not have (cache miss) and forwards it. This packet reaches the intended client and the client replies with NA.

This cache miss scenario occurs rarely, and only very few clients which do not implement complete IPv6 stack may not advertise their IPv6 address during NDP.

RA Guard

IPv6 clients configure IPv6 addresses and populate their router tables based on IPv6 router advertisement (RA) packets. The RA guard feature is similar to the RA guard feature of wired networks. RA guard increases the security of the IPv6 network by dropping the unwanted or rogue RA packets that come from clients. If this feature is not configured, malicious IPv6 clients announce themselves as the router for the network often with high priority, which would take higher precedence over legitimate IPv6 routers.

RA-Guard also examines the incoming RA's and decides whether to switch or block them based solely on information found in the message or in the switch configuration. The information available in the frames received is useful for RA validation:

- Port on which the frame is received
- IPv6 source address
- Prefix list

The following configuration information created on the switch is available to RA-Guard to validate against the information found in the received RA frame:

- Trusted/Untrusted ports for receiving RA-guard messages
- Trusted/Untrusted IPv6 source addresses of RA-sender
- Trusted/Untrusted Prefix list and Prefix ranges
- Router Preference

RA guard occurs at the device. You can configure the device to drop RA messages at the device. All IPv6 RA messages are dropped, which protects other clients and upstream wired network from malicious IPv6 clients.

```
//Create a policy for RA Guard//
ipv6 nd rguard policy rguard-router
trusted-port
device-role router

//Applying the RA Guard Policy on port/interface//
interface tengigabitethernet1/0/1 (Katana)
interface gigabitethernet1/0/1 (Edison)

ipv6 nd rguard attach-policy rguard-router
```

Configuring IPv6 Unicast

IPv6 unicasting must always be enabled on the switch . IPv6 unicast routing is disabled.

To configure IPv6 unicast, perform this procedure:

Before you begin

To enable the forwarding of IPv6 unicast datagrams, use the **ipv6 unicast-routing** command in global configuration mode. To disable the forwarding of IPv6 unicast datagrams, use the **no** form of this command.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 unicast routing**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	ipv6 unicast routing Example: Device(config)# ipv6 unicast routing	enable the forwarding of IPv6 unicast datagrams

Configuring RA Guard Policy

Configure RA Guard policy on the device to add IPv6 client addresses and populate the router table based on IPv6 router advertisement packets.

To configuring RA guard policy, perform this procedure:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 nd rguard policy rguard-router**
4. **trustedport**
5. **device-role router**
6. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	ipv6 nd raguard policy raguard-router Example: Device(config)# ipv6 nd raguard policy raguard-router	Defines the RA guard policy name and enters RA guard policy configuration mode.
Step 4	trustedport Example: Device(config-ra-guard)# trustedport	(Optional) Specifies that this policy is being applied to trusted ports.
Step 5	device-role router Example: Device(config-ra-guard)# device-role router	Specifies the role of the device attached to the port.
Step 6	exit Example: Device(config-ra-guard)# exit	Exits RA guard policy configuration mode and returns to global configuration mode.

Applying RA Guard Policy

Applying the RA Guard policy on the device will block all the untrusted RA's.

To apply RA guard policy, perform this procedure:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface tengigabitethernet 1/0/1**
4. **ipv6 nd raguard attach-policy raguard-router**
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	interface tengigabitethernet 1/0/1 Example: Device(config)# interface tengigabitethernet 1/0/1	Specifies an interface type and number, and places the device in interface configuration mode.
Step 4	ipv6 nd raguard attach-policy raguard-router Example: Device(config-if)# ipv6 nd raguard attach-policy raguard-router	Applies the IPv6 RA Guard feature to a specified interface.
Step 5	exit Example: Device(config-if)# exit	Exits interface configuration mode.

Configuring IPv6 Snooping

IPv6 snooping must always be enabled on the switch .

To configuring IPv6 snooping, perform this procedure:

Before you begin

Enable IPv6 on the client machine.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vlan configuration 1**
4. **ipv6 snooping**
5. **ipv6 nd suppress**
6. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	vlan configuration 1 Example: Device(config)# vlan configuration 1	Enters VLAN configuration mode.
Step 4	ipv6 snooping Example: Device(config-vlan)# ipv6 snooping	Enables IPv6 snooping on the Vlan.
Step 5	ipv6 nd suppress Example: Device(config-vlan-config)# ipv6 nd suppress	Enables the IPv6 ND suppress on the Vlan.
Step 6	exit Example: Device(config-vlan-config)# exit	Saves the configuration and comes out of the Vlan configuration mode.

Configuring IPv6 ND Suppress Policy

The IPv6 neighbor discovery (ND) multicast suppress feature stops as many ND multicast neighbor solicit (NS) messages as possible by dropping them (and responding to solicitations on behalf of the targets) or converting them into unicast traffic. This feature runs on a layer 2 switch and is used to reduce the amount of control traffic necessary for proper link operations.

When an address is inserted into the binding table, an address resolution request sent to a multicast address is intercepted, and the device either responds on behalf of the address owner or, at layer 2, converts the request into a unicast message and forwards it to its destination.

To configure IPv6 ND suppress policy, perform this procedure:

SUMMARY STEPS

1. **enable**

2. **configure terminal**
3. **ipv6 nd suppress policy**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	ipv6 nd suppress policy Example: Device(config)# ipv6 nd suppress policy	Defines the ND suppress policy name and enters ND suppress policy configuration mode.

Configuring IPv6 Snooping on VLAN/PortChannel

Neighbor Discover (ND) suppress can be enabled or disabled on either the VLAN or a switchport.

To configure IPv6 snooping on VLAN/PortChannel, perform this procedure:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vlan config901**
4. **ipv6 nd suppress**
5. **end**
6. **interface gi1/0/1**
7. **ipv6 nd suppress**
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. Enter your password if prompted.

	Command or Action	Purpose
Step 2	configure terminal Example: Device# <code>configure terminal</code>	Enters global configuration mode.
Step 3	vlan config901 Example: Device(config)# <code>vlan config901</code>	Creates a VLAN and enter the VLAN configuration mode
Step 4	ipv6 nd suppress Example: Device(config-vlan)# <code>ipv6 nd suppress</code>	Applies the IPv6 nd suppress on VLAN.
Step 5	end Example: Device(config-vlan)# <code>end</code>	Exits vlan configuration mode and enters the global configuration mode.
Step 6	interface gi1/0/1 Example: Device(config)# <code>interface gi1/0/1</code>	Creates a gigabitethernet port interface.
Step 7	ipv6 nd suppress Example: Device(config-vlan)# <code>ipv6 nd suppress</code>	Applies the IPv6 nd suppress on the interface.
Step 8	end Example: Device(config-vlan)# <code>end</code>	Exits vlan configuration mode and enters the global configuration mode.

Configuring IPv6 on Interface

To configure IPv6 on an interface, perform this procedure:

Before you begin

Enable IPv6 on the client and IPv6 support on the wired infrastructure.

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `interface vlan 1`
4. `ip address fe80::1 link-local`

5. `ipv6 enable`
6. `end`

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> <code>enable</code>	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: Device# <code>configure terminal</code>	Enters global configuration mode.
Step 3	interface vlan 1 Example: Device(config)# <code>interface vlan 1</code>	Creates a interface and enters interface configuration mode.
Step 4	ip address fe80::1 link-local Example: Device(config-if)# <code>ip address 198.51.100.1 255.255.255.0</code> Device(config-if)# <code>ipv6 address fe80::1 link-local</code> Device(config-if)# <code>ipv6 address 2001:DB8:0:1:FFFF:1234::5/64</code> Device(config-if)# <code>ipv6 address 2001:DB8:0:0:E000::F/64</code>	Configures IPv6 address on the interface using the link-local option.
Step 5	ipv6 enable Example: Device(config)# <code>ipv6 enable</code>	(Optional) Enables IPv6 on the interface.
Step 6	end Example: Device(config)# <code>end</code>	Exits from the interface mode.

Configuring DHCP Pool

To configure DHCP Pool on an interface, perform this procedure:

SUMMARY STEPS

1. `enable`

2. **configure terminal**
3. **ipv6 dhcp pool Vlan21**
4. **address prefix 2001:DB8:0:1:FFFF:1234::/64 lifetime 300 10**
5. **dns-server 2001:100:0:1::1**
6. **domain-name example.com**
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	ipv6 dhcp pool Vlan21 Example: Device(config)# ipv6 dhcp pool vlan1	Enters the configuration mode and configures the IPv6 DHCP pool on the Vlan.
Step 4	address prefix 2001:DB8:0:1:FFFF:1234::/64 lifetime 300 10 Example: Device(config-dhcpv6)# address prefix 2001:DB8:0:1:FFFF:1234::/64 lifetime 300 10	Enters the configuration-dhcp mode and configures the address pool and its lifetime on a Vlan.
Step 5	dns-server 2001:100:0:1::1 Example: Device(config-dhcpv6)# dns-server 2001:20:21::1	Configures the DNS servers for the DHCP pool.
Step 6	domain-name example.com Example: Device(config-dhcpv6)# domain-name example.com	Configures the domain name to complete unqualified host names.
Step 7	end Example: Device(config)# end	Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.

Configuring Stateless Auto Address Configuration Without DHCP (CLI)

To configure stateless auto address configuration without DHCP, perform this procedure:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface vlan 1**
4. **ip address fe80::1 link-local**
5. **ipv6 enable**
6. **no ipv6 nd managed-config-flag**
7. **no ipv6 nd other-config-flag**
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	interface vlan 1 Example: Device(config)# interface vlan 1	Creates a interface and enters interface configuration mode.
Step 4	ip address fe80::1 link-local Example: Device(config-if)# ip address 198.51.100.1 255.255.255.0 Device(config-if)# ipv6 address fe80::1 link-local Device(config-if)# ipv6 address 2001:DB8:0:1:FFFF:1234::5/64 Device(config-if)# ipv6 address 2001:DB8:0:0:E000::F/64	Configures IPv6 address on the interface using the link-local option.
Step 5	ipv6 enable Example:	(Optional) Enables IPv6 on the interface.

	Command or Action	Purpose
	Device(config)# ipv6 enable	
Step 6	no ipv6 nd managed-config-flag Example: Device(config)# interface vlan 1 Device(config-if)# no ipv6 nd managed-config-flag	Ensures the attached hosts do not use stateful autoconfiguration to obtain addresses.
Step 7	no ipv6 nd other-config-flag Example: Device(config-if)# no ipv6 nd other-config-flag	Ensures the attached hosts do not use stateful autoconfiguration to obtain non-address options from DHCP (domain etc).
Step 8	end Example: Device(config)# end	Returns to privileged EXEC mode. Alternatively, you can also press Ctrl-Z to exit global configuration mode.

Configuring Stateless Auto Address Configuration With DHCP

To configure stateless auto address configuration with DHCP, perform this procedure:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface vlan 1**
4. **ip address fe80::1 link-local**
5. **ipv6 enable**
6. **no ipv6 nd managed-config-flag**
7. **ipv6 nd other-config-flag**
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
Step 3	interface vlan 1 Example: Device(config)# interface vlan 1	Creates a interface and enters interface configuration mode.
Step 4	ip address fe80::1 link-local Example: Device(config-if)# ip address 198.51.100.1 255.255.255.0 Device(config-if)# ipv6 address fe80::1 link-local Device(config-if)# ipv6 address 2001:DB8:0:1:FFFF:1234::5/64 Device(config-if)# ipv6 address 2001:DB8:0:0:E000::F/64	Configures IPv6 address on the interface using the link-local option.
Step 5	ipv6 enable Example: Device(config)# ipv6 enable	(Optional) Enables IPv6 on the interface.
Step 6	no ipv6 nd managed-config-flag Example: Device(config)# interface vlan 1 Device(config-if)# no ipv6 nd managed-config-flag	Ensures the attached hosts do not use stateful autoconfiguration to obtain addresses.
Step 7	ipv6 nd other-config-flag Example: Device(config-if)# no ipv6 nd other-config-flag	Ensures the attached hosts do not use stateful autoconfiguration to obtain non-address options from DHCP (domain etc).
Step 8	end Example: Device(config)# end	Exits from the interface mode.

Configuring Stateful DHCP Locally

This interface configuration is for a Cisco IOS IPv6 router implementing stateful DHCPv6 on a local Device

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 unicast-routing**
4. **ipv6 dhcp pool IPv6_DHCPOOL**
5. **address prefix 2001:DB8:0:1:FFFF:1234::/64**
6. **dns-server 2001:100:0:1::1**
7. **domain-name example.com**

8. `exit`
9. `interface vlan1`
10. `description IPv6-DHCP-Stateful`
11. `ipv6 address 2001:DB8:0:20::1/64`
12. `ip address 192.168.20.1 255.255.255.0`
13. `ipv6 nd prefix 2001:db8::/64 no-advertise`
14. `ipv6 nd managed-config-flag`
15. `ipv6 nd other-config-flag`
16. `ipv6 dhcp server IPv6_DHCPPPOOL`

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> <code>enable</code>	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: Device# <code>configure terminal</code>	Enters global configuration mode.
Step 3	ipv6 unicast-routing Example: Device(config)# <code>ipv6 unicast-routing</code>	Configures IPv6 for unicasting.
Step 4	ipv6 dhcp pool IPv6_DHCPPPOOL Example: Device (config)# <code>ipv6 dhcp pool IPv6_DHCPPPOOL</code>	Enters the configuration mode and configures the IPv6 DHCP pool on the VLAN.
Step 5	address prefix 2001:DB8:0:1:FFFF:1234::/64 Example: Device (config-dhcpv6)# <code>address prefix 2001:DB8:0:1:FFFF:1234::/64</code>	Specifies the address range to provide in the pool.
Step 6	dns-server 2001:100:0:1::1 Example: Device (config-dhcpv6)# <code>dns-server 2001:100:0:1::1</code>	Provides the DNS server option to DHCP clients.
Step 7	domain-name example.com Example: Device (config-dhcpv6)# <code>domain-name example.com</code>	Provides the domain name option to DHCP clients.

	Command or Action	Purpose
Step 8	exit Example: Device (config-dhcpv6)# exit	Returns to the previous mode.
Step 9	interface vlan1 Example: Device (config)# interface vlan 1	Enters the interface mode to configure the stateful DHCP.
Step 10	description IPv6-DHCP-Stateful Example: Device (config-if)# description IPv6-DHCP-Stateful	Enter description for the stateful IPv6 DHCP.
Step 11	ipv6 address 2001:DB8:0:20::1/64 Example: Device (config-if)# ipv6 address 2001:DB8:0:20::1/64	Enters the IPv6 address for the stateful IPv6 DHCP.
Step 12	ip address 192.168.20.1 255.255.255.0 Example: Device (config-if)# ip address 192.168.20.1 255.255.255.0	Enters the IPv6 address for the stateful IPv6 DHCP.
Step 13	ipv6 nd prefix 2001:db8::/64 no-advertise Example: Device (config-if)# ipv6 nd prefix 2001:db8::/64 no-advertise	Configures the IPv6 routing prefix advertisement that must not be advertised.
Step 14	ipv6 nd managed-config-flag Example: Device (config-if)# ipv6 nd managed-config-flag	Configures IPv6 interfaces neighbor discovery to allow the hosts to uses DHCP for address configuration.
Step 15	ipv6 nd other-config-flag Example: Device (config-if)# ipv6 nd other-config-flag	Configures IPv6 interfaces neighbor discovery to allow the hosts to uses DHCP for non-address configuration.
Step 16	ipv6 dhcp server IPv6_DHCPPPOOL Example: Device (config-if)# ipv6 dhcp server IPv6_DHCPPPOOL	Configures the DHCP server on the interface.

Configuring Stateful DHCP Externally

This interface configuration is for a Cisco IOS IPv6 router implementing stateful DHCPv6 on an external DHCP server.

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `ipv6 unicast-routing`
4. `dns-server 2001:100:0:1::1`
5. `domain-name example.com`
6. `exit`
7. `interface vlan1`
8. `description IPv6-DHCP-Stateful`
9. `ipv6 address 2001:DB8:0:20::1/64`
10. `ip address 192.168.20.1 255.255.255.0`
11. `ipv6 nd prefix 2001:db8::/64 no-advertise`
12. `ipv6 nd managed-config-flag`
13. `ipv6 nd other-config-flag`
14. `ipv6 dhcp relaydestination 2001:DB8:0:20::2`

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> <code>enable</code>	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	configure terminal Example: Device# <code>configure terminal</code>	Enters global configuration mode.
Step 3	ipv6 unicast-routing Example: Device(config)# <code>ipv6 unicast-routing</code>	Configures the IPv6 for unicasting.
Step 4	dns-server 2001:100:0:1::1 Example: Device(config-dhcpv6)# <code>dns-server 2001:100:0:1::1</code>	Provides the DNS server option to DHCP clients.
Step 5	domain-name example.com Example: Device(config-dhcpv6)# <code>domain-name example.com</code>	Provides the domain name option to DHCP clients.
Step 6	exit Example: Device(config-dhcpv6)# <code>exit</code>	Returns to the previous mode.

	Command or Action	Purpose
Step 7	interface vlan1 Example: Device(config)# interface vlan 1	Enters the interface mode to configure the stateful DHCP.
Step 8	description IPv6-DHCP-Stateful Example: Device(config-if)# description IPv6-DHCP-Stateful	Enter description for the stateful IPv6 DHCP.
Step 9	ipv6 address 2001:DB8:0:20::1/64 Example: Device(config-if)# ipv6 address 2001:DB8:0:20::1/64	Enters the IPv6 address for the stateful IPv6 DHCP.
Step 10	ip address 192.168.20.1 255.255.255.0 Example: Device(config-if)# ip address 192.168.20.1 255.255.255.0	Enters the IPv6 address for the stateful IPv6 DHCP.
Step 11	ipv6 nd prefix 2001:db8::/64 no-advertise Example: Device(config-if)# ipv6 nd prefix 2001:db8::/64 no-advertise	Configures the IPv6 routing prefix advertisement that must not be advertised.
Step 12	ipv6 nd managed-config-flag Example: Device(config-if)# ipv6 nd managed-config-flag	Configures IPv6 interfaces neighbor discovery to allow the hosts to uses DHCP for address configuration.
Step 13	ipv6 nd other-config-flag Example: Device(config-if)# ipv6 nd other-config-flag	Configures IPv6 interfaces neighbor discovery to allow the hosts to uses DHCP for non-address configuration.
Step 14	ipv6 dhcp relaydestination 2001:DB8:0:20::2 Example: Device(config-if)# ipv6 dhcp relay destination 2001:DB8:0:20::2	Configures the DHCP server on the interface.

Verifying IPv6 Address Learning Configuration

This example displays the output of the **show ipv6 dhcp pool** command. This command displays the IPv6 service configuration on the device. The vlan 21 configured pool detail displays 6 clients that are currently using addresses from the pool.

SUMMARY STEPS

1. `show ipv6 dhcp pool`

DETAILED STEPS

	Command or Action	Purpose
Step 1	show ipv6 dhcp pool Example: <pre> Deviceshow ipv6 dhcp pool DHCPv6 pool: vlan21 Address allocation prefix: 2001:DB8:0:1:FFFF:1234::/64 valid 86400 preferred 86400 (6 in use, 0 conflicts) DNS server: 2001:100:0:1::1 Domain name: example.com Active clients: 6 </pre>	Displays the IPv6 service configuration on the device.

Additional References

Related Documents

Related Topic	Document Title
IPv6 command reference	<i>IPv6 Command Reference (Catalyst 3650 Switches)</i>
IP command reference	<i>IP Command Reference (Catalyst 3650 Switches)</i>

Error Message Decoder

Description	Link
To help you research and resolve system error messages in this release, use the Error Message Decoder tool.	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIBs

MIB	MIBs Link
All the supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/support

Feature Information for IPv6 Client Address Learning

This table lists the features in this module and provides links to specific configuration information:

Feature	Release	Modification
IPv6 Client Address Learning Functionality	Cisco IOS XE 3.3SE Cisco IOS XE 3.3SE	This feature was introduced.