Configuring IPv6 Client IP Address Learning

Prerequisites for IPv6 Client Address Learning

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

Related Topics

Configuring RA Guard Policy (CLI), on page 8

Information About IPv6 Client Address Learning

Client Address Learning is configured on switch to learn the wireless client's IPv4 and IPv6 address and clients transition state maintained by the switch 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 switch 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:

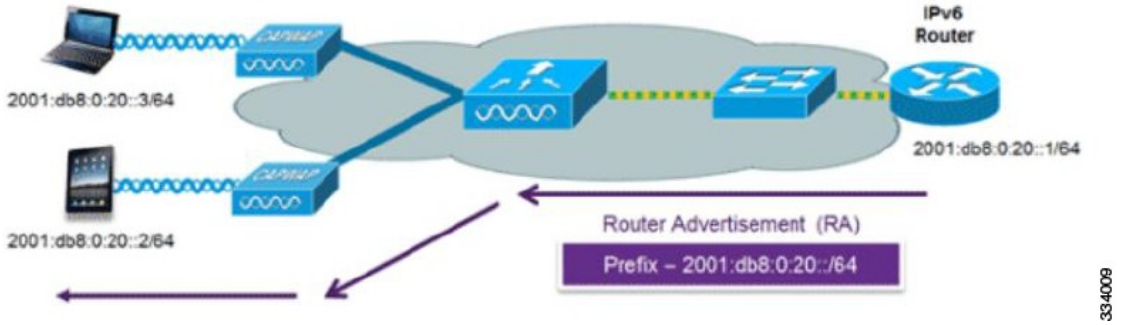
- Host sends a router solicitation message.
- Hosts waits for a Router Advertisement message.
- Hosts take the first 64 bits of the IPv6 prefix from the Router Advertisement message and combines it with the 64 bit EUI-64 address (in the case of ethernet, this is created from the MAC Address) to create 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:

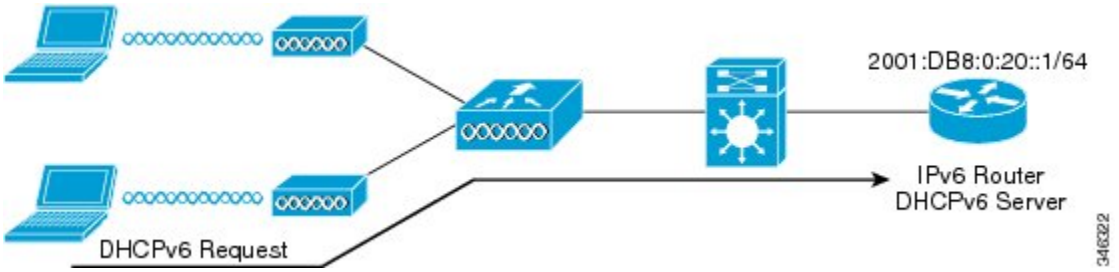
```
ipv6 unicast-routing
interface Vlan20
description IPv6-SLAAC
ip address 192.168.20.1 255.255.255.0
ipv6 address FE80:DB8:0:20::1 linklocal
ipv6 address 2001:DB8:0:20::1/64
ipv6 enable
end
```

Related Topics

Configuring IPv6 Snooping (CLI), on page 12
Configuring DHCP Pool (CLI), on page 16
Configuring Stateless Auto Address Configuration Without DHCP (CLI), on page 17
Configuring Stateless Auto Address Configuration With DHCP (CLI), on page 19
Configuring Stateful DHCP Locally (CLI), on page 20
Configuring Stateful DHCP Externally (CLI), on page 22

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_DHCPPOOL
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_DHCPPOOL
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 Switch:

```
ipv6 unicast-routing
ipv6 dhcp pool IPV6_DHCPPOOL
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_DHCPPOOL
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
```

Related Topics

Configuring IPv6 Snooping (CLI), on page 12
Configuring DHCP Pool (CLI), on page 16
Configuring Stateless Auto Address Configuration Without DHCP (CLI), on page 17
Configuring Stateless Auto Address Configuration With DHCP (CLI), on page 19
Configuring Stateful DHCP Locally (CLI), on page 20
Configuring Stateful DHCP Externally (CLI), on page 22

Static IP Address Assignment

Statically configured address on a client.

Router Solicitation

A Router Solicitation message is issued by a host controller 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.

Related Topics

Configuring IPv6 ND Suppress Policy (CLI), on page 13

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.

Related Topics

Configuring IPv6 ND Suppress Policy (CLI), on page 13

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.

Related Topics

Configuring IPv6 ND Suppress Policy (CLI), on page 13

Neighbor Discovery Suppression

The IPv6 addresses of wireless clients are cached by the switch. When the switch receives an NS multicast looking for an IPv6 address, and if the target address is known to the switch and belongs to one of its clients, the switch 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 switch acts like proxy and respond with NA, only when the **ipv6 nd suppress** command is configured

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

Related Topics

Configuring IPv6 ND Suppress Policy (CLI), on page 13

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 wireless clients. If this feature is not configured, malicious IPv6 wireless 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 switch. You can configure the switch to drop RA messages at the switch. All IPv6 RA messages are dropped, which protects other wireless clients and upstream wired network from malicious IPv6 clients.

```
//Create a policy for RA Guard//
ipv6 nd raguard policy raguard-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 raguard attach-policy raguard-router
```

Related Topics

Configuring RA Guard Policy (CLI), on page 8
Applying RA Guard Policy (CLI), on page 9
Configuring RA Throttle Policy (CLI), on page 10
Applying RA Throttle Policy on VLAN (CLI), on page 11

RA Throttling

RA throttling allows the controller to enforce limits to RA packets headed toward the wireless network. By enabling RA throttling, routers that send many RA packets can be trimmed to a minimum frequency that will still maintain an IPv6 client connectivity. If a client sends an RS packet, an RA is sent back to the client. This RA is allowed through the controller and unicasted to the client. This process ensures that the new clients or roaming clients are not affected by the RA throttling.

Related Topics

Configuring RA Guard Policy (CLI), on page 8
Applying RA Guard Policy (CLI), on page 9
Configuring RA Throttle Policy (CLI), on page 10
Applying RA Throttle Policy on VLAN (CLI), on page 11

Configuring IPv6 Unicast (CLI)

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

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. **configure terminal**
2. **ipv6 unicast routing**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.

	Command or Action	Purpose
Step 2	**ipv6 unicast routing** **Example:** `Switch (config)# ipv6 unicast routing`	enable the forwarding of IPv6 unicast datagrams

Configuring RA Guard Policy (CLI)

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

Before You Begin

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 2	**ipv6 nd raguard policy** raguard-router **Example:** `Switch(config)# ipv6 nd raguard policy raguard-router`	Defines the RA guard policy name and enters RA guard policy configuration mode.
Step 3	**trustedport** **Example:** `Switch(config-ra-guard)# trustedport`	(Optional) Specifies that this policy is being applied to trusted ports.
Step 4	**device-role router** **Example:** `Switch(config-ra-guard)# device-role router`	Specifies the role of the device attached to the port.

	Command or Action	Purpose
Step 5	**exit** **Example:** `Switch(config-ra-guard)# exit`	Exits RA guard policy configuration mode and returns to global configuration mode.

Related Topics

Prerequisites for IPv6 Client Address Learning, on page 1
RA Guard, on page 6
RA Throttling, on page 7
Applying RA Guard Policy (CLI), on page 9
Configuring RA Throttle Policy (CLI), on page 10
Applying RA Throttle Policy on VLAN (CLI), on page 11

Applying RA Guard Policy (CLI)

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

Before You Begin

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 2	**interface tengigabitethernet** 1/0/1 **Example:** `Switch (config)# interface tengigabitethernet 1/0/1`	Specifies an interface type and number, and places the device in interface configuration mode.

	Command or Action	Purpose
Step 3	**ipv6 nd raguard attach-policy** raguard-router **Example:** `Switch(config-if)# ipv6 nd raguard attach-policy raguard-router`	Applies the IPv6 RA Guard feature to a specified interface.
Step 4	**exit** **Example:** `Switch(config-if)# exit`	Exits interface configuration mode.

Related Topics

Configuring RA Guard Policy (CLI), on page 8
RA Guard, on page 6
RA Throttling, on page 7
Configuring RA Throttle Policy (CLI), on page 10
Applying RA Throttle Policy on VLAN (CLI), on page 11

Configuring RA Throttle Policy (CLI)

Configure RA Throttle policy to allow the enforce the limits

Before You Begin

SUMMARY STEPS

1. **configure terminal**
2. **ipv6 nd ra-throttler policy** ra-throttler1
3. **throttleperiod**500
4. **max-through**10
5. **allow-atleast** 5 **at-most** 10

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.

	Command or Action	Purpose
Step 2	**ipv6 nd ra-throttler policy** ra-throttler1 **Example:** `Switch(config)# ipv6 nd ra-throttler policy ra-throttler1`	Define the router advertisement (RA) throttler policy name and enter IPv6 RA throttle policy configuration mode.
Step 3	**throttleperiod**500 **Example:** `Switch(config-nd-ra-throttle)# throttleperiod 500`	Configures the throttle period in an IPv6 RA throttler policy.
Step 4	**max-through**10 **Example:** `Switch(config-nd-ra-throttle)# max-through 500`	Limits multicast RAs per VLAN per throttle period.
Step 5	**allow-atleast** 5 **at-most** 10 **Example:** `Switch(config-nd-ra-throttle)# allow-atleast 5 at-most 10`	Limits the number of multicast RAs per device per throttle period in an RA throttler policy.

Related Topics

Configuring RA Guard Policy (CLI), on page 8
Applying RA Guard Policy (CLI), on page 9
RA Guard, on page 6
RA Throttling, on page 7
Applying RA Throttle Policy on VLAN (CLI), on page 11

Applying RA Throttle Policy on VLAN (CLI)

Applying the RA Throttle policy on a VLAN. By enabling RA throttling, routers that send many RA packets can be trimmed to a minimum frequency that will still maintain an IPv6 client connectivity.

Before You Begin

SUMMARY STEPS

1. **configure terminal**
2. **vlan configuration** 1
3. **ipv6 nd ra throttler attach-policy** ra-throttler1

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 2	**vlan configuration** 1 **Example:** `Switch(config)# vlan configuration 1`	Configures a VLAN or a collection of VLANs and enters VLAN configuration mode.
Step 3	**ipv6 nd ra throttler attach-policy** ra-throttler1 **Example:** `Switch(config-vlan)# ipv6 nd ra throttler attach-policy ra-throttler1`	Attaches an IPv6 RA throttler policy to a VLAN or a collection of VLANs.

Related Topics

Configuring RA Guard Policy (CLI), on page 8
Applying RA Guard Policy (CLI), on page 9
Configuring RA Throttle Policy (CLI), on page 10
RA Guard, on page 6
RA Throttling, on page 7

Configuring IPv6 Snooping (CLI)

IPv6 snooping must always be enabled on the switch and the controller.

Before You Begin

Enable IPv6 on the client machine.

SUMMARY STEPS

1. **vlan configuration 1**
2. **ipv6 snooping**
3. **ipv6 nd suppress**
4. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**vlan configuration 1** **Example:** `Switch(config)# vlan configuration 1`	Enters Vlan configuration mode.
Step 2	**ipv6 snooping** **Example:** `Switch(config-vlan)# ipv6 snooping`	Enables IPv6 snooping on the Vlan.
Step 3	**ipv6 nd suppress** **Example:** `Switch(config-vlan-config)# ipv6 nd suppress`	Enables the IPv6 ND suppress on the Vlan.
Step 4	**exit** **Example:** `Switch(config-vlan-config)# exit`	Saves the configuration and comes out of the Vlan configuration mode.

Related Topics

SLAAC Address Assignment, on page 2
Stateful DHCPv6 Address Assignment, on page 3

Configuring IPv6 ND Suppress Policy (CLI)

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 or a wireless controller 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.

Before You Begin

SUMMARY STEPS

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

DETAILED STEPS

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

Related Topics

Router Solicitation, on page 5
Router Advertisement, on page 5
Neighbor Discovery, on page 5
Neighbor Discovery Suppression, on page 5

Configuring IPv6 Snooping on VLAN/PortChannel

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

Before You Begin

SUMMARY STEPS

1. **vlan config901**
2. **ipv6 nd suppress**
3. **end**
4. **interface gi1/0/1**
5. **ipv6 nd suppress**
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**vlan config901** **Example:** `Switch(config)# vlan config901`	Creates a VLAN and enter the VLAN configuration mode
Step 2	**ipv6 nd suppress** **Example:** `Switch(config-vlan)# ipv6 nd suppress`	Applies the IPv6 nd suppress on VLAN.
Step 3	**end** **Example:** `Switch(config-vlan)# end`	Exits vlan configuration mode and enters the global configuration mode.
Step 4	**interface gi1/0/1** **Example:** `Switch (config)# interface gi1/0/1`	Creates a gigabitethernet port interface.
Step 5	**ipv6 nd suppress** **Example:** `Switch(config-vlan)# ipv6 nd suppress`	Applies the IPv6 nd suppress on the interface.
Step 6	**end** **Example:** `Switch(config-vlan)# end`	Exits vlan configuration mode and enters the global configuration mode.

Configuring IPv6 on Switch (CLI)

Use this configuration example to configure IPv6 on an interface.

Before You Begin

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

SUMMARY STEPS

1. **interface vlan** 1
2. **ip address** fe80::1 link-local
3. **ipv6 enable**
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**interface vlan** 1 **Example:** `Switch(config)# interface vlan 1`	Creates a interface and enters interface configuration mode.

Step 2	**ip address** fe80::1 link-local
	
	Example:
	`Switch(config-if)# ip address 198.51.100.1 255.255.255.0`
	
	`Switch(config-if)# ipv6 address fe80::1 link-local`
	`Switch(config-if)# ipv6 address 2001:DB8:0:1:FFFF:1234::5/64`
	`Switch(config-if)# ipv6 address 2001:DB8:0:0:E000::F/64`
		Configures IPv6 address on the interface using the link-local option.

Step 3	**ipv6 enable** **Example:** `Switch(config)# ipv6 enable`	(Optional) Enables IPv6 on the interface.
Step 4	**end** **Example:** `Switch(config)# end`	Exits from the interface mode.

Configuring DHCP Pool (CLI)

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**ipv6 dhcp pool** Vlan21 **Example:** `Switch(config)# ipv6 dhcp pool vlan1`	Enters the configuration mode and configures the IPv6 DHCP pool on the Vlan.

	Command or Action	Purpose
Step 2	**address prefix** 2001:DB8:0:1:FFFF:1234::/64 **lifetime** 300 10 **Example:** `Switch(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 3	**dns-server** 2001:100:0:1::1 **Example:** `Switch(config-dhcpv6)# dns-server 2001:20:21::1`	Configures the DNS servers for the DHCP pool.
Step 4	**domain-name** example.com **Example:** `Switch(config-dhcpv6)# domain-name example.com`	Configures the domain name to complete unqualified host names.
Step 5	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Related Topics

SLAAC Address Assignment, on page 2
Stateful DHCPv6 Address Assignment, on page 3

Configuring Stateless Auto Address Configuration Without DHCP (CLI)

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**interface vlan** 1 **Example:** `Switch(config)# interface vlan 1`	Creates a interface and enters interface configuration mode.

Step 2	**ip address** fe80::1 link-local
	
	Example:
	`Switch(config-if)# ip address 198.51.100.1 255.255.255.0`
	`Switch(config-if)# ipv6 address fe80::1 link-local`
	`Switch(config-if)# ipv6 address 2001:DB8:0:1:FFFF:1234::5/64`
	`Switch(config-if)# ipv6 address 2001:DB8:0:0:E000::F/64`
		Configures IPv6 address on the interface using the link-local option.

Step 3	**ipv6 enable** **Example:** `Switch(config)# ipv6 enable`	(Optional) Enables IPv6 on the interface.

Step 4	**no ipv6 nd managed-config-flag**
	
	Example:
	`Switch(config)#interface vlan 1`
	`Switch(config-if)# no ipv6 nd managed-config-flag`
		Ensures the attached hosts do not use stateful autoconfiguration to obtain addresses.

Step 5	**no ipv6 nd other-config-flag** **Example:** `Switch(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 6	**end** **Example:** `Switch(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Related Topics

SLAAC Address Assignment, on page 2
Stateful DHCPv6 Address Assignment, on page 3

Configuring Stateless Auto Address Configuration With DHCP (CLI)

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**interface vlan** 1 **Example:** `Switch(config)# interface vlan 1`	Creates a interface and enters interface configuration mode.

Step 2	**ip address** fe80::1 link-local
	
	Example:
	`Switch(config-if)# ip address 198.51.100.1 255.255.255.0`
	`Switch(config-if)# ipv6 address fe80::1 link-local`
	
	`Switch(config-if)# ipv6 address 2001:DB8:0:1:FFFF:1234::5/64`
	`Switch(config-if)# ipv6 address 2001:DB8:0:0:E000::F/64`
		Configures IPv6 address on the interface using the link-local option.

Step 3	**ipv6 enable** **Example:** `Switch(config)# ipv6 enable`	(Optional) Enables IPv6 on the interface.

Step 4	**no ipv6 nd managed-config-flag**
	
	Example:
	`Switch(config)#interface vlan 1`
	`Switch(config-if)# no ipv6 nd managed-config-flag`
		Ensures the attached hosts do not use stateful autoconfiguration to obtain addresses.

Step 5	**ipv6 nd other-config-flag** **Example:** `Switch(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).

	Command or Action	Purpose
Step 6	**end** **Example:** `Switch(config)# end`	Exits from the interface mode.

Related Topics

SLAAC Address Assignment, on page 2
Stateful DHCPv6 Address Assignment, on page 3

Configuring Stateful DHCP Locally (CLI)

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

Before You Begin

SUMMARY STEPS

1. **configure terminal**
2. **ipv6 unicast-routing**
3. **ipv6 dhcp pool** IPv6_DHCPPOOL
4. **address prefix** 2001:DB8:0:1:FFFF:1234::/64
5. **dns-server** 2001:100:0:1::1
6. **domain-name** example.com
7. **exit**
8. **interface** vlan1
9. **description IPv6-DHCP-Stateful**
10. **ipv6 address** 2001:DB8:0:20::1/64
11. **ip address** 192.168.20.1 255.255.255.0
12. **ipv6 nd prefix** 2001:db8::/64 **no-advertise**
13. **ipv6 nd managed-config-flag**
14. **ipv6 nd other-config-flag**
15. **ipv6 dhcp server** IPv6_DHCPPOOL

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 2	**ipv6 unicast-routing** **Example:** `Switch(config)# ipv6 unicast-routing`	Configures IPv6 for unicasting.
Step 3	**ipv6 dhcp pool** IPv6_DHCPPOOL **Example:** `Switch (config)# ipv6 dhcp pool IPv6_DHCPPOOL`	Enters the configuration mode and configures the IPv6 DHCP pool on the VLAN.
Step 4	**address prefix** 2001:DB8:0:1:FFFF:1234::/64 **Example:** `Switch (config-dhcpv6)# address prefix 2001:DB8:0:1:FFFF:1234::/64`	Specifies the address range to provide in the pool.
Step 5	**dns-server** 2001:100:0:1::1 **Example:** `Switch (config-dhcpv6)# dns-server 2001:100:0:1::1`	Provides the DNS server option to DHCP clients.
Step 6	**domain-name** example.com **Example:** `Switch (config-dhcpv6)# domain-name example.com`	Provides the domain name option to DHCP clients.
Step 7	**exit** **Example:** `Switch (config-dhcpv6)# exit`	Returns to the previous mode.
Step 8	**interface** vlan1 **Example:** `Switch (config)# interface vlan 1`	Enters the interface mode to configure the stateful DHCP.
Step 9	**description IPv6-DHCP-Stateful** **Example:** `Switch (config-if)# description IPv6-DHCP-Stateful`	Enter description for the stateful IPv6 DHCP.
Step 10	**ipv6 address** 2001:DB8:0:20::1/64 **Example:** `Switch (config-if)# ipv6 address 2001:DB8:0:20::1/64`	Enters the IPv6 address for the stateful IPv6 DHCP.

	Command or Action	Purpose
Step 11	**ip address** 192.168.20.1 255.255.255.0 **Example:** `Switch (config-if)# ip address 192.168.20.1 255.255.255.0`	Enters the IPv6 address for the stateful IPv6 DHCP.
Step 12	**ipv6 nd prefix** 2001:db8::/64 **no-advertise** **Example:** `Switch (config-if)# ipv6 nd prefix 2001:db8::/64 no-advertise`	Configures the IPv6 routing prefix advertisement that must not be advertised.
Step 13	**ipv6 nd managed-config-flag** **Example:** `Switch (config-if)# ipv6 nd managed-config-flag`	Configures IPv6 interfaces neighbor discovery to allow the hosts to uses DHCP for address configuration.
Step 14	**ipv6 nd other-config-flag** **Example:** `Switch (config-if)# ipv6 nd other-config-flag`	Configures IPv6 interfaces neighbor discovery to allow the hosts to uses DHCP for non-address configuration.
Step 15	**ipv6 dhcp server** IPv6_DHCPPOOL **Example:** `Switch (config-if)# ipv6 dhcp server IPv6_DHCPPOOL`	Configures the DHCP server on the interface.

Related Topics

SLAAC Address Assignment, on page 2
Stateful DHCPv6 Address Assignment, on page 3

Configuring Stateful DHCP Externally (CLI)

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

Before You Begin

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Switch# configure terminal`	Enters the global configuration mode.
Step 2	**ipv6 unicast-routing** **Example:** `Switch(config)# ipv6 unicast-routing`	Configures the IPv6 for unicasting.
Step 3	**dns-server** 2001:100:0:1::1 **Example:** `Switch (config-dhcpv6)# dns-server 2001:100:0:1::1`	Provides the DNS server option to DHCP clients.
Step 4	**domain-name** example.com **Example:** `Switch (config-dhcpv6)# domain-name example.com`	Provides the domain name option to DHCP clients.
Step 5	**exit** **Example:** `Switch (config-dhcpv6)# exit`	Returns to the previous mode.

	Command or Action	Purpose
Step 6	**interface** vlan1 **Example:** `Switch (config)# interface vlan 1`	Enters the interface mode to configure the stateful DHCP.
Step 7	**description IPv6-DHCP-Stateful** **Example:** `Switch (config-if)# description IPv6-DHCP-Stateful`	Enter description for the stateful IPv6 DHCP.
Step 8	**ipv6 address** 2001:DB8:0:20::1/64 **Example:** `Switch (config-if)# ipv6 address 2001:DB8:0:20::1/64`	Enters the IPv6 address for the stateful IPv6 DHCP.
Step 9	**ip address** 192.168.20.1 255.255.255.0 **Example:** `Switch (config-if)# ip address 192.168.20.1 255.255.255.0`	Enters the IPv6 address for the stateful IPv6 DHCP.
Step 10	**ipv6 nd prefix** 2001:db8::/64 **no-advertise** **Example:** `Switch (config-if)# ipv6 nd prefix 2001:db8::/64 no-advertise`	Configures the IPv6 routing prefix advertisement that must not be advertised.
Step 11	**ipv6 nd managed-config-flag** **Example:** `Switch (config-if)# ipv6 nd managed-config-flag`	Configures IPv6 interfaces neighbor discovery to allow the hosts to uses DHCP for address configuration.
Step 12	**ipv6 nd other-config-flag** **Example:** `Switch (config-if)# ipv6 nd other-config-flag`	Configures IPv6 interfaces neighbor discovery to allow the hosts to uses DHCP for non-address configuration.
Step 13	**ipv6 dhcp_relaydestination** 2001:DB8:0:20::2 **Example:** `Switch (config-if)# ipv6 dhcp_relay destination 2001:DB8:0:20::2`	Configures the DHCP server on the interface.

Related Topics

SLAAC Address Assignment, on page 2
Stateful DHCPv6 Address Assignment, on page 3

Monitoring IPv6 Clients (GUI)

To view the IPv6 clients associated with the Switch

Before You Begin

Select **Monitor** > **Clients**
The Clients page is displayed. The Clients page contains the following details:

- Client MAC Address— Displays the MAC address of the client.
- AP Name— Displays the access point name to which the client is connected to.
- WLAN— Displays the WLAN associated with the client.
- State— Displays the client authentication.
- Protocol— Displays the protocol used.

To view the client related general details, click the **Client MAC Address** parameter in the Clients page. The **Client > Detail** page displays IPv6 addresses of the client under the **General** tab.

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 switch. 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:
	`Switchshow 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`
		Displays the IPv6 service configuration on the switch.

Additional References

Related Documents

Related Topic	Document Title
IPv6 command reference	*IPv6 Command Reference (Catalyst 3850 Switches)*
IP command reference	*IP Command Reference (Catalyst 3850 Switches)*

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 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
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. 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. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	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 3.2SE	This feature was introduced.