IP Addressing: DHCP Configuration Guide, Cisco IOS Release 15E

First Published: August 26, 2013

Last Modified: August 26, 2013

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

CONTENTS

CHAPTER 1

DHCP Gleaning

This document describes the Dynamic Host Configuration Protocol Gleaning feature.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for DHCP Gleaning

- Ensure that the interface to be configured is a Layer 2 interface.
- Ensure that global snooping is enabled.

Information About DHCP Gleaning

Overview of DHCP Gleaning

Gleaning helps extract location information from Dynamic Host Configuration Protocol (DHCP) messages when messages are forwarded by a DHCP relay agent; the process is a completely passive snooping functionality that neither blocks nor modifies DHCP packets. Additionally, gleaning helps to differentiate an untrusted device port that is connected to an end user from a trusted port connected to a DHCP server.

DHCP gleaning is a read–only DHCP snooping functionality that allows components to register and glean only DHCP version 4 packets. When you enable DHCP gleaning, it does a read-only snooping on all active interfaces on which DHCP snooping is disabled. You can add a secondary VLAN to a private VLAN. When add a secondary VLAN to a private VLAN, ensure that gleaning is enabled on the secondary VLAN, even though snooping is disabled on the primary VLAN. By default, the gleaning functionality is disabled. However, when you enable a device sensor, DHCP gleaning is automatically enabled.

DHCP Snooping

Dynamic Host Configuring Protocol (DHCP) snooping is a security feature that acts like a firewall between untrusted hosts and trusted DHCP servers. The DHCP snooping feature performs the following activities:

- Validates DHCP messages received from untrusted sources and filters out invalid messages.
- Rate-limits DHCP traffic from trusted and untrusted sources.
- Builds and maintains the DHCP snooping binding database, which contains information about untrusted hosts with leased IP addresses.
- Utilizes the DHCP snooping binding database to validate subsequent requests from untrusted hosts.

Other security features, such as dynamic Address Resolution Protocol (ARP) inspection (DAI), also uses information stored in the DHCP snooping binding database.

DHCP snooping is enabled on a per-VLAN basis. By default, the feature is inactive on all VLANs. You can enable the feature on a single VLAN or on a range of VLANs.

How to Configure DHCP Gleaning

Configuring an Interface as a Trusted or an Untrusted Source for DHCP Gleaning

You can enable or disable DHCP gleaning on a device. You can configure an interface as a trusted or untrusted source of DHCP messages. Verify that no DHCP packets are dropped when DHCP gleaning is enabled on an untrusted interface or on a device port.

Note By default, DHCP gleaning is disabled.

You can configure DHCP trust on the following types of interfaces:

- Layer 2 Ethernet interfaces
- Layer 2 port-channel interfaces

Note By default, all interfaces are untrusted.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip dhcp snooping glean**
4. **interface** *type number*
5. [**no**] **ip dhcp snooping trust**
6. **end**
7. **show ip dhcp snooping statistics**
8. **show ip dhcp snooping**

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	**ip dhcp snooping glean** **Example:** `Device(config)# ip dhcp snooping glean`	Enables DHCP gleaning on an interface.

Step 4	**interface** *type number*
	Example:
	`Device(config)# interface gigabitEthernet 1/0/1`
	`Device(config-if)#`
		Enters interface configuration mode, where *type number* is the Layer 2 Ethernet interface which you want to configure as trusted or untrusted for DHCP snooping.

	Command or Action	Purpose
Step 5	[**no**] **ip dhcp snooping trust** **Example:** `Device(config-if)# ip dhcp snooping trust`	Configures the interface as a trusted interface for DHCP snooping. The **no** option configures the port as an untrusted interface.

Step 6	**end**
	Example:
	`Device(config-if)# end`
		Exits interface configuration mode and returns to privileged EXEC mode.

Step 7	**show ip dhcp snooping statistics** **Example:** `Device# show ip dhcp snooping statistics`	Displays packets that were dropped on the device port configured as an untrusted interface.
Step 8	**show ip dhcp snooping** **Example:** `Device# show ip dhcp snooping`	Displays DHCP snooping configuration information, including information about DHCP gleaning.

Configuration Examples for DHCP Gleaning

Example: Configuring an Interface as a Trusted or an Untrusted Source for DHCP Gleaning

This example shows how to enable Dynamic Host Configuration Protocol (DHCP) gleaning and configure an interface as a trusted interface:

```
configure terminal
 ip dhcp snooping glean
 interface gigabitEthernet 1/0/1
  ip dhcp snooping trust
  exit
```

Additional References

Related Documents

Related Topic	Document Title
Master Commands List	Cisco IOS Master Commands List

Related Topic	Document Title
DHCP Commands	Cisco IOS IP Addressing Services Command Reference
IP Source Guard	IP Source Guard
Dynamic ARP Inspection	Configuring Dynamic ARP Inspection

Standards and RFCs

Standard/RFC	Title
RFC-2131	Dynamic Host Configuration Protocol
RFC-4388	DHCP Leasequery

MIBs

MIB	MIBs Link
	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 DHCP Gleaning

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for DHCP Gleaning

Feature Name	Releases	Feature Information
DHCP Gleaning	Cisco IOS 15.2(1)E Cisco IOS 15.2(2)E	This document describes the DHCP Gleaning feature. In Cisco IOS Release 15.2(2)E, this feature is supported on the following platforms: • Cisco Catalyst 3750-E Series Switches • Cisco Catalyst 2960-S Series Switches The following commands were introduced or modified for this feature:**ip dhcp snooping glean**, **show ip dhcp snooping**

CHAPTER 2

DHCP—DHCPv6 Guard

This module describes the Dynamic Host Configuration Protocol version 6 (DHCPv6) Guard feature. This feature blocks DHCP reply and advertisement messages that originate from unauthorized DHCP servers and relay agents that forward DHCP packets from servers to clients. Client messages or messages sent by relay agents from clients to servers are not blocked. The filtering decision is determined by the device role assigned to the receiving switch port, trunk, or VLAN. In addition, to provide a finer level of filter granularity, messages can be filtered based on the address of the sending server or relay agent, or by the prefixes and addresses ranges listed in the reply message. This functionality helps to prevent traffic redirection or denial of service (DoS).

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for DHCPv6 Guard

- The DHCPv6 guard feature is not supported on Etherchannel ports.

Information About DHCPv6 Guard

DHCPv6 Guard Overview

The DHCPv6 Guard feature blocks reply and advertisement messages that come from unauthorized DHCP servers and relay agents.

Packets are classified into one of the three DHCP type messages. All client messages are always switched regardless of device role. DHCP server messages are only processed further if the device role is set to server. Further processing of server messages includes DHCP server advertisements (for source validation and server preference) and DHCP server replies (for permitted prefixes).

If the device is configured as a DHCP server, all the messages need to be switched, regardless of the device role configuration.

How to Configure DHCPv6 Guard

Configuring DHCP—DHCPv6 Guard

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 access-list** *access-list-name*
4. **permit host** *address* **any**
5. **exit**
6. **ipv6 prefix-list** *list-name* **permit** *ipv6-prefix* **128**
7. **ipv6 dhcp guard policy** *policy-name*
8. **device-role** {**client** | **server**}
9. **match server access-list** *ipv6-access-list-name*
10. **match reply prefix-list** *ipv6-prefix-list-name*
11. **preference min** *limit*
12. **preference max** *limit*
13. **trusted-port**
14. **exit**
15. **interface** *type number*
16. **switchport**
17. **ipv6 dhcp guard** [**attach-policy** *policy-name*] [**vlan** {**add** | **all** | **all** | **except** | **none** | **remove**} *vlan-id*][... *vlan-id*]]
18. **exit**
19. **vlan** *vlan-id*
20. **ipv6 dhcp guard** [**attach-policy** *policy-name*]
21. **exit**
22. **exit**
23. **show ipv6 dhcp guard policy** [*policy-name*]

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# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 access-list** *access-list-name* **Example:** `Device(config)# ipv6 access-list acl1`	Defines the IPv6 access list and enters IPv6 access list configuration mode.
Step 4	**permit host** *address* **any** **Example:** `Device(config-ipv6-acl)# permit host FE80::A8BB:CCFF:FE01:F700 any`	Sets the conditions in the named IP access list.
Step 5	**exit** **Example:** `Device(config-ipv6-acl)# exit`	Exits IPv6 access list configuration mode and returns to global configuration mode.
Step 6	**ipv6 prefix-list** *list-name* **permit** *ipv6-prefix* **128** **Example:** `Device(config)# ipv6 prefix-list abc permit 2001:0DB8::/64 le 128`	Creates an entry in an IPv6 prefix list.
Step 7	**ipv6 dhcp guard policy** *policy-name* **Example:** `Device(config)# ipv6 dhcp guard policy pol1`	Defines the DHCPv6 guard policy name and enters DHCP guard configuration mode.

Step 8	**device-role** {**client** | **server**}
	Example:
	`Device(config-dhcp-guard)# device-role server`
		Specifies the device role of the device attached to the target (interface or VLAN).

Step 9	**match server access-list** *ipv6-access-list-name* **Example:** `Device(config-dhcp-guard)# match server access-list acl1`	(Optional) Enables verification of the advertised DHCP server and relay address in inspected messages from the configured authorized server access list. If not configured, this check will be bypassed. An empty access list is treated as a permit.

	Command or Action	Purpose
Step 10	**match reply prefix-list** *ipv6-prefix-list-name* **Example:** `Device(config-dhcp-guard)# match reply prefix-list abc`	(Optional) Enables verification of the advertised prefixes in DHCP reply messages from the configured authorized prefix list. If not configured, this check will be bypassed. An empty prefix list is treated as a permit.
Step 11	**preference min** *limit* **Example:** `Device(config-dhcp-guard)# preference min 0`	(Optional) Enables verification that the advertised preference (in preference option) is greater than the specified limit. If not specified, this check will be bypassed.
Step 12	**preference max** *limit* **Example:** `Device(config-dhcp-guard)# preference max 255`	(Optional) Enables verification that the advertised preference (in preference option) is less than the specified limit. If not specified, this check will be bypassed.
Step 13	**trusted-port** **Example:** `Device(config-dhcp-guard)# trusted-port`	(Optional) Specifies that this policy is being applied to trusted ports. All DHCP guard policing will be disabled.
Step 14	**exit** **Example:** `Device(config-dhcp-guard)# exit`	Exits DHCP guard configuration mode and returns to global configuration mode.
Step 15	**interface** *type number* **Example:** `Device(config)# interface GigabitEthernet 0/2/0`	Specifies an interface and enters interface configuration mode.
Step 16	**switchport** **Example:** `Device(config-if)# switchport`	Puts an interface that is in Layer 3 mode into Layer 2 mode for Layer 2 configuration.
Step 17	**ipv6 dhcp guard** [**attach-policy** *policy-name*] [**vlan** {**add** | **all** | **all** | **except** | **none** | **remove**} *vlan-id*][... *vlan-id*]] **Example:** `Device(config-if)# ipv6 dhcp guard attach-policy pol1 vlan add vlan1`	Attaches a DHCPv6 guard policy to an interface. The **attach-policy** and **vlan** keywords are optional in the interface command. If no VLAN number is specified, traffic from all VLANs on the port will be checked.

	Command or Action	Purpose
Step 18	**exit** **Example:** `Device(config-if)# exit`	Exits interface configuration mode and returns to global configuration mode.
Step 19	**vlan** *vlan-id* **Example:** `Device(config)# vlan 1`	Specifies a VLAN and enters VLAN configuration mode.
Step 20	**ipv6 dhcp guard** [**attach-policy** *policy-name*] **Example:** `Device(config-vlan)# ipv6 dhcp guard attach-policy pol1`	Attaches a DHCPv6 guard policy to a VLAN.
Step 21	**exit** **Example:** `Device(config-vlan)# exit`	Exits interface configuration mode and returns to global configuration mode.
Step 22	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.
Step 23	**show ipv6 dhcp guard policy** [*policy-name*] **Example:** `Device# show ipv6 dhcp policy guard pol1`	(Optional) Displays the policy configuration as well as all the interfaces where the policy is applied.

Configuration Examples for DHCPv6 Guard

Example: Configuring DHCP—DHCPv6 Guard

The following example displays a sample configuration for DHCPv6 Guard:

```
enable
configure terminal
ipv6 access-list acl1
 permit host FE80::A8BB:CCFF:FE01:F700 any
```

```
ipv6 prefix-list abc permit 2001:0DB8::/64 le 128
ipv6 dhcp guard policy pol1
 device-role server
 match server access-list acl1
 match reply prefix-list abc
 preference min 0
 preference max 255
 trusted-port
interface GigabitEthernet 0/2/0
 switchport
 ipv6 dhcp guard attach-policy pol1 vlan add 1
 vlan 1
  ipv6 dhcp guard attach-policy pol1
show ipv6 dhcp guard policy pol1
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
DHCP commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*Cisco IOS IP Addressing Services Command Reference*
DHCP conceptual and configuration information	*Cisco IOS IP Addressing Services Configuration Guide*

Standards/RFCs

Standard	Title
No new or modified standards/RFCs are supported by this feature.	—

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature.	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 and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for DHCP—DHCPv6 Guard

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 2: Feature Information for DHCP—DHCPv6 Guard

Feature Name	Releases	Feature Information
DHCP—DHCPv6 Guard	15.2(1)E	The DHCP—DHCPv6 Guard feature blocks DHCP reply and advertisement messages that originate from unauthorized DHCP servers and relay agents that forward DHCP packets from servers to clients. Client messages or messages sent by relay agents from clients to servers are not blocked. The following commands were introduced or modified: **device-role** , **ipv6 dhcp guard attach-policy (DHCPv6 Guard)**, **ipv6 dhcp guard policy**, **match reply prefix-list**, **match server access-list**, **preference (DHCPv6 Guard)**, **show ipv6 dhcp guard policy**, **trusted-port (DHCPv6 Guard)**.

CHAPTER 3

IPv6 Access Services: DHCPv6 Relay Agent

A Dynamic Host Configuration Protocol for IPv6 (DHCPv6) relay agent, which may reside on the client's link, is used to relay messages between the client and the server.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About IPv6 Access Services: DHCPv6 Relay Agent

DHCPv6 Relay Agent

A DHCPv6 relay agent, which may reside on the client’s link, is used to relay messages between the client and the server. The DHCPv6 relay agent operation is transparent to the client. A DHCPv6 client locates a DHCPv6 server using a reserved, link-scoped multicast address. For direct communication between the DHCPv6 client and the DHCPv6 server, both of them must be attached to the same link. However, in some situations where ease of management, economy, or scalability is a concern, it is desirable to allow a DHCPv6 client to send a message to a DHCPv6 server that is not connected to the same link.

DHCPv6 Relay Agent Notification for Prefix Delegation

The DHCPv6 relay agent notification for prefix delegation allows the device working as a DHCPv6 relay agent to find prefix delegation options by reviewing the contents of a DHCPv6 RELAY-REPLY packet that is relayed by the relay agent to the client. When a prefix delegation option is found by the relay agent, the relay agent extracts the information about the prefix that is being delegated and inserts an IPv6 static route matching the prefix delegation information onto the relay agent. Future packets destined to that prefix via relay will be forwarded based on the information contained in the prefix delegation. The IPv6 static route is then left in the routing table until the prefix delegation lease time expires or the relay agent receives a release packet from the client releasing the prefix delegation.

No user configuration is required for this feature. Static route management is done automatically by the relay agent.

IPv6 routes are added when the relay agent relays a RELAY-REPLY packet, and IPv6 routes are deleted when the prefix delegation lease time expires or the relay agent receives a release message. An IPv6 static route in the routing table of the relay agent can be updated when the prefix delegation lease time is extended.

The DHCP—DHCPv6 Relay Agent Notification for Prefix Delegation feature leaves a static IPv6 route on the routing table of the relay agent. The registered IPv6 address allows unicast reverse packet forwarding (uRPF) to work by allowing the device doing the reverse lookup to confirm that the IPv6 address on the relay agent is not malformed or spoofed. The static route that remains in the routing table of the relay agent can be redistributed to other routing protocols to advertise the subnets to other nodes. Static routes will be removed when a DHCP_DECLINE message is sent by the client.

DHCPv6 Relay Options: Remote-ID for Gigabit Ethernet and Fast Ethernet Interfaces

The DHCPv6 Ethernet Remote ID Option feature adds the remote identification (remote-ID) option to relayed (RELAY-FORWARD) DHCPv6 packets.

The remote-ID option provides information to the DHCPv6 server, which includes port information, the system's DUID, and the VLAN ID. This information can be used to uniquely identify both the relay and the port on the relay through which the client packet arrived. The DHCPv6 server uses this information to select parameters specific to a particular user, host, or subscriber modem.

The addition of the remote-ID option to the RELAY-FORWARD packet occurs automatically and no user configuration is necessary.

The DHCPv6 server does not need to echo the remote-ID option in the RELAY-REPLY packet. The Internet Assigned Numbers Authority (IANA) has assigned the DHCPv6 option code 37 for the relay agent remote-ID option.

If the remote-ID option is included in the RELAY-REPLY packet, the option is removed from the packet before it is relayed to the client.

DHCPv6 Relay Options: Reload Persistent Interface ID

The DHCPv6 Relay—Reload Persistent Interface ID Option feature makes the interface ID option persistent. The interface ID is used by relay agents to decide which interface should be used to forward a RELAY-REPLY packet. A persistent interface-ID option will not change if the device acting as a relay agent goes offline during a reload or a power outage. When the device acting as a relay agent returns online, it is possible that changes to the internal interface index of the relay agent may have occurred in certain scenarios (such as, when the relay agent reboots and the number of interfaces in the interface index changes, or when the relay agents boot up and has more virtual interfaces than it did before the reboot). This feature prevents such scenarios from causing any problems.

This feature changes the DHCPv6 interface-ID option to be expressed as the short form of the interface name. The interface name as the DHCPv6 interface ID helps avoid potential problems that could arise due to physical or logical interfaces changing on the relay agent after a reload.

DHCPv6 Relay Chaining

DHCPv6 messages can be relayed through multiple relay agents. This configuration is called *relay chaining*. A relay chaining configuration can be supported only when each relay agent adds information to DHCPv6 messages before relaying them. The information helps in relaying the DHCPv6 reply back to the DHCPv6 client through the same path.

The delegated IPv6 prefix must be routable in order to be useful. The actual DHCPv6 Prefix Delegation (PD) client may not be permitted to inject routes into the delegating network. In service provider (SP) networks, for example, an edge device typically acts as a DHCPv6 relay agent, and this edge device often has the responsibility to maintain routes within the SP network for clients' PD bindings. In the event that DHCPv6 requests and responses are relayed through a chain of DHCPv6 relays, there may be a need to introduce appropriate routes (particularly with DHCPv6 PD) in the Forwarding Information Base (FIB) so that routing is handled transparently.

DHCPv6 Relay Agent Notification for Prefix Delegation

The DHCPv6 relay agent notification for prefix delegation allows the device working as a DHCPv6 relay agent to find prefix delegation options by reviewing the contents of a DHCPv6 RELAY-REPLY packet that is relayed by the relay agent to the client. When a prefix delegation option is found by the relay agent, the relay agent extracts the information about the prefix that is being delegated and inserts an IPv6 static route matching the prefix delegation information onto the relay agent. Future packets destined to that prefix via relay will be forwarded based on the information contained in the prefix delegation. The IPv6 static route is then left in the routing table until the prefix delegation lease time expires or the relay agent receives a release packet from the client releasing the prefix delegation.

No user configuration is required for this feature. Static route management is done automatically by the relay agent.

IPv6 routes are added when the relay agent relays a RELAY-REPLY packet, and IPv6 routes are deleted when the prefix delegation lease time expires or the relay agent receives a release message. An IPv6 static route in the routing table of the relay agent can be updated when the prefix delegation lease time is extended.

The DHCP—DHCPv6 Relay Agent Notification for Prefix Delegation feature leaves a static IPv6 route on the routing table of the relay agent. The registered IPv6 address allows unicast reverse packet forwarding (uRPF) to work by allowing the device doing the reverse lookup to confirm that the IPv6 address on the relay agent is not malformed or spoofed. The static route that remains in the routing table of the relay agent can be redistributed to other routing protocols to advertise the subnets to other nodes. Static routes will be removed when a DHCP_DECLINE message is sent by the client.

DHCPv6 Relay SSO and ISSU

In specific Cisco networking devices that support dual route processors (RPs), stateful switchover (SSO) takes advantage of RP redundancy to increase network availability. The feature establishes one of the RPs as the active processor while the other RP is designated as the standby processor, and then synchronizing critical state information between them. Following an initial synchronization between the two processors, SSO dynamically maintains RP state information between them.

The Cisco in-service software upgrade (ISSU) process allows Cisco software to be updated or otherwise modified while packet forwarding continues. In most networks, planned software upgrades are a significant cause of downtime. ISSU allows the Cisco software to be modified while packet forwarding continues. This increases network availability and reduces downtime caused by planned software upgrades.

The SSO and the ISSU use redundant hardware, with the active and standby RP each running an instance of the DHCPv6 relay agent. Both instances exchange run-time state data.

DHCPv6 Relay Options: Remote ID for Ethernet Interfaces

This feature adds the remote identification (remote-ID) option to relayed (RELAY-FORWARD) DHCPv6 packets.

The remote-ID option provides information to the DHCPv6 server, including port information, the system's DUID, and the VLAN ID. Collectively, this information can be used to uniquely identify both the relay and the port on the relay through which the client's packet arrived. The DHCPv6 server uses this information to select parameters specific to a particular user, host, or subscriber modem. This feature works only for Ethernet interfaces at this time.

This feature introduces no user configuration. Because the addition of the remote-ID option to the RELAY-FORWARD packet occurs automatically, no user configuration is necessary.

The DHCPv6 server does not need to echo the remote-ID option in the RELAY-REPLY packet. Internet Assigned Numbers Authority (IANA) has assigned the DHCPv6 option code 37 for the relay agent remote-ID option.

If the remote-ID option is included in the RELAY-REPLY packet, the option is stripped out of the packet before the packet is relayed to the client.

DHCPv6 Relay Options: Reload Persistent Interface ID Option

This feature makes the interface-ID option, which is used by relay agents to decide which interface should be used when forwarding a RELAY-REPLY packet, persistent. A persistent interface-ID option will not change if the router acting as a relay agent goes offline (such as during a reload or a power outage). When the router acting as a relay agent returns online, it is possible that changes to the internal interface index of the relay agent may have occurred in certain scenarios (such as cases where the relay agent reboots and has a change in the number of interfaces in the interface index, or the relay agents boots up and has more virtual interfaces than it did before the reboot). This feature prevents this scenario from causing any problems.

This feature changes the DHCPv6 interface-ID option to be expressed as simply the short form of the interface name. This syntax helps avoid potential problems that could arise due to physical or logical interfaces changing on the relay agent after a reload.

How to Configure IPv6 Access Services: DHCPv6 Relay Agent

Configuring the DHCPv6 Relay Agent

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 dhcp relay destination** *ipv6-address* [*interface-type interface-number*]
5. **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** *type number* **Example:** `Device(config)# interface gigabitethernet 4/2/0`	Specifies an interface type and number, and enters interface configuration mode.
Step 4	**ipv6 dhcp relay destination** *ipv6-address* [*interface-type interface-number*] **Example:** `Device(config-if) ipv6 dhcp relay destination FE80::250:A2FF:FEBF:A056 gigabitethernet 4/3/0`	Specifies a destination address to which client packets are forwarded and enables the DHCPv6 relay service on the interface.

Step 5	**end**
	Example:
	`Device(config-if)# end`
		Returns to privileged EXEC mode.

Configuration Examples for IPv6 Access Services: DHCPv6 Relay Agent

Example: Configuring the DHCPv6 Relay Agent

```
Device# show ipv6 dhcp interface

Ethernet1/0 is in relay mode
  Relay destinations:
    3FFB:C00:C18:6:A8BB:CCFF:FE03:2701
Serial3/0 is in relay mode
  Relay destinations:
    3FFB:C00:C18:6:A8BB:CCFF:FE03:2600
    FE80::A8BB:CCFF:FE03:2801 on Serial3/0
    FF05::1:3
```

Additional References

Related Documents

Related Topic	Document Title
IPv6 addressing and connectivity	*IPv6 Configuration Guide*
Cisco IOS commands	Cisco IOS Master Command List, All Releases
IPv6 commands	Cisco IOS IPv6 Command Reference
Cisco IOS IPv6 features	Cisco IOS IPv6 Feature Mapping

Standards and RFCs

Standard/RFC	Title
RFCs for IPv6	*IPv6 RFCs*

MIBs

MIB	MIBs Link
	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 and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for IPv6 Access Services: DHCPv6 Relay Agent

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 3: Feature Information for IPv6 Access Services: DHCPv6 Relay Agent

Feature Name	Releases	Feature Information
IPv6 Access Services: DHCPv6 Relay Agent	15.2(1)E	A DHCP relay agent, which may reside on the client's link, is used to relay messages between the client and server. The following commands were introduced or modified: **ipv6 dhcp relay destination**, **show ipv6 dhcp interface**.

Feature Name	Releases	Feature Information
DHCPv6 Relay Agent Notification for Prefix Delegation	15.2(1)E	DHCPv6 relay agent notification for prefix delegation allows the device working as a DHCPv6 relay agent to find prefix delegation options by reviewing the contents of a DHCPv6 packet that is being relayed by the relay agent to the client.
DHCPv6 Relay: Reload Persistent Interface ID Option	15.2(1)E	This feature makes the interface-ID option, which is used by relay agents to decide which interface should be used when forwarding a RELAY-REPLY packet, persistent.
DHCPv6—Relay chaining for Prefix Delegation	15.2(1)E	This feature enables DHCPv6 messages to be relayed through multiple relay agents.

CHAPTER 4

DHCPv6Relay—LightweightDHCPv6RelayAgent

The DHCPv6 Relay—Lightweight DHCPv6 Relay Agent feature allows relay agent information to be inserted by an access node that performs a link-layer bridging (non-routing) function. Lightweight DHCPv6 Relay Agent (LDRA) functionality can be implemented in existing access nodes, such as DSL access multiplexers (DSLAMs) and Ethernet switches, that do not support IPv6 control or routing functions. LDRA is used to insert relay-agent options in DHCP version 6 (DHCPv6) message exchanges primarily to identify client-facing interfaces. LDRA functionality can be enabled on an interface and on a VLAN.

An LDRA device or interface has the following features:

- Maintains interoperability with existing DHCPv6 relay agents and servers.
- Is functionally the equivalent of a Layer 2 relay agent, without routing capabilities.

Note LDRA is a device or interface on which LDRA functionality is configured.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for DHCPv6 Relay—Lightweight DHCPv6 Relay Agent

- You must understand DHCP and the functions of DHCP version 6 (DHCPv6) relay agents.

Restrictions for DHCPv6 Relay—Lightweight DHCPv6 Relay Agent

- An interface or port cannot be configured as both client facing and server facing at the same time.
- Access nodes implementing Lightweight DHCPv6 Relay Agent (LDRA) do not support IPv6 control or routing.
- Unlike a DHCPv6 relay agent, an LDRA does not implement any IPv6 control functions (like Internet Control Message Protocol version 6 [ICMPv6] functions) nor does it have any routing capability in the node.

Information About DHCPv6 Relay—Lightweight DHCPv6 Relay Agent

Background

A variety of different link-layer network topologies exist for the aggregation of IPv6 nodes into one or more routers. In Layer 2 aggregation networks (IEEE 802.1D bridging or similar) that have many nodes on a single link, a DHCP version 6 (DHCPv6) server or DHCP relay agent normally does not recognize how a DHCP client is attached to a network. Lightweight DHCPv6 Relay Agent (LDRA) allows relay-agent information, including the Interface-ID option, to be inserted by the access node so that the information may be used by the DHCPv6 server for client identification.

Interoperability between DHCPv6 Relay Agents and LDRA

DHCP version 6 (DHCPv6) relay agents are used to forward DHCPv6 messages between a client and a server when the client and server are not on the same IPv6 link. A DHCPv6 relay agent also adds an interface identifier option in the upstream DHCPv6 message (from client to server) to identify the interface on which the client is connected. This information is used by the DHCPv6 relay agent while forwarding the downstream

DHCPv6 message to the DHCPv6 client. The DHCPv6 relay agent is implemented alongside the routing functionality on the common node.

To maintain interoperability with existing DHCP relays and servers, Lightweight DHCPv6 Relay Agent (LDRA) implements the same message types (Relay-Forward and Relay-Reply) as a DHCPv6 relay agent.

LDRA allows relay-agent information to be inserted by an access node that performs a link-layer bridging (i.e., non-routing) function. The LDRA resides on the same IPv6 link as the client and a DHCPv6 relay agent or server.

LDRA for VLANs and Interfaces

You can configure LDRA on VLANs and interfaces. LDRA is not enabled by default. You must enable it on the VLAN or interface first.

In a typical deployment, a majority of the interfaces or ports on a device are client facing. In such a scenario, you can configure Lightweight DHCPv6 Relay Agent (LDRA) functionality on the VLAN. When you configure LDRA functionality on a VLAN, the functionality is configured on all the ports or interfaces within the VLAN. Instead of configuring LDRA functionality individually on the interfaces and ports within a VLAN, you can configure LDRA on the entire VLAN. As a result, all the ports or interfaces associated with the VLAN will be configured as client facing.

Note The LDRA configuration on a VLAN has to be configured as trusted or untrusted.

You can also configure LDRA functionality on a specific interface or port. An interface or port can be configured as - client-facing trusted, client-facing untrusted, or server facing.

Note An LDRA must implement a configuration setting for all client-facing interfaces, marking them as trusted or as untrusted.

By default, any interface that is configured as client facing will be configured as an untrusted interface. When a client-facing interface is deemed untrusted, LDRA will discard any message of type RELAY-FORWARD received from the client-facing interface.

How to Configure a Lightweight DHCPv6 Relay Agent

Configuring LDRA Functionality on a VLAN

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 dhcp-ldra** {**enable** | **disable**}
4. **vlan configuration** *vlan-number*
5. **ipv6 dhcp ldra attach-policy** {**client-facing-trusted** | **client-facing-untrusted**}
6. **exit**
7. **interface** *type number*
8. **switchport**
9. **switchport access vlan** *vlan-number*
10. **ipv6 dhcp-ldra attach-policy** {**client-facing-trusted** | **client-facing-untrusted** | **client-facing-disable** | **server-facing**}
11. **exit**
12. **interface** *type number*
13. **switchport**
14. **switchport access vlan** *vlan-number*
15. **ipv6 dhcp-ldra attach-policy** {**client-facing-trusted** | **client-facing-untrusted** | **client-facing-disable** | **server-facing**}
16. **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	**ipv6 dhcp-ldra** {**enable** | **disable**}
	Example:
	`Device(config)# ipv6 dhcp-ldra enable`
		Enables LDRA functionality globally.
		Note You need to enable LDRA functionality in global configuration mode before configuring it on a VLAN.

Step 4	**vlan configuration** *vlan-number* **Example:** `Device(config)# vlan configuration 5`	Specifies a VLAN number and enters into VLAN configuration mode.

Step 5	**ipv6 dhcp ldra attach-policy** {**client-facing-trusted** | **client-facing-untrusted**}
	Example:
	`Device (config-vlan-config)# ipv6 dhcp ldra attach-policy client-facing-trusted`
		Enables LDRA functionality on a specified VLAN.
		Note The **client-facing-trusted** keyword configures all the ports or interfaces associated with the VLAN as client facing, trusted ports. The **client-facing-untrusted** keyword configures all the ports or interfaces associated with the VLAN as client facing, untrusted ports.

Step 6	**exit** **Example:** `Device (config-vlan-config)# exit`	Exits VLAN configuration mode and returns to global configuration mode.
Step 7	**interface** *type number* **Example:** `Device(config)# interface ethernet 0/0`	Specifies an interface type and number, and enters interface configuration mode.
Step 8	**switchport** **Example:** `Device(config-if)# switchport`	Switches an interface that is in Layer 3 mode into Layer 2 mode for Layer 2 configuration.
Step 9	**switchport access vlan** *vlan-number* **Example:** `Device(config-if)# switchport access vlan 5`	Specifies that an interface operates in VLAN 5 instead of the default VLAN in the interface configuration mode.

Step 10	**ipv6 dhcp-ldra attach-policy** {**client-facing-trusted** | **client-facing-untrusted** | **client-facing-disable** | **server-facing**}
	Example:
	`Device(config-if)# ipv6 dhcp-ldra attach-policy client-facing-trusted`
		Enables LDRA functionality on a specified interface or port.
		Note The **client-facing-trusted** keyword configures the specified port or interface as a client facing, trusted port. The **client-facing-disable** keyword disables LDRA functionality on an interface or port. The **server-facing** keyword specifies an interface or port as server facing.

Step 11	**exit** **Example:** `Device (config-if)# exit`	Exits interface configuration mode and returns to global configuration mode.

	Command or Action	Purpose
Step 12	**interface** *type number* **Example:** `Device(config)# interface ethernet 1/0`	Specifies an interface type and number, and enters interface configuration mode.
Step 13	**switchport** **Example:** `Device(config-if)# switchport`	Switches an interface that is in Layer 3 mode into Layer 2 mode for Layer 2 configuration.
Step 14	**switchport access vlan** *vlan-number* **Example:** `Device(config-if)# switchport access vlan 5`	Specifies that an interface operates in VLAN 5 instead of the default VLAN in the interface configuration mode.

Step 15	**ipv6 dhcp-ldra attach-policy** {**client-facing-trusted** | **client-facing-untrusted** | **client-facing-disable** | **server-facing**}
	Example:
	`Device(config-if)# ipv6 dhcp-ldra attach-policy server-facing`
		Enables the LDRA functionality on the specified interface.
		Note The **client-facing-trusted** keyword configures the specified port or interface as a client facing, trusted port. The **client-facing-disable** keyword disables LDRA functionality on an interface or port. The **server-facing** keyword specifies an interface or port as server facing.

Step 16	**end**
	Example:
	`Device(config-if)# end`
		Exits VLAN configuration mode and returns to user EXEC mode.

Configuring LDRA Functionality on an Interface

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 dhcp-ldra** {**enable** | **disable**}
4. **interface** *type number*
5. **switchport**
6. **ipv6 dhcp-ldra attach-policy** {**client-facing-trusted** | **client-facing-untrusted** | **client-facing-disable** | **server-facing**}
7. **exit**
8. **interface** *type number*
9. **switchport**
10. **ipv6 dhcp-ldra attach-policy** {**client-facing-trusted** | **client-facing-untrusted** | **client-facing-disable** | **server-facing**}
11. **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-ldra** {**enable** | **disable**}
	Example:
	`Device(config)# ipv6 dhcp-ldra enable`
		Enables LDRA functionality globally.
		Note You need to enable LDRA functionality in global configuration mode before configuring it on an interface.

Step 4	**interface** *type number* **Example:** `Device(config)# interface ethernet 0/0`	Specifies an interface type and number, and enters interface configuration mode.
Step 5	**switchport** **Example:** `Device(config-if)# switchport`	Switches an interface that is in Layer 3 mode into Layer 2 mode for Layer 2 configuration.

	Command or Action	Purpose

Step 6	**ipv6 dhcp-ldra attach-policy** {**client-facing-trusted** | **client-facing-untrusted** | **client-facing-disable** | **server-facing**}
	Example:
	`Device(config-if)# ipv6 dhcp-ldra attach-policy client-facing-trusted`
		Enables LDRA functionality on a specified interface or port.
		Note The **client-facing-trusted** keyword configures the specified port or interface as a client facing, trusted port. The **client-facing-disable** keyword disables LDRA functionality on an interface or port. The **server-facing** keyword specifies an interface or port as server facing.

Step 7	**exit** **Example:** `Device(config-if)# exit`	Exits interface configuration mode and returns to global configuration mode.
Step 8	**interface** *type number* **Example:** `Device(config)# interface ethernet 1/0`	Specifies an interface type and number, and enters interface configuration mode.
Step 9	**switchport** **Example:** `Device(config-if)# switchport`	Switches an interface that is in Layer 3 mode into Layer 2 mode for Layer 2 configuration.

Step 10	**ipv6 dhcp-ldra attach-policy** {**client-facing-trusted** | **client-facing-untrusted** | **client-facing-disable** | **server-facing**}
	Example:
	`Device(config-if)# ipv6 dhcp-ldra attach-policy server-facing`
		Enables the LDRA functionality on the specified interface.
		Note The **client-facing-trusted** keyword configures the specified port or interface as a client facing, trusted port. The **client-facing-disable** keyword disables LDRA functionality on an interface or port. The **server-facing** keyword specifies an interface or port as server facing.

Step 11	**end**
	Example:
	`Device (config-if)# end`
		Exits interface configuration mode and returns to user EXEC mode.

Verifying and Troubleshooting LDRA

SUMMARY STEPS

1. **show ipv6 dhcp-ldra**
2. **show ipv6 dhcp-ldra statistics**
3. **debug ipv6 dhcp-ldra all**

DETAILED STEPS

Step 1 **show ipv6 dhcp-ldra**

This command displays LDRA configuration details. The fields in the example given below are self-explanatory.

Example:

```
Device # show ipv6 dhcp-ldra

DHCPv6 LDRA is Enabled.
DHCPv6 LDRA policy: client-facing-disable
       Target: none
DHCPv6 LDRA policy: client-facing-trusted
       Target: vlan 5
DHCPv6 LDRA policy: client-facing-untrusted
       Target: none
DHCPv6 LDRA policy: server-facing
       Target: Gi1/0/7
```

Step 2 **show ipv6 dhcp-ldra statistics**

This command displays LDRA configuration statistics before and after initiating a DHCP session. The fields in the examples below are self-explanatory.

Example:

```
Device # show ipv6 dhcp-ldra statistics

           DHCPv6 LDRA client facing statistics.
 Messages received 0
 Messages sent 0
 Messages discarded 0

           DHCPv6 LDRA server facing statistics.
 Messages received 0
 Messages sent 0
 Messages discarded 0

Device # show ipv6 dhcp-ldra statistics

           DHCPv6 LDRA client facing statistics.
 Messages received 2
 Messages sent 2
 Messages discarded 0
 Messages Received
 SOLICIT 1
 REQUEST 1
 Messages Sent
 RELAY-FORWARD 2
           DHCPv6 LDRA server facingstatistics.
 Messages received 2
 Messages sent 2
 Messages discarded 0
 Messages Received
 RELAY-REPLY 2
 Messages Sent
 ADVERTISE 1
 REPLY 1
```

Step 3 **debug ipv6 dhcp-ldra all**

This command enables all LDRA debugging flows. The fields in the example below are self-explanatory.

Example:

```
Device# debug ipv6 dhcp-ldra all
```

```
05:44:10: DHCPv6 LDRA API: Entered ipv6_dhcp_ldra_post_processor.
05:44:10: DHCPv6 LDRA EVENT: [Gi1/0/3 Vlan 5] Received SOLICIT from 2001:DB8:1::1
 to FF02::1:2.
05:44:10:   type SOLICIT(1), xid 8035955
05:44:10:   option ELAPSED-TIME(8), len 2
05:44:10:     elapsed-time 0
05:44:10:   option CLIENTID(1), len 10
05:44:10:     000300010015F906981B
05:44:10:   option ORO(6), len 4
05:44:10:     DNS-SERVERS,DOMAIN-LIST
05:44:10:   option IA-NA(3), len 12
05:44:10:     IAID 0x00040001, T1 0, T2 0
05:44:10: DHCPv6 LDRA API: Entered dhcpv6_ldra_client_facing_new_pak.
05:44:10: DHCPv6 LDRA EVENT: [Vlan 5] Sending RELAY-FORWARD from 2001:DB8:1::1
to FF02::1:2.
05:44:10:   type RELAY-FORWARD(12), hop 0
05:44:10:   link ::
05:44:10:   peer 2001:DB8:1::1
05:44:10:   option RELAY-MSG(9), len 48
05:44:10:     type SOLICIT(1), xid 8035955
05:44:10:     option ELAPSED-TIME(8), len 2
05:44:10:       elapsed-time 0
05:44:10:     option CLIENTID(1), len 10
05:44:10:       000300010015F906981B
05:44:10:     option ORO(6), len 4
05:44:10:       DNS-SERVERS,DOMAIN-LIST
05:44:10:     option IA-NA(3), len 12
05:44:10:       IAID 0x00040001, T1 0, T2 0
05:44:10:   option INTERFACE-ID(18), len 7
05:44:10:     0x4769312F302F33
05:44:10:   option REMOTEID(37), len 22
05:44:10:     0x000000090200130000050000A00030001588D09F89A00
05:44:11: DHCPv6 LDRA API: Entered ipv6_dhcp_ldra_post_processor.
05:44:11: DHCPv6 LDRA EVENT: [Gi1/0/3 Vlan 5] Received SOLICIT from 2001:DB8:1::1
 to FF02::1:2.
05:44:11:   type SOLICIT(1), xid 8035955
05:44:11:   option ELAPSED-TIME(8), len 2
05:44:11:     elapsed-time 0
05:44:11:   option CLIENTID(1), len 10
05:44:11:     000300010015F906981B
05:44:11:   option ORO(6), len 4
05:44:11:     DNS-SERVERS,DOMAIN-LIST
05:44:11:   option IA-NA(3), len 12
05:44:11:     IAID 0x00040001, T1 0, T2 0
05:44:11: DHCPv6 LDRA API: Entered dhcpv6_ldra_client_facing_new_pak.
05:44:11: DHCPv6 LDRA EVENT: [Vlan 5] Sending RELAY-FORWARD from 2001:DB8:1::1
to FF02::1:2.
05:44:11:   type RELAY-FORWARD(12), hop 0
```

```
05:44:11:   link ::
05:44:11:   peer 2001:DB8:1::1
05:44:11:   option RELAY-MSG(9), len 48
05:44:11:     type SOLICIT(1), xid 8035955
05:44:11:     option ELAPSED-TIME(8), len 2
05:44:11:       elapsed-time 0
05:44:11:     option CLIENTID(1), len 10
05:44:11:       000300010015F906981B
05:44:11:     option ORO(6), len 4
05:44:11:       DNS-SERVERS,DOMAIN-LIST
05:44:11:     option IA-NA(3), len 12
05:44:11:       IAID 0x00040001, T1 0, T2 0
05:44:11:   option INTERFACE-ID(18), len 7
05:44:11:     0x4769312F302F33
05:44:11:   option REMOTEID(37), len 22
05:44:11:     0x00000009020013000005000A00030001588D09F89A00
05:44:13: DHCPv6 LDRA API: Entered ipv6_dhcp_ldra_post_processor.
05:44:13: DHCPv6 LDRA EVENT: [Gi1/0/3 Vlan 5] Received SOLICIT from 2001:DB8:1::1
 to FF02::1:2.
05:44:13:   type SOLICIT(1), xid 8035955
05:44:13:   option ELAPSED-TIME(8), len 2
05:44:13:     elapsed-time 0
05:44:13:   option CLIENTID(1), len 10
05:44:13:     000300010015F906981B
05:44:13:   option ORO(6), len 4
05:44:13:     DNS-SERVERS,DOMAIN-LIST
05:44:13:   option IA-NA(3), len 12
05:44:13:     IAID 0x00040001, T1 0, T2 0
05:44:13: DHCPv6 LDRA API: Entered dhcpv6_ldra_client_facing_new_pak.
05:44:13: DHCPv6 LDRA EVENT: [Vlan 5] Sending RELAY-FORWARD from 2001:DB8:1::1
to FF02::1:2.
05:44:13:   type RELAY-FORWARD(12), hop 0
05:44:13:   link ::
05:44:13:   peer 2001:DB8:1::1
05:44:13:   option RELAY-MSG(9), len 48
05:44:13:     type SOLICIT(1), xid 8035955
05:44:13:     option ELAPSED-TIME(8), len 2
05:44:13:       elapsed-time 0
05:44:13:     option CLIENTID(1), len 10
05:44:13:       000300010015F906981B
05:44:13:     option ORO(6), len 4
05:44:13:       DNS-SERVERS,DOMAIN-LIST
05:44:13:     option IA-NA(3), len 12
05:44:13:       IAID 0x00040001, T1 0, T2 0
05:44:13:   option INTERFACE-ID(18), len 7
05:44:13:     0x4769312F302F33
05:44:13:   option REMOTEID(37), len 22
05:44:13:     0x00000009020013000005000A00030001588D09F89A00
05:44:17: DHCPv6 LDRA API: Entered ipv6_dhcp_ldra_post_processor.
05:44:17: DHCPv6 LDRA EVENT: [Gi1/0/3 Vlan 5] Received SOLICIT from 2001:DB8:1::1
 to FF02::1:2.
05:44:17:   type SOLICIT(1), xid 8035955
05:44:17:   option ELAPSED-TIME(8), len 2
05:44:17:     elapsed-time 0
05:44:17:   option CLIENTID(1), len 10
05:44:17:     000300010015F906981B
05:44:17:   option ORO(6), len 4
05:44:17:     DNS-SERVERS,DOMAIN-LIST
05:44:17:   option IA-NA(3), len 12
05:44:17:     IAID 0x00040001, T1 0, T2 0
```

```
05:44:17: DHCPv6 LDRA API: Entered dhcpv6_ldra_client_facing_new_pak.
05:44:17: DHCPv6 LDRA EVENT: [Vlan 5] Sending RELAY-FORWARD from 2001:DB8:1::1
to FF02::1:2.
05:44:17:   type RELAY-FORWARD(12), hop 0
05:44:17:   link ::
05:44:17:   peer 2001:DB8:1::1
05:44:17:   option RELAY-MSG(9), len 48
05:44:17:     type SOLICIT(1), xid 8035955
05:44:17:     option ELAPSED-TIME(8), len 2
05:44:17:       elapsed-time 0
05:44:17:     option CLIENTID(1), len 10
05:44:17:       000300010015F906981B
05:44:17:     option ORO(6), len 4
05:44:17:       DNS-SERVERS,DOMAIN-LIST
05:44:17:     option IA-NA(3), len 12
05:44:17:       IAID 0x00040001, T1 0, T2 0
05:44:17:   option INTERFACE-ID(18), len 7
05:44:17:     0x4769312F302F33
05:44:17:   option REMOTEID(37), len 22
05:44:17:     0x000000090200130000050000A00030001588D09F89A00
```

Configuration Examples for a Lightweight DHCPv6 Relay Agent

Example: Configuring LDRA Functionality on a VLAN

The following example shows how to configure Lightweight DHCPv6 Relay Agent (LDRA) on a VLAN numbered 5.

```
Device> enable
Device# configure terminal
Device(config)# ipv6 dhcp-ldra enable
Device(config)# vlan configuration 5
Device(config-vlan-config)# ipv6 dhcp ldra attach-policy client-facing-trusted
Device(config-vlan-config)# exit
Device(config)# interface ethernet 0/0
Device(config-if)# switchport
Device(config-if)# switchport access vlan 5
Device(config-if)# ipv6 dhcp-ldra attach-policy client-facing-trusted
Device(config-if)# exit
Device(config)# interface ethernet 1/0
Device(config-if)# switchport
Device(config-if)# switchport access vlan 5
Device(config-if)# ipv6 dhcp-ldra attach-policy server-facing
Device(config-if)# end
```

Example: Configuring LDRA Functionality on an Interface

In the following example, LDRA is configured on the interfaces ethernet 0/0 and ethernet 1/0:

```
Device> enable
Device # configure terminal
```

```
Device(config)# ipv6 dhcp-ldra enable
Device(config)# interface ethernet 0/0
Device(config-if)# switchport
Device(config-if)# ipv6 dhcp-ldra attach-policy client-facing-trusted
Device(config-if)# exit
Device(config)# interface ethernet 1/0
Device(config-if)# switchport
Device(config-if)# ipv6 dhcp-ldra attach-policy server-facing
Device(config-if)# end
```

Additional References for DHCPv6 Relay—Lightweight DHCPv6 Relay Agent

Related Documents

Related Topic	Document Title
Configuring the DHCPv6 Relay Agent	*IP Addressing: DHCP Configuration Guide*
Cisco IOS commands	Cisco IOS Master Command List, All Releases
DHCP commands	Cisco IOS IP Addressing Services Command Reference
DHCP conceptual information	*DHCP Overview module in the IP Addressing: DHCP Configuration Guide*

Standards and RFCs

Standard/RFC	Title
RFC 6221	*Lightweight DHCPv6 Relay Agent*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for DHCPv6 Relay—Lightweight DHCPv6 Relay Agent

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 4: Feature Information for Lightweight DHCPv6 Relay Agent

Feature Name	Releases	Feature Information
DHCPv6 Relay—Lightweight DHCPv6 Relay Agent	15.1(2)E	The DHCPv6 Relay—Lightweight DHCPv6 Relay Agent feature allows relay agent information to be inserted by an access node that performs a link-layer bridging function. The following commands were introduced or modified: **clear ipv6 dhcp-ldra statistics**, **debug ipv6 dhcp-ldra**, **ipv6 dhcp ldra attach-policy**, **ipv6 dhcp-ldra**, **ipv6 dhcp-ldra attach-policy**, **show ipv6 dhcp-ldra**.

Glossary

Access Node —A device that combines many interfaces onto one link. An access node is not IP-aware in a data path.

Client facing —An interface on an access node that carries traffic towards a DHCPv6 client.

LDRA—Lightweight DHCPv6 Relay Agent. An interface or device on which LDRA functionality is configured (or that supports LDRA functionality.)

LDRA function—A function on an access node that intercepts DHCP messages between clients and servers.

Link—A communication facility or medium over which nodes can communicate at the link layer.

Link-local address—An IP address having only local scope that can be used to reach neighboring nodes attached to the same link. Every interface has a link-local address, which is defined by the address prefix fe80::/10.

Network-facing—An interface on an access node that carries traffic towards a DHCPv6 server.

Relay Agent—A node that acts as an intermediary to deliver DHCP messages between clients and servers.

CHAPTER 5

DHCPv6 Relay and Server - MPLS VPN Support

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About DHCPv6 Relay and Server - MPLS VPN Support

DHCPv6 Server and Relay—MPLS VPN Support

To facilitate managed central services in a Multiprotocol Label Switching (MPLS)-based network, DHCPv6 must be made MPLS-aware so that a single resource can be used to serve multiple VPNs instead of dedicating a resource to a single VPN.

The DHCPv6 server implementation of MPLS VPN allows a per-pool configuration so that DHCPv6 pools can be associated with a VPN routing and forwarding (VRF) instance. The DHCPv6 server differentiates clients from various VRFs and assigns an IPv6 prefix accordingly from the respective VRF pools. Meanwhile, the DHCPv6 bindings store the clients' VRF information.

The DHCPv6 relay implementation allows the configuration of the destination VRF instance to which the relay messages will be forwarded. The relay adds the client's VPN information while forwarding the client's DHCPv6 requests toward the server, and the relay agent then processes the client's VPN information in reply packets from the server.

The relay agent adds IPv6 static routes for delegated prefixes in corresponding clients' VRF, and the relay agent's high availability (HA) functionality synchronizes the VRF information while synchronizing static routes created by the relay process.

The DHCPv6 relay and server VRF-aware features are disabled by default.

How to Configure DHCPv6 Relay and Server - MPLS VPN Support

Configuring a VRF-Aware Relay and Server for MPLS VPN Support

Configuring a VRF-Aware Relay

Note You do not have to configure this feature on specified interfaces. If you want the feature to be enabled globally only on a device, perform steps 1, 2, and 3

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ipv6 dhcp-relay option vpn**
4. **interface** *type number*
5. **ipv6 dhcp relay option vpn**
6. **ipv6 dhcp relay destination** *ipv6-address* [*interface-type interface-number* | **vrf** *vrf-name* | **global**]
7. **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# configure terminal`	Enters global configuration mode.
Step 3	**ipv6 dhcp-relay option vpn** **Example:** `Device(config)# ipv6 dhcp-relay option vpn`	Enables the DHCP for IPv6 relay VRF-aware feature globally.
Step 4	**interface** *type number* **Example:** `Device(config)# interface gigabitethernet 0/0/0`	Specifies an interface type and number, and enters interface configuration mode.
Step 5	**ipv6 dhcp relay option vpn** **Example:** `Device(config-if)# ipv6 dhcp relay option vpn`	Enables the DHCP for IPv6 relay VRF-aware feature on the specified interface. Enabling this command supersedes the configuration that is enabled by using the **ipv6 dhcp-relay option vpn** command.
Step 6	**ipv6 dhcp relay destination** *ipv6-address* [*interface-type interface-number* | **vrf** *vrf-name* | **global**] **Example:** `Device(config-if)# ipv6 dhcp relay destination FE80::250:A2FF:FEBF:A056 ethernet 0/0`	Specifies a destination address to which client messages are forwarded.

Step 7	**end**
	Example:
	`Device(config-if)# end`
		Returns to privileged EXEC mode.

Configuring a VRF-Aware Server

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 dhcp server vrf enable**
5. **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** *type number* **Example:** `Device(config)# interface gigabitethernet 0/0/0`	Specifies an interface type and number, and enters interface configuration mode.
Step 4	**ipv6 dhcp server vrf enable** **Example:** `Device(config-if)# ipv6 dhcp server vrf enable`	Enables the DHCPv6 server VRF-aware feature on an interface.

Step 5	**end**
	Example:
	`Device(config-if)# end`
		Returns to privileged EXEC mode.

Configuration Examples for DHCPv6 Server - MPLS VPN Support

Example: Configuring a VRF-Aware Relay

```
Device# show ipv6 dhcp relay binding

Relay Bindings associated with default vrf:
Prefix: 2001:DB8:0:1::/64 (Ethernet0/0)
  DUID: 00030001AABBCC006500
  IAID: 196609
  lifetime: 2592000
  expiration: 12:34:28 IST Oct 14 2010
Summary:
  Total number of Relay bindings = 1
  Total number of Relay bindings added by Bulk lease = 0
RELAY#
```

Example: Configuring a VRF-Aware Server

```
Device# show ipv6 dhcp binding

Client: FE80::A8BB:CCFF:FE00:6400
  DUID: 00030001AABBCC006400
  VRF : global
  Interface : Ethernet0/0
  IA PD: IA ID 0x00030001, T1 302400, T2 483840
    Prefix: 2001::1/64
            preferred lifetime 604800, valid lifetime 2592000
            expires at Oct 15 2010 03:18 PM (2591143 seconds)

Device# show ipv6 route static

IPv6 Routing Table - default - 4 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2
       IA - ISIS interarea, IS - ISIS summary, D - EIGRP, EX - EIGRP external
       ND - Neighbor Discovery
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
S   2001::/64 [1/0]
     via FE80::A8BB:CCFF:FE00:6400, Ethernet0/0
```

Additional References

Related Documents

Related Topic	Document Title
IPv6 addressing and connectivity	*IPv6 Configuration Guide*
Cisco IOS commands	Cisco IOS Master Command List, All Releases

Related Topic	Document Title
IPv6 commands	*Cisco IOS IPv6 Command Reference*
Cisco IOS IPv6 features	Cisco IOS IPv6 Feature Mapping

Standards and RFCs

Standard/RFC	Title
RFCs for IPv6	*IPv6 RFCs*

MIBs

MIB	MIBs Link
	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 and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for DHCPv6 Relay and Server - MPLS VPN Support

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 5: Feature Information for DHCPv6 Relay and Server - MPLS VPN Support

Feature Name	Releases	Feature Information
DHCPv6 Relay - MPLS VPN Support	15.2(3)E	The DHCPv6 relay implementation of MPLS VPN allows configuration of the destination VRF instance to which the relay messages are forwarded. The following commands were introduced or modified: **ipv6 dhcp relay destination**, **ipv6 dhcp relay option vpn**, **ipv6 dhcp server vrf enable**, **show ipv6 dhcp relay binding**.
DHCPv6 Server - MPLS VPN Support	15.2(3)E	The DHCPv6 server implementation of MPLS VPN allows a per-pool configuration so that DHCPv6 pools can be associated with a VPN routing and forwarding (VRF) instance. The following commands were introduced or modified: **ipv6 dhcp relay destination**, **ipv6 dhcp relay option vpn**, **ipv6 dhcp server vrf enable**, **show ipv6 dhcp relay binding**.
VRF Aware DHCPv6 Server and Relay for Prefix Delegation	15.2(3)E	The VRF Aware DHCPv6 Server and Relay for Prefix Delegation feature ensures that the DHCPv6 server and relay involved in delegating prefixes are VRF aware.
VRF aware DHCPv6 server/Relay for IANA	15.2(3)E	The VRF aware DHCPv6 server/Relay for IANA feature ensures that the DHCPv6 server and relay used for IP address provision are VRF aware.
VRF aware DHCPv6 relay	15.2(3)E	The VRF aware DHCPv6 relay feature ensures that the DHCPv6 relay involved in forwarding IP addresses is VRF aware.