



DHCP—DHCPv6 Guard

Last Updated: December 3, 2012

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, page 1](#)
- [Restrictions for DHCPv6 Guard, page 1](#)
- [Information About DHCPv6 Guard, page 2](#)
- [How to Configure DHCPv6 Guard, page 2](#)
- [Configuration Examples for DHCPv6 Guard, page 7](#)
- [Additional References, page 7](#)
- [Feature Information for DHCP—DHCPv6 Guard, page 8](#)

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.



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Information About DHCPv6 Guard

- [DHCPv6 Guard Overview, page 2](#)

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, page 3](#)

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	<p>enable</p> <p>Example:</p> <pre>Device> enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> • 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 <i>access-list-name</i> Example: Device(config)# ipv6 access-list acl1	Defines the IPv6 access list and enters IPv6 access list configuration mode.
Step 4	permit host <i>address any</i> 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 <i>list-name</i> permit <i>ipv6-prefix</i> 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 <i>policy-name</i> Example: Device(config)# ipv6 dhcp guard policy poll	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).

Command or Action	Purpose
<p>Step 9 <code>match server access-list <i>ipv6-access-list-name</i></code></p> <p>Example:</p> <pre>Device(config-dhcp-guard)# match server access-list acl1</pre>	<p>(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.</p>
<p>Step 10 <code>match reply prefix-list <i>ipv6-prefix-list-name</i></code></p> <p>Example:</p> <pre>Device(config-dhcp-guard)# match reply prefix-list abc</pre>	<p>(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.</p>
<p>Step 11 <code>preference min <i>limit</i></code></p> <p>Example:</p> <pre>Device(config-dhcp-guard)# preference min 0</pre>	<p>(Optional) Enables verification that the advertised preference (in preference option) is greater than the specified limit. If not specified, this check will be bypassed.</p>
<p>Step 12 <code>preference max <i>limit</i></code></p> <p>Example:</p> <pre>Device(config-dhcp-guard)# preference max 255</pre>	<p>(Optional) Enables verification that the advertised preference (in preference option) is less than the specified limit. If not specified, this check will be bypassed.</p>
<p>Step 13 <code>trusted-port</code></p> <p>Example:</p> <pre>Device(config-dhcp-guard)# trusted-port</pre>	<p>(Optional) Specifies that this policy is being applied to trusted ports. All DHCP guard policing will be disabled.</p>
<p>Step 14 <code>exit</code></p> <p>Example:</p> <pre>Device(config-dhcp-guard)# exit</pre>	<p>Exits DHCP guard configuration mode and returns to global configuration mode.</p>
<p>Step 15 <code>interface <i>type number</i></code></p> <p>Example:</p> <pre>Device(config)# interface GigabitEthernet 0/2/0</pre>	<p>Specifies an interface and enters interface configuration mode.</p>

Command or Action	Purpose
<p>Step 16 <code>switchport</code></p> <p>Example:</p> <pre>Device(config-if)# switchport</pre>	<p>Puts an interface that is in Layer 3 mode into Layer 2 mode for Layer 2 configuration.</p>
<p>Step 17 <code>ipv6 dhcp guard [attach-policy <i>policy-name</i>] [vlan {add all all except none remove} <i>vlan-id</i>][... <i>vlan-id</i>]</code></p> <p>Example:</p> <pre>Device(config-if)# ipv6 dhcp guard attach-policy poll vlan add vlan1</pre>	<p>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.</p>
<p>Step 18 <code>exit</code></p> <p>Example:</p> <pre>Device(config-if)# exit</pre>	<p>Exits interface configuration mode and returns to global configuration mode.</p>
<p>Step 19 <code>vlan <i>vlan-id</i></code></p> <p>Example:</p> <pre>Device(config)# vlan 1</pre>	<p>Specifies a VLAN and enters VLAN configuration mode.</p>
<p>Step 20 <code>ipv6 dhcp guard [attach-policy <i>policy-name</i>]</code></p> <p>Example:</p> <pre>Device(config-vlan)# ipv6 dhcp guard attach-policy poll</pre>	<p>Attaches a DHCPv6 guard policy to a VLAN.</p>
<p>Step 21 <code>exit</code></p> <p>Example:</p> <pre>Device(config-vlan)# exit</pre>	<p>Exits interface configuration mode and returns to global configuration mode.</p>
<p>Step 22 <code>exit</code></p> <p>Example:</p> <pre>Device(config)# exit</pre>	<p>Exits global configuration mode and returns to privileged EXEC mode.</p>

Command or Action	Purpose
Step 23 <code>show ipv6 dhcp guard policy [policy-name]</code> Example: Device# <code>show ipv6 dhcp policy guard poll</code>	(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, page 7](#)

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 poll
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 poll vlan add 1
  vlan 1
  ipv6 dhcp guard attach-policy poll
show ipv6 dhcp guard policy poll
```

Additional References

Related Documents

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

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 1 **Feature Information for DHCP—DHCPv6 Guard**

Feature Name	Releases	Feature Information
DHCP—DHCPv6 Guard	15.2(4)S 15.0(2)SE 15.1(2)SG Cisco IOS XE Release 3.8S Cisco IOS XE Release 3.2SE	<p>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.</p> <p>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).</p>

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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.

© 2012 Cisco Systems, Inc. All rights reserved.