

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).

- Restrictions for DHCPv6 Guard, on page 1
- Information About DHCPv6 Guard, on page 1
- How to Configure DHCPv6 Guard, on page 2
- Configuration Examples for DHCPv6 Guard, on page 5
- Additional References, on page 5
- Feature Information for DHCP—DHCPv6 Guard, on page 6

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. **exit**
18. **exit**
19. **show ipv6 dhcp guard policy** [*policy-name*]

DETAILED STEPS

Procedure

	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 access-list** *access-list-name* **Example:**	Defines the IPv6 access list and enters IPv6 access list configuration mode.

	Command or Action	Purpose
	`Device(config)# ipv6 access-list acl1`	
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.
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.

	Command or Action	Purpose
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	**exit** **Example:** `Device(config-if)# exit`	Exits interface configuration mode and returns to global configuration mode.
Step 18	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.
Step 19	**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:

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 1: Feature Information for DHCP—DHCPv6 Guard

Feature Name	Releases	Feature Information
DHCP—DHCPv6 Guard		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)**.