



IP Addressing: DHCP Configuration Guide, Cisco IOS XE Release 3E

First Published: August 27, 2013

Last Modified: August 27, 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.

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: <http://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)

© Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1

DHCP—DHCPv6 Guard 1

- Finding Feature Information 1
- Restrictions for DHCPv6 Guard 1
- Information About DHCPv6 Guard 2
 - DHCPv6 Guard Overview 2
- How to Configure DHCPv6 Guard 3
 - Configuring DHCP—DHCPv6 Guard 3
- Configuration Examples for DHCPv6 Guard 6
 - Example: Configuring DHCP—DHCPv6 Guard 6
- Additional References 7
- Feature Information for DHCP—DHCPv6 Guard 8

CHAPTER 2

DHCP Gleaning 11

- Finding Feature Information 11
- Prerequisites for DHCP Gleaning 11
- Information About DHCP Gleaning 12
 - Overview of DHCP Gleaning 12
 - DHCP Snooping 12
- How to Configure DHCP Gleaning 12
 - Configuring an Interface as a Trusted or an Untrusted Source for DHCP Gleaning 12
- Configuration Examples for DHCP Gleaning 14
 - Example: Configuring an Interface as a Trusted or an Untrusted Source for DHCP Gleaning 14
- Additional References 14
- Feature Information for DHCP Gleaning 16



CHAPTER

1

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, page 1](#)
- [Restrictions for DHCPv6 Guard, page 1](#)
- [Information About DHCPv6 Guard, page 2](#)
- [How to Configure DHCPv6 Guard, page 3](#)
- [Configuration Examples for DHCPv6 Guard, page 6](#)
- [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.

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. exit
18. vlan configuration *vlan-id*
19. ipv6 dhcp guard [attach-policy *policy-name*]
20. exit
21. exit
22. 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</i> 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 <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).
Step 9	match server access-list <i>ipv6-access-list-name</i> 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 <i>ipv6-prefix-list-name</i> Example: <pre>Device(config-dhcp-guard)# match reply prefix-list abc</pre>	(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 <i>limit</i> Example: <pre>Device(config-dhcp-guard)# preference min 0</pre>	(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 <i>limit</i> Example: <pre>Device(config-dhcp-guard)# preference max 255</pre>	(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: <pre>Device(config-dhcp-guard)# trusted-port</pre>	(Optional) Specifies that this policy is being applied to trusted ports. All DHCP guard policing will be disabled.
Step 14	exit Example: <pre>Device(config-dhcp-guard)# exit</pre>	Exits DHCP guard configuration mode and returns to global configuration mode.
Step 15	interface <i>type number</i> Example: <pre>Device(config)# interface GigabitEthernet 0/2/0</pre>	Specifies an interface and enters interface configuration mode.
Step 16	switchport Example: <pre>Device(config-if)# switchport</pre>	Puts an interface that is in Layer 3 mode into Layer 2 mode for Layer 2 configuration.
Step 17	exit Example: <pre>Device(config-if)# exit</pre>	Exits interface configuration mode and returns to global configuration mode.

	Command or Action	Purpose
Step 18	vlan configuration <i>vlan-id</i> Example: Device(config)# vlan configuration 1	Specifies a VLAN and enters VLAN configuration mode.
Step 19	ipv6 dhcp guard [attach-policy <i>policy-name</i>] Example: Device(config-vlan-config)# ipv6 dhcp guard attach-policy poll	Attaches a DHCPv6 guard policy to a VLAN.
Step 20	exit Example: Device(config-vlan-config)# exit	Exits VLAN configuration mode and returns to global configuration mode.
Step 21	exit Example: Device(config)# exit	Exits global configuration mode and returns to privileged EXEC mode.
Step 22	show ipv6 dhcp guard policy [<i>policy-name</i>] Example: Device# show ipv6 dhcp policy guard poll	(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 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 configuration 1
   ipv6 dhcp guard attach-policy poll
 show ipv6 dhcp guard policy poll

```

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	<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 [http://www.cisco.com/go/featurenavigator](#). An account on Cisco.com is not required.

Table 1: Feature Information for DHCP—DHCPv6 Guard

Feature Name	Releases	Feature Information
DHCP—DHCPv6 Guard	Cisco IOS XE Release 3.5E Cisco IOS XE 3.5 SE Cisco IOS XE Release 3.6E	<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>In Cisco IOS XE Release 3.6E, this feature is supported on Cisco Catalyst 3850 Series Switches</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>



CHAPTER 2

DHCP Gleaning

This document describes the Dynamic Host Configuration Protocol Gleaning feature.

- [Finding Feature Information, page 11](#)
- [Prerequisites for DHCP Gleaning, page 11](#)
- [Information About DHCP Gleaning, page 12](#)
- [How to Configure DHCP Gleaning, page 12](#)
- [Configuration Examples for DHCP Gleaning, page 14](#)
- [Additional References, page 14](#)
- [Feature Information for DHCP Gleaning, page 16](#)

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.

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, glean helps to differentiate an untrusted device port that is connected to an end user from a trusted port connected to a DHCP server.

DHCP glean is a read-only DHCP snooping functionality that allows components to register and glean only DHCP version 4 packets. When you enable DHCP glean, 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 you add a secondary VLAN to a private VLAN, ensure that glean is enabled on the secondary VLAN, even though snooping is disabled on the primary VLAN. By default, the glean functionality is disabled. However, when you enable a device sensor, DHCP glean 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 glean 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 glean is enabled on an untrusted interface or on a device port.

**Note**

By default, DHCP glean 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. <ul style="list-style-type: none"> • 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 <i>type number</i> Example: Device(config)# interface gigabitEthernet 1/0/1 Device(config-if)#	Enters interface configuration mode, where <i>type number</i> 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
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/support

Feature Information for 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 [http://www.cisco.com/go/featurenavigator](#). An account on Cisco.com is not required.

Table 2: Feature Information for DHCP Gleaning

Feature Name	Releases	Feature Information
DHCP Gleaning	Cisco IOS XE 3.6E	<p>This document describes the DHCP Gleaning feature.</p> <p>In Cisco IOS Release Cisco IOS XE Release 3.6E, this feature is supported on the following platforms:</p> <ul style="list-style-type: none"> • Cisco Catalyst 3850 Series Switches • Cisco Catalyst 3650 Series Switches • Cisco Catalyst 4500E Supervisor Engine 8-E <p>The following commands were introduced or modified for this feature: ip dhcp snooping glean, show ip dhcp snooping</p>