



Implementing the DHCP on Cisco ASR 9000 Series Routers

This module describes the concepts and tasks you will use to configure Dynamic Host Configuration Protocol (DHCP) features on Cisco ASR 9000 Series Aggregation Services Routers.



Note

For a complete description of the DHCP commands listed in this module, refer to the *Cisco ASR 9000 Series Aggregation Services Router IP Addresses and Services Command Reference* publication. To locate documentation of other commands that appear in this chapter, use the command reference master index, or search online.

Feature History for Implementing the DHCP on the Cisco ASR 9000 Series Router

| Release | Modification |
|---------------|---|
| Release 3.7.2 | This feature was introduced on Cisco ASR 9000 Series Routers. |
| Release 3.9.0 | No modification. |
| Release 3.9.1 | No modification. |

Contents

- [Implementing DHCP Snooping on Cisco ASR 9000 Series Routers, page 102](#)
- [Additional References, page 114](#)

Implementing DHCP Relay Agent on Cisco ASR 9000 Series Routers

- [Prerequisites for Configuring DHCP Relay Agent, page 88](#)
- [Information About DHCP Relay Agent, page 88](#)
- [How to Configure and Enable DHCP Relay Agent, page 88](#)
- [Configuration Examples for DHCP Relay Agent, page 101](#)

Prerequisites for Configuring DHCP Relay Agent

The following prerequisites are required to configure a DHCP relay agent:

- A Cisco ASR 9000 Series Router running Cisco IOS XR software
- A configured and running DHCP client and DHCP server
- Connectivity between the relay agent and DHCP server

Information About DHCP Relay Agent

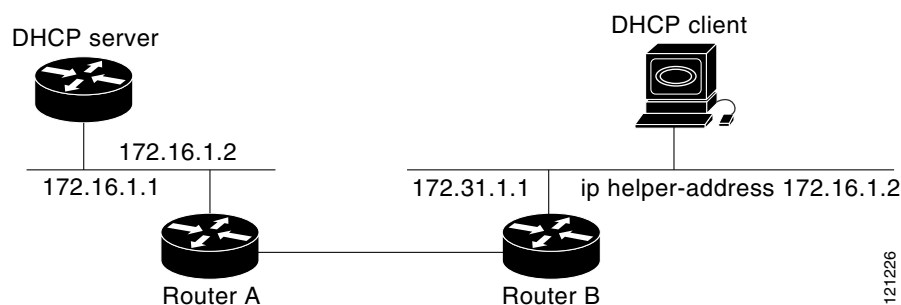
A DHCP relay agent is a host that forwards DHCP packets between clients and servers that do not reside on a shared physical subnet. Relay agent forwarding is distinct from the normal forwarding of an IP router where IP datagrams are switched between networks transparently.

DHCP clients use User Datagram Protocol (UDP) broadcasts to send DHCPDISCOVER messages when they lack information about the network to which they belong.

If a client is on a network segment that does not include a server, a relay agent is needed on that network segment to ensure that DHCP packets reach the servers on another network segment. UDP broadcast packets are not forwarded, because most routers are not configured to forward broadcast traffic. You can configure a DHCP relay agent to forward DHCP packets to a remote server by configuring a DHCP relay profile and configure one or more helper addresses in it. You can assign the profile to an interface or a VRF.

Figure 2 demonstrates the process. The DHCP client broadcasts a request for an IP address and additional configuration parameters on its local LAN. Acting as a DHCP relay agent, Router B picks up the broadcast, changes the destination address to the DHCP server's address and sends the message out on another interface. The relay agent inserts the IP address of the interface, on which the DHCP client's packets are received, into the gateway address (giaddr) field of the DHCP packet, which enables the DHCP server to determine which subnet should receive the offer and identify the appropriate IP address range. The relay agent unicasts the messages to the server address, in this case 172.16.1.2 (which is specified by the helper address in the relay profile).

Figure 2 Forwarding UDP Broadcasts to a DHCP Server Using a Helper Address



121226

How to Configure and Enable DHCP Relay Agent

This section contains the following tasks:

- [Configuring and Enabling DHCP Relay Agent, page 89](#)

- [This task describes how to configure DHCP ., page 90](#)
- [Enabling DHCP Relay Agent on an Interface, page 92](#)
- [Disabling DHCP Relay on an Interface, page 94](#)
- [Enabling DHCP Relay on a VRF, page 95](#)
- [Configuring theRelay Agent Information Option, page 96](#)
- [Configuring Relay Agent Giaddr Policy, page 99](#)

Configuring and Enabling DHCP Relay Agent

This task describes how to configure and enable DHCP relay agent.

SUMMARY STEPS

1. **configure**
2. **dhcp ipv4**
3. **end**
or
commit

DETAILED STEPS

| | Command or Action | Purpose |
|--------|---|--|
| Step 1 | configure Example: RP/0/RSP0/CPU0:router# configure | Enters global configuration mode. |
| Step 2 | dhcp ipv4 Example: RP/0/RSP0/CPU0:router(config)# dhcp ipv4 | Enters DHCP IPv4 configuration submenu. |
| Step 3 | end or commit Example: RP/0/RSP0/CPU0:router(config)# end OR RP/0/RSP0/CPU0:router(config)# commit | Saves configuration changes. <ul style="list-style-type: none"> When you issue the end command, the system prompts you to commit changes: Uncommitted changes found, commit them before exiting (yes/no/cancel)? [cancel]: <ul style="list-style-type: none"> Entering yes saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode. Entering no exits the configuration session and returns the router to EXEC mode without committing the configuration changes. Entering cancel leaves the router in the current configuration session without exiting or committing the configuration changes. Use the commit command to save the configuration changes to the running configuration file and remain within the configuration session. |

This task describes how to configure DHCP .

SUMMARY STEPS

- configure**
- dhcp ipv4**
- profile name relay**
- helper-address [vrf name] address**
- end**
or
commit

DETAILED STEPS

| | Command or Action | Purpose |
|--------|--|---|
| Step 1 | <p>configure</p> <p>Example: RP/0/RSP0/CPU0:router# configure</p> | Enters global configuration mode. |
| Step 2 | <p>dhcp ipv4</p> <p>Example: RP/0/RSP0/CPU0:router(config)# dhcp ipv4</p> | Enters DHCP IPv4 configuration submenu. |
| Step 3 | <p>profile profile-name relay</p> <p>Example: RP/0/RSP0/CPU0:router(config-dhcpv4)# profile client relay</p> | Enters DHCP IPv4 profile relay submenu. |
| Step 4 | <p>helper-address [vrf vrf-name] address</p> <p>Example: RP/0/RSP0/CPU0:router(config-dhcpv4-relay-profile)# helper-address vrf vrf1 10.10.1.1</p> | <p>Forwards UDP broadcasts, including BOOTP and DHCP.</p> <ul style="list-style-type: none"> The value of the <i>address</i> argument can be a specific DHCP server address or a network address (if other DHCP servers are on the destination network segment). Using the network address enables other servers to respond to DHCP requests. For multiple servers, configure one helper address for each server. |
| Step 5 | <p>end</p> <p>or</p> <p>commit</p> <p>Example: RP/0/RSP0/CPU0:router(config)# end or RP/0/RSP0/CPU0:router(config)# commit</p> | <p>Saves configuration changes.</p> <ul style="list-style-type: none"> When you issue the end command, the system prompts you to commit changes: Uncommitted changes found, commit them before exiting (yes/no/cancel)? [cancel]: <ul style="list-style-type: none"> Entering yes saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode. Entering no exits the configuration session and returns the router to EXEC mode without committing the configuration changes. Entering cancel leaves the router in the current configuration session without exiting or committing the configuration changes. Use the commit command to save the configuration changes to the running configuration file and remain within the configuration session. |

Enabling DHCP Relay Agent on an Interface

This task describes how to enable the Cisco IOS XR DHCP relay agent on an interface.



Note

On Cisco IOS XR software, the DHCP relay agent is disabled by default.

SUMMARY STEPS

1. **configure**
2. **dhcp ipv4**
3. **interface** *type instance* **relay profile** *profile-name*
4. **end**
or
commit

DETAILED STEPS

| | Command or Action | Purpose |
|--------|---|---|
| Step 1 | configure Example: RP/0/RSP0/CPU0:router# configure | Enters global configuration mode. |
| Step 2 | dhcp ipv4 Example: RP/0/RSP0/CPU0:router(config)# dhcp ipv4 | Enters DHCP IPv4 configuration submenu. |

| Command or Action | Purpose |
|--|---|
| <p>Step 3</p> <pre>interface <i>type instance</i> relay profile <i>profile-name</i></pre> <p>Example: RP/0/RSP0/CPU0:router(config-dhcpv4)# interface gigabitethernet 0/0/0/0 relay profile client</p> | <p>Attaches a relay profile to an interface.</p> |
| <p>Step 4</p> <pre>end or commit</pre> <p>Example: RP/0/RSP0/CPU0:router(config-if)# end or RP/0/RSP0/CPU0:router(config)# commit</p> | <p>Saves configuration changes.</p> <ul style="list-style-type: none"> • When you issue the end command, the system prompts you to commit changes: Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]: <ul style="list-style-type: none"> – Entering yes saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode. – Entering no exits the configuration session and returns the router to EXEC mode without committing the configuration changes. – Entering cancel leaves the router in the current configuration session without exiting or committing the configuration changes. • Use the commit command to save the configuration changes to the running configuration file and remain within the configuration session. |

Disabling DHCP Relay on an Interface

This task describes how to disable the DHCP relay on an interface by assigning the none profile to the interface.

SUMMARY STEPS

1. **configure**
2. **dhcp ipv4**
3. **interface** *type name* **none**
4. **end**
or
commit

DETAILED STEPS

| | Command or Action | Purpose |
|--------|---|---|
| Step 1 | configure Example: RP/0/RSP0/CPU0:router# configure | Enters global configuration mode. |
| Step 2 | dhcp ipv4 Example: RP/0/RSP0/CPU0:router(config)# dhcp ipv4 | Enters DHCP IPv4 configuration submenu. |

| | Command or Action | Purpose |
|--------|---|--|
| Step 3 | <p>interface <i>type instance none</i></p> <p>Example: RP/0/RSP0/CPU0:router(config-dhcpv4-relay-profile)# interface gigabitethernet 0/1/4/1 none</p> | Disables the DHCP relay on the interface. |
| Step 4 | <p>end or commit</p> <p>Example: RP/0/RSP0/CPU0:router(config)# end or RP/0/RSP0/CPU0:router(config)# commit</p> | <p>Saves configuration changes.</p> <ul style="list-style-type: none"> When you issue the end command, the system prompts you to commit changes: Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]: <ul style="list-style-type: none"> Entering yes saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode. Entering no exits the configuration session and returns the router to EXEC mode without committing the configuration changes. Entering cancel leaves the router in the current configuration session without exiting or committing the configuration changes. Use the commit command to save the configuration changes to the running configuration file and remain within the configuration session. |

Enabling DHCP Relay on a VRF

This task describes how to enable DHCP relay on a VRF.

SUMMARY STEPS

- configure**
- dhcp ipv4**
- vrf** *vrf-name* **relay** *profile profile-name*
- end**
or
commit

DETAILED STEPS

| | Command or Action | Purpose |
|--------|---|--|
| Step 1 | <p>configure</p> <p>Example: RP/0/RSP0/CPU0:router# configure</p> | Enters global configuration mode. |
| Step 2 | <p>dhcp ipv4</p> <p>Example: RP/0/RSP0/CPU0:router(config)# dhcp ipv4</p> | Enters DHCP IPv4 configuration submenu. |
| Step 3 | <p>vrf vrf-name relay profile profile-name</p> <p>Example: RP/0/RSP0/CPU0:router(config-dhcpv4)# vrf default relay profile client</p> | Enables DHCP relay on a VRF. |
| Step 4 | <p>end or commit</p> <p>Example: RP/0/RSP0/CPU0:router(config)# end or RP/0/RSP0/CPU0:router(config)# commit</p> | <p>Saves configuration changes.</p> <ul style="list-style-type: none"> When you issue the end command, the system prompts you to commit changes: Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]: <ul style="list-style-type: none"> Entering yes saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode. Entering no exits the configuration session and returns the router to EXEC mode without committing the configuration changes. Entering cancel leaves the router in the current configuration session without exiting or committing the configuration changes. Use the commit command to save the configuration changes to the running configuration file and remain within the configuration session. |

Configuring the Relay Agent Information Option

This task describes how to configure the DHCP relay agent information option processing capabilities. A DHCP relay agent may receive a message from another DHCP relay agent that already contains relay information. By default, the relay information from the previous relay agent is replaced (using the replace option).

SUMMARY STEPS

1. **configure**
2. **dhcp ipv4**
3. **profile *profile-name* relay**
4. **relay information option**
5. **relay information check**
6. **relay information policy {drop | keep}**
7. **relay information option allow-untrusted**
8. **end**
or
commit

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | configure Example: RP/0/RSP0/CPU0:router# configure | Enters global configuration mode. |
| Step 2 | dhcp ipv4 Example: RP/0/RSP0/CPU0:router(config)# dhcp ipv4 | Enters DHCP IPv4 configuration submode. |
| Step 3 | profile <i>profile-name</i> relay Example: RP/0/RSP0/CPU0:router(config-dhcpv4)# profile client relay | Enters DHCP IPv4 profile relay submode. |

| Command or Action | Purpose |
|--|---|
| <p>Step 4 <code>relay information option</code></p> <p>Example: RP/0/RSP0/CPU0:router(config-dhcpv4-relay-profile)# relay information option</p> | <p>Enables the system to insert the DHCP relay agent information option (option-82 field) in forwarded BOOTREQUEST messages to a DHCP server.</p> <ul style="list-style-type: none"> This option is injected by the relay agent while forwarding client-originated DHCP packets to the server. Servers recognizing this option can use the information to implement IP address or other parameter assignment policies. When replying, the DHCP server echoes the option back to the relay agent. The relay agent removes the option before forwarding the reply to the client. The relay agent information is organized as a single DHCP option that contains one or more suboptions. These options contain the information known by the relay agent. <p>The supported suboptions are:</p> <ul style="list-style-type: none"> Remote ID Circuit ID <p>Note This function is disabled by default.</p> |
| <p>Step 5 <code>relay information check</code></p> <p>Example: RP/0/RSP0/CPU0:router(config-dhcpv4-relay-profile)# relay information check</p> | <p>(Optional) Configures DHCP to check the validity of the relay agent information option in forwarded BOOTREPLY messages. If an invalid message is received, the relay agent drops the message. If a valid message is received, the relay agent removes the relay agent information option field and forwards the packet.</p> <ul style="list-style-type: none"> By default, DHCP does not check the validity of the relay agent information option field in DHCP reply packets, received from the DHCP server. <p>Note Use the relay information check command to reenables this functionality if the functionality has been disabled.</p> |
| <p>Step 6 <code>relay information policy {drop keep}</code></p> <p>Example: RP/0/RSP0/CPU0:router(config)# dhcp relay information policy drop</p> | <p>(Optional) Configures the reforwarding policy for a DHCP relay agent; that is, whether the relay agent will drop or keep the relay information.</p> <p>By default, the DHCP relay agent replaces the relay information option.</p> |

| Command or Action | Purpose |
|---|--|
| <p>Step 7</p> <pre>relay information option allow-untrusted</pre> <p>Example: RP/0/RSP0/CPU0:router(config-dhcpv4-relay-profile)# relay information option allow-untrusted </p> | <p>(Optional) Configures the DHCP IPv4 Relay not to discard BOOTREQUEST packets that have an existing relay information option and the giaddr set to zero.</p> |
| <p>Step 8</p> <pre>end or commit</pre> <p>Example: RP/0/RSP0/CPU0:router(config)# end or RP/0/RSP0/CPU0:router(config)# commit </p> | <p>Saves configuration changes.</p> <ul style="list-style-type: none"> When you issue the end command, the system prompts you to commit changes: <pre>Uncommitted changes found, commit them before exiting (yes/no/cancel)? [cancel]:</pre> <ul style="list-style-type: none"> Entering yes saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode. Entering no exits the configuration session and returns the router to EXEC mode without committing the configuration changes. Entering cancel leaves the router in the current configuration session without exiting or committing the configuration changes. Use the commit command to save the configuration changes to the running configuration file and remain within the configuration session. |

Configuring Relay Agent Giaddr Policy

This task describes how to configure the DHCP relay agent's processing capabilities for received BOOTREQUEST packets that already contain a nonzero giaddr attribute.

SUMMARY STEPS

1. **configure**
2. **dhcp ipv4**
3. **profile *profile-name* relay**
4. **giaddr policy {replace | drop}**
5. **end**
or
commit

DETAILED STEPS

| | Command or Action | Purpose |
|--------|--|--|
| Step 1 | configure Example: RP/0/RSP0/CPU0:router# configure | Enters global configuration mode. |
| Step 2 | dhcp ipv4 Example: RP/0/RSP0/CPU0:router(config)# dhcp ipv4 | Enables the DHCP IPv4 configuration submode. |
| Step 3 | profile profile-name relay Example: RP/0/RSP0/CPU0:router(config-dhcpv4)# profile client relay | Enables profile relay submode. |

| | Command or Action | Purpose |
|--------|--|--|
| Step 4 | <pre>giaddr policy {replace drop}</pre> <p>Example: RP/0/RSP0/CPU0:router(config-dhcpv4-relay-profile)# giaddr policy drop</p> | <p>Specifies the giaddr policy.</p> <ul style="list-style-type: none"> replace—Replaces the existing giaddr value with a value that it generates. drop—Drops the packet that has an existing nonzero giaddr value. <p>By default, the DHCP relay agent keeps the existing giaddr value.</p> <ul style="list-style-type: none"> |
| Step 5 | <pre>end or commit</pre> <p>Example: RP/0/RSP0/CPU0:router(config)# end OR RP/0/RSP0/CPU0:router(config)# commit</p> | <p>Saves configuration changes.</p> <ul style="list-style-type: none"> When you issue the end command, the system prompts you to commit changes: <pre>Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]:</pre> <ul style="list-style-type: none"> Entering yes saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode. Entering no exits the configuration session and returns the router to EXEC mode without committing the configuration changes. Entering cancel leaves the router in the current configuration session without exiting or committing the configuration changes. Use the commit command to save the configuration changes to the running configuration file and remain within the configuration session. |

Configuration Examples for DHCP Relay Agent

This section provides the following configuration examples:

- [DHCP Relay Profile: Example, page 102](#)
- [DHCP Relay on an Interface: Example, page 102](#)
- [DHCP Relay on a VRF: Example, page 102](#)
- [Relay Agent Information Option Support: Example, page 102](#)
- [Relay Agent Giaddr Policy: Example, page 102](#)

DHCP Relay Profile: Example

The following example shows how to configure the Cisco IOS XR relay profile:

```
dhcp ipv4
  profile client relay
    helper-address vrf foo 10.10.1.1
  !
  ! ...
```

DHCP Relay on an Interface: Example

The following example shows how to enable the DHCP relay agent on an interface:

```
dhcp ipv4
  interface gigabitethernet 0/1/1/0 relay profile client
  !
```

DHCP Relay on a VRF: Example

The following example shows how to enable the DHCP relay agent on a VRF:

```
dhcp ipv4
  vrf default relay profile client
  !
```

Relay Agent Information Option Support: Example

The following example shows how to enable the relay agent and the insertion and removal of the DHCP relay information option:

```
dhcp ipv4
  profile client relay
  relay information option
  !
  !
```

Relay Agent Giaddr Policy: Example

The following example shows how to configure relay agent giaddr policy:

```
dhcp ipv4
  profile client relay
  giaddr policy drop
  !
  !
```

Implementing DHCP Snooping on Cisco ASR 9000 Series Routers

- [Prerequisites for Configuring DHCP Snooping, page 103](#)

- [Information about DHCP Snooping, page 104](#)
- [How to Configure DHCP Snooping, page 106](#)
- [Configuration Examples for DHCP Snooping, page 113](#)

Prerequisites for Configuring DHCP Snooping

The following prerequisites are required to configure DHCP IPv4 snooping:

- You must be in a user group associated with a task group that includes the proper task IDs. The command reference guides include the task IDs required for each command. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.
- A Cisco ASR 9000 Series Router running Cisco IOS XR software.
- A configured and running DHCP client and DHCP server.

DETAILED STEPS

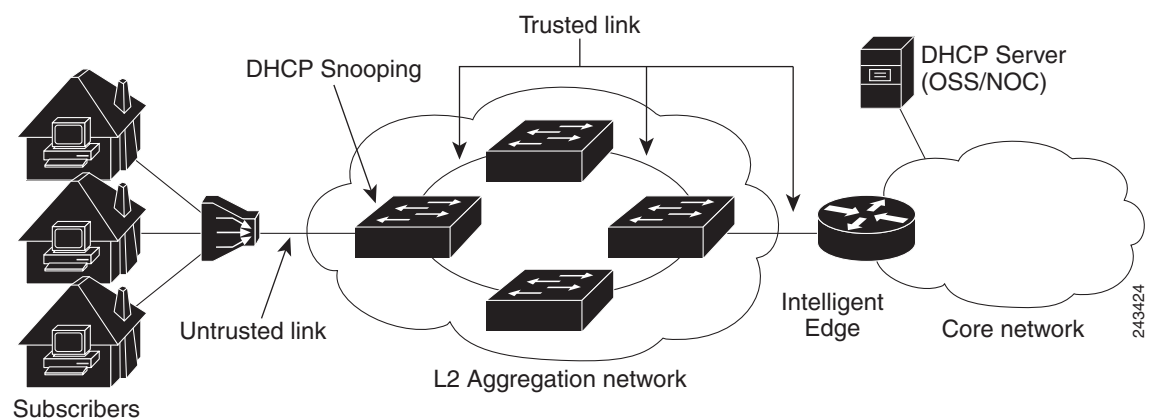
Information about DHCP Snooping

| | Command or Action | Purpose |
|--------|--|---|
| Step 1 | configure Example: RP/0//CPU0:router# configure | Enters global configuration mode. |
| Step 2 | dhcp ipv4 Example: RP/0//CPU0:router(config)# dhcp ipv4 | Configures DHCP IPv4 mode. |
| Step 3 | profile profile name relay Example: RP/0//CPU0:router(config-dhcpv4)# profile client relay | Enables profile relay mode. |
| Step 4 | broadcast-flag policy check Example: RP/0//CPU0:router(config-dhcpv4-relay-profile)# broadcast-flag policy check | Enables checking of the broadcast flag in packets. |
| Step 5 | end OR commit Example: RP/0//CPU0:router(config)# end OR RP/0//CPU0:router(config)# commit | Saves configuration changes. <ul style="list-style-type: none"> When you issue the end command, the system prompts you to commit changes: <pre>Uncommitted changes found, commit them before exiting (yes/no/cancel)? [cancel]:</pre> <ul style="list-style-type: none"> Entering yes saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode. Entering no exits the configuration session and returns the router to EXEC mode without committing the configuration changes. Entering cancel leaves the router in the current configuration session without exiting or committing the configuration changes. Use the commit command to save the configuration changes to the running configuration file and remain within the configuration session. |

DHCP Snooping features are focused on the edge of the aggregation network. Security features are applied at the first point of entry for subscribers. Relay agent information option information is used to identify the subscriber's line, which is either the DSL line to the subscriber's home or the first port in the aggregation network.

The central concept for DHCP snooping is that of trusted and untrusted links. A trusted link is one providing secure access for traffic on that link. On an untrusted link, subscriber identity and subscriber traffic cannot be determined. DHCP snooping runs on untrusted links to provide subscriber identity. [Figure 3](#) shows an aggregation network. The link from the DSLAM to the aggregation network is untrusted and is the point of presence for DHCP snooping. The links connecting the switches in the aggregation network and the link from the aggregation network to the intelligent edge is considered trusted.

Figure 3 DHCP Snooping in an Aggregation Network



Trusted and Untrusted Ports

On trusted ports, DHCP BOOTREQUEST packets are forwarded by DHCP snooping. The client's address lease is not tracked and the client is not bound to the port. DHCP BOOTREPLY packets are forwarded.

When the first DHCP BOOTREQUEST packet from a client is received on an untrusted port, DHCP snooping binds the client to the bridge port and tracks the client's address lease. When that address lease expires, the client is deleted from the database and is unbound from the bridge port. Packets from this client received on this bridge port are processed and forwarded as long as the binding exists. Packets that are received on another bridge port from this client are dropped while the binding exists. DHCP snooping only forwards DHCP BOOTREPLY packets for this client on the bridge port that the client is bound to. DHCP BOOTREPLY packets that are received on untrusted ports are not forwarded.

DHCP Snooping in a Bridge Domain

To enable DHCP snooping in a bridge domain, there must be at least two profiles, a trusted profile and an untrusted profile. The untrusted profile is assigned to the client-facing ports, and the trusted profile is assigned to the server-facing ports. In most cases, there are many client-facing ports and few server-facing ports. The simplest example is two ports, a client-facing port and a server-facing port, with an untrusted profile explicitly assigned to the client-facing port and a trusted profile assigned to the server-facing port.

Assigning Profiles to a Bridge Domain

Because there are normally many client-facing ports and a small number of server-facing ports, the operator assigns the untrusted profile to the bridge domain. This configuration effectively assigns an untrusted profile to every port in the bridge domain. This action saves the operator from explicitly assigning the untrusted profile to all of the client-facing ports. Because there also must be server-facing ports that have trusted DHCP snooping profiles, in order for DHCP snooping to function properly, this untrusted DHCP snooping profile assignment is overridden to server-facing ports by specifically configuring trusted DHCP snooping profiles on the server-facing ports. For ports in the bridge domain that do not require DHCP snooping, all should have the **none** profile assigned to them to disable DHCP snooping on those ports.

Relay Information Options

You can configure a DHCP snooping profile to insert the relay information option (option 82) into DHCP client packets only when it is assigned to a client port. The **relay information option allow-untrusted** command addresses what to do with DHCP client packets when there is a null giaddr and a relay-information option already in the client packet when it is received. This is a different condition than a DHCP snooping trusted/untrusted port. The **relay information option allow-untrusted** command determines how the DHCP snooping application handles untrusted relay information options.

How to Configure DHCP Snooping

This section contains the following tasks:

- [Enabling DHCP Snooping in a Bridge Domain, page 106](#)
- [Disabling DHCP Snooping on a Specific Bridge Port, page 109](#)
- [Using the Relay Information Option, page 112](#)

Enabling DHCP Snooping in a Bridge Domain

The following configuration creates two ports, a client-facing port and a server-facing port. In Step 1 through Step 8, an untrusted DHCP snooping profile is assigned to the client bridge port and trusted DHCP snooping profile is assigned to the server bridge port. In Step 9 through Step 18, an untrusted DHCP snooping profile is assigned to the bridge domain and trusted DHCP snooping profiles are assigned to server bridge ports.

SUMMARY STEPS

1. **configure**
2. **profile *profile-name* snoop**
3. **exit**
4. **dhcp ipv4**
5. **profile *profile-name* snoop**
6. **trusted**
7. **exit**
8. **l2vpn**

9. **bridge group** *group-name*
10. **bridge-domain** *bridge-domain-name*
11. **interface gigabitethernet** *type instance*
12. **dhcp ipv4 snoop profile** *profile-name*
13. **interface** *type instance*
14. **dhcp ipv4 snoop profile** *profile-name*
15. **exit**
16. **exit**
17. **end**
or
commit

DETAILED STEPS

| | Command or Action | Purpose |
|--------|--|--|
| Step 1 | configure Example: RP/0/RSP0/CPU0:router# configure | Enters global configuration mode. |
| Step 2 | dhcp ipv4 Example: RP/0/RSP0/CPU0:router(config)# dhcp ipv4 | Enters DHCP IPv4 profile configuration submode. |
| Step 3 | profile <i>untrusted-profile-name</i> snoop Example: RP/0/RSP0/CPU0:router(config-dhcpv4)# profile untrustedClientProfile snoop | Configures an untrusted DHCP snooping profile for the client port. |
| Step 4 | exit Example: RP/0/RSP0/CPU0:router(config-dhcpv4)# exit | Exits DHCP IPv4 profile configuration mode. |
| Step 5 | dhcp ipv4 Example: RP/0/RSP0/CPU0:router(config)# dhcp ipv4 | Enables DHCP for IPv4 and enters DHCP IPv4 profile configuration mode. |
| Step 6 | profile <i>profile-name</i> snoop Example: RP/0/RSP0/CPU0:router(config-dhcpv4)# profile trustedServerProfile snoop | Configures a trusted DHCP snooping profile for the server port. |

| | Command or Action | Purpose |
|---------|--|---|
| Step 7 | trusted Example: RP/0/RSP0/CPU0:router(config-dhcv4)# trusted | Configures a DHCP snoop profile to be trusted. |
| Step 8 | exit Example: RP/0/RSP0/CPU0:router(config-dhcv4)# exit | Exits DHCP IPv4 profile configuration mode. |
| Step 9 | l2vpn Example: RP/0/RSP0/CPU0:router(config)# l2vpn | Enters l2vpn configuration mode. |
| Step 10 | bridge group <i>group-name</i> Example: RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group ccc | Creates a bridge group to contain bridge domains and enters l2vpn bridge group configuration submode. |
| Step 11 | bridge-domain <i>bridge-domain-name</i> Example: RP/0/RSP0/CPU0:router(config-l2vpn-bg)# bridge-domain ddd | Establishes a bridge domain. |
| Step 12 | interface <i>type instance</i> Example: RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# interface gigabitethernet 0/1/0/0 | Identifies an interface. |
| Step 13 | dhcp ipv4 snoop profile <i>untrusted-profile-name</i> Example: RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-ac)# dhcp ipv4 snoop profile untrustedClientProfile | Attaches an untrusted DHCP snoop profile to the bridge port. |
| Step 14 | interface <i>type instance</i> Example: RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-ac)# gigabitethernet 0/1/0/1 | Identifies an interface. |
| Step 15 | dhcp ipv4 snoop profile <i>trusted-profile-name</i> Example: RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-ac)# dhcp ipv4 snoop profile trustedServerProfile | Attaches a trusted DHCP snoop profile to the bridge port. |
| Step 16 | exit Example: RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-ac)# exit | Exits the l2vpn bridge group bridge-domain interface configuration submode. |

| | Command or Action | Purpose |
|---------|---|---|
| Step 17 | <code>exit</code> Example: RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# exit | Exits the l2vpn bridge group bridge-domain configuration submode. |
| Step 18 | <code>end</code> OR <code>commit</code> Example: RP/0/RSP0/CPU0:router(config-l2vpn-bg)# end OR RP/0/RSP0/CPU0:router(config-l2vpn-bg)# commit | Saves configuration changes. <ul style="list-style-type: none"> When you issue the end command, the system prompts you to commit changes: Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]: <ul style="list-style-type: none"> Entering yes saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode. Entering no exits the configuration session and returns the router to EXEC mode without committing the configuration changes. Entering cancel leaves the router in the current configuration session without exiting or committing the configuration changes. Use the commit command to save the configuration changes to the running configuration file and remain within the configuration session. |

Disabling DHCP Snooping on a Specific Bridge Port

The following configuration enables DHCP to snoop packets on all bridge ports in the bridge domain ISP1 except for bridge port GigabitEthernet 0/1/0/1 and GigabitEthernet 0/1/0/2. DHCP snooping is disabled on bridge port GigabitEthernet 0/1/0/1. Bridge port GigabitEthernet 0/1/0/2 is the trusted port that connects to the server. In this example, no additional features are enabled, so only DHCP snooping is running.

SUMMARY STEPS

- `configure`
- `l2vpn`
- `bridge group group-name`
- `bridge-domain bridge-domain-name`
- `dhcp ipv4 snoop profile profile-name`
- `interface type instance`
- `dhcp ipv4 none`
- `interface type instance`

9. **dhcp ipv4 snoop profile** *profile-name*
10. **exit**
11. **exit**
12. **end**
or
commit

DETAILED STEPS

| | Command or Action | Purpose |
|--------|---|---|
| Step 1 | configure Example: RP/0/RSP0/CPU0:router# configure | Enters global configuration mode. |
| Step 2 | l2vpn Example: RP/0/RSP0/CPU0:router(config)# l2vpn | Enters l2vpn configuration submode. |
| Step 3 | bridge group <i>group-name</i> Example: RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group GRP1 | Creates a bridge group to contain bridge domains and enters l2vpn bridge group configuration submode. |
| Step 4 | bridge-domain <i>bridge-domain-name</i> Example: RP/0/RSP0/CPU0:router(config-l2vpn-bg)# bridge-domain ISP1 | Establishes a bridge domain and enters l2vpn bridge group bridge-domain configuration submode. |
| Step 5 | dhcp ipv4 snoop profile <i>profile-name</i> Example: RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# dhcp ipv4 snoop profile untrustedClientProfile | Attaches the untrusted DHCP snooping profile to the bridge domain. |
| Step 6 | interface <i>type instance</i> Example: RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# interface gigabitethernet 0/1/0/1 | Identifies an interface and enters l2vpn bridge group bridge-domain interface configuration submode. |
| Step 7 | dhcp ipv4 none Example: RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-if)# dhcp ipv4 none | Disables DHCP snooping on the port. |

| | Command or Action | Purpose |
|---------|--|--|
| Step 8 | <p>interface <i>type instance</i></p> <p>Example: RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# interface gigabitethernet 0/1/0/2</p> | Identifies an interface and enters l2vpn bridge group bridge-domain interface configuration submenu. |
| Step 9 | <p>dhcp ipv4 snoop profile <i>profile-name</i></p> <p>Example: RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# dhcp ipv4 snoop profile trustedServerProfile</p> | Attaches the trusted DHCP snooping profile to a port. |
| Step 10 | <p>exit</p> <p>Example: RP/0/RSP0/CPU0:router (config-l2vpn-bd-bg)# exit</p> | Exits l2vpn bridge-domain bridge group interface configuration submenu. |
| Step 11 | <p>exit</p> <p>Example: RP/0/RSP0/CPU0:router (config-l2vpn-bg)# exit</p> | Exits l2vpn bridge-domain submenu. |
| Step 12 | <p>end OR commit</p> <p>Example: RP/0/RSP0/CPU0:router(config-l2vpn)# end OR RP/0/RSP0/CPU0:router(config-l2vpn)# commit</p> | <p>Saves configuration changes.</p> <ul style="list-style-type: none"> When you issue the end command, the system prompts you to commit changes: Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]: <ul style="list-style-type: none"> Entering yes saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode. Entering no exits the configuration session and returns the router to EXEC mode without committing the configuration changes. Entering cancel leaves the router in the current configuration session without exiting or committing the configuration changes. Use the commit command to save the configuration changes to the running configuration file and remain within the configuration session. |

Using the Relay Information Option

This task show how to use the relay information commands to insert the relay information option (option 82) into DHCP client packets and forward DHCP packets with untrusted relay information options.

SUMMARY STEPS

1. **configure**
2. **dhcp ipv4**
3. **profile *profile-name* snoop**
4. **relay information option**
5. **relay information option allow-untrusted**
6. **end**
or
commit

DETAILED STEPS

| | Command or Action | Purpose |
|--------|---|--|
| Step 1 | configure Example: RP/0/RSP0/CPU0:router# configure | Enters global configuration mode. |
| Step 2 | dhcp ipv4 Example: RP/0/RSP0/CPU0:router(config)# dhcp ipv4 | Enters DHCP IPv4 profile configuration submode. |
| Step 3 | profile <i>profile-name</i> snoop Example: RP/0/RSP0/CPU0:router(config-dhcpv4)# profile untrustedClientProfile snoop | Configures an untrusted DHCP snooping profile for the client port. |
| Step 4 | relay information option Example: RP/0/RSP0/CPU0:router(config-dhcpv4-snoop-profile)# relay information option | Enables the system to insert the DHCP relay information option field in forwarded BOOTREQUEST messages to a DHCP server. |

| | Command or Action | Purpose |
|--------|--|--|
| Step 5 | <pre>relay information option allow-untrusted</pre> <p>Example: RP/0/RSP0/CPU0:router(config-dhcpv4-snoop-profile)# relay information option allow-untrusted </p> | Configures DHCP IPv4 relay not to discard BOOTREQUEST packets that have an existing relay information option and the giaddr set to zero. |
| Step 6 | <pre>end or commit</pre> <p>Example: RP/0/RSP0/CPU0:router(config-dhcpv4-snoop-profile)# end or RP/0/RSP0/CPU0:router(config-dhcpv4-snoop-profile)# commit </p> | <p>Saves configuration changes.</p> <ul style="list-style-type: none"> When you issue the end command, the system prompts you to commit changes: Uncommitted changes found, commit them before exiting(yes/no/cancel)? [cancel]: <ul style="list-style-type: none"> Entering yes saves configuration changes to the running configuration file, exits the configuration session, and returns the router to EXEC mode. Entering no exits the configuration session and returns the router to EXEC mode without committing the configuration changes. Entering cancel leaves the router in the current configuration session without exiting or committing the configuration changes. Use the commit command to save the configuration changes to the running configuration file and remain within the configuration session. |

Configuration Examples for DHCP Snooping

This section provides the following configuration examples:

- [Assigning a DHCP Profile to a Bridge Domain: Example, page 113](#)
- [Disabling DHCP Snooping on a Specific Bridge Port: Example, page 114](#)
- [Configuring a DHCP Profile for Trusted Bridge Ports: Example, page 114](#)
- [Configuring an Untrusted Profile on a Bridge Domain: Example, page 114](#)
- [Configuring a Trusted Bridge Port: Example, page 114](#)

Assigning a DHCP Profile to a Bridge Domain: Example

The following example shows how to enable DHCP snooping in a bridge domain:

```
l2vpn
bridge group GRP1
bridge-domain ISP1
dhcp ipv4 profile untrustedClientProfile snoop
```

Disabling DHCP Snooping on a Specific Bridge Port: Example

The following example shows how to disable DHCP snooping on a specific bridge port:

```
interface gigabitethernet 0/1/0/1
  dhcp ipv4 none
```

Configuring a DHCP Profile for Trusted Bridge Ports: Example

The following example shows how to configure a DHCP profile for trusted bridge ports:

```
dhcp ipv4 profile trustedServerProfile snoop
  trusted
```

Configuring an Untrusted Profile on a Bridge Domain: Example

The following example shows how to attach a profile to a bridge domain and disable snooping on a bridge port.

```
l2vpn
  bridge group GRP1
  bridge-domain ISP1
  dhcp ipv4 profile untrustedClientProfile snoop
  interface gigabitethernet 0/1/0/1
  dhcp ipv4 none
```

Configuring a Trusted Bridge Port: Example

The following example shows how to assign a trusted DHCP snooping profile to a bridge port:

```
l2vpn
  bridge group GRP1
  bridge-domain ISP1
  interface gigabitethernet 0/1/0/2
  dhcp ipv4 profile trustedServerProfile snoop
```

Additional References

The following sections provide references related to implementing the DHCP relay agent and DHCP snooping features.

Related Documents

| Related Topic | Document Title |
|----------------------------|--|
| Cisco IOS XR DHCP commands | <i>DHCP Commands on Cisco ASR 9000 Series Routers</i> module in the <i>Cisco ASR 9000 Series Aggregation Services Router IP Addresses and Services Command Reference</i> |

| Related Topic | Document Title |
|---|---|
| Cisco ASR 9000 Series Router getting started material | <i>Cisco ASR 9000 Series Aggregation Services Router Getting Started Guide</i> |
| Information about user groups and task IDs | <i>Configuring AAA Services on Cisco IOS XR Software</i> module in the <i>Cisco ASR 9000 Series Aggregation Services Router System Security Configuration Guide</i> |

Standards

| Standards | Title |
|---|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | — |

MIBs

| MIBs | MIBs Link |
|------|--|
| — | To locate and download MIBs using Cisco IOS XR software, use the Cisco MIB Locator found at the following URL and choose a platform under the Cisco Access Products menu: http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml |

RFCs

| RFC | Title |
|----------|--|
| RFC 2131 | <i>Dynamic Host Configuration Protocol</i> |

Technical Assistance

| Description | Link |
|---|---|
| The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content. | http://www.cisco.com/techsupport |

