CONFIGURATION GUIDE

Ruckus FastIron DHCP Configuration Guide, 08.0.61

Supporting FastIron Software Release 08.0.61

Part Number: 53-1005199-06
Publication Date: 25 January 2019

Copyright, Trademark and Proprietary Rights Information

© 2019 ARRIS Enterprises LLC. All rights reserved.

No part of this content may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from ARRIS International plc and/or its affiliates ("ARRIS"). ARRIS reserves the right to revise or change this content from time to time without obligation on the part of ARRIS to provide notification of such revision or change.

Export Restrictions

These products and associated technical data (in print or electronic form) may be subject to export control laws of the United States of America. It is your responsibility to determine the applicable regulations and to comply with them. The following notice is applicable for all products or technology subject to export control:

These items are controlled by the U.S. Government and authorized for export only to the country of ultimate destination for use by the ultimate consignee or end-user(s) herein identified. They may not be resold, transferred, or otherwise disposed of, to any other country or to any person other than the authorized ultimate consignee or end-user(s), either in their original form or after being incorporated into other items, without first obtaining approval from the U.S. government or as otherwise authorized by U.S. law and regulations.

Disclaimer

THIS CONTENT AND ASSOCIATED PRODUCTS OR SERVICES ("MATERIALS"), ARE PROVIDED "AS IS" AND WITHOUT WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED. TO THE FULLEST EXTENT PERMISSIBLE PURSUANT TO APPLICABLE LAW, ARRIS DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT, FREEDOM FROM COMPUTER VIRUS, AND WARRANTIES ARISING FROM COURSE OF DEALING OR COURSE OF PERFORMANCE. ARRIS does not represent or warrant that the functions described or contained in the Materials will be uninterrupted or error-free, that defects will be corrected, or are free of viruses or other harmful components. ARRIS does not make any warranties or representations regarding the use of the Materials in terms of their completeness, correctness, accuracy, adequacy, usefulness, timeliness, reliability or otherwise. As a condition of your use of the Materials, you warrant to ARRIS that you will not make use thereof for any purpose that is unlawful or prohibited by their associated terms of use.

Limitation of Liability

IN NO EVENT SHALL ARRIS, ARRIS AFFILIATES, OR THEIR OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS, LICENSORS AND THIRD PARTY PARTNERS, BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER, EVEN IF ARRIS HAS BEEN PREVIOUSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, WHETHER IN AN ACTION UNDER CONTRACT, TORT, OR ANY OTHER THEORY ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIALS. Because some jurisdictions do not allow limitations on how long an implied warranty lasts, or the exclusion or limitation of liability for consequential or incidental damages, some of the above limitations may not apply to you.

Trademarks

ARRIS, the ARRIS logo, Ruckus, Ruckus Wireless, Ruckus Networks, Ruckus logo, the Big Dog design, BeamFlex, ChannelFly, EdgeIron, FastIron, HyperEdge, ICX, IronPoint, OPENG, SmartCell, Unleashed, Xclaim, ZoneFlex are trademarks of ARRIS International plc and/or its affiliates. Wi-Fi Alliance, Wi-Fi, the Wi-Fi logo, the Wi-Fi CERTIFIED logo, Wi-Fi Protected Access (WPA), the Wi-Fi Protected Setup logo, and WMM are registered trademarks of Wi-Fi Alliance. Wi-Fi Protected Setup™, Wi-Fi Multimedia™, and WPA2™ are trademarks of Wi-Fi Alliance. All other trademarks are the property of their respective owners.

Contents

Preface **7**
- Document Conventions 7
  - Notes, Cautions, and Warnings 7
- Command Syntax Conventions 8
- Document Feedback 8
- Ruckus Product Documentation Resources 8
- Online Training Resources 9
- Contacting Ruckus Customer Services and Support 9
  - What Support Do I Need? 9
  - Open a Case 9
  - Self-Service Resources 9

About This Document **11**
- Supported hardware and software 11
- What's new in this document 11

Dynamic Host Configuration Protocol Overview **13**
- DHCP overview 13

DHCP Clients **15**
- DHCP client 15
  - DHCP over default Virtual Ethernet port (Layer 3 devices) 16
  - Default Virtual Ethernet port creation (Layer 3 devices) 16
  - DHCP client in continuous discovery mode (Layer 2 and Layer 3 devices) 17
  - DHCP client as a new device 17
  - DHCP client behavior after reboot 18
- BootP and DHCP relay parameters 19
- Configuring an IP helper address 19
- Configuring the BOOTP and DHCP reply source address 20
- Changing the IP address used for stamping BootP and DHCP requests 20
- Changing the maximum number of hops to a BootP relay server 21
- DHCP auto-provisioning 21
- Auto-provisioning using the bootfile.bin option 22
- DHCP auto-provisioning using the manifest file option 23
- DHCP auto-provisioning options 24
- Disabling or re-enabling the DHCP client 24
- DHCP auto-provisioning on Layer 2 and Layer 3 devices 25
  - Scenario 1: DHCP auto-provisioning on a Layer 3 device 25
  - Scenario 2: DHCP auto-provisioning with a TFTP server in a different network 26
  - Scenario 3: DHCP client connected through a DHCP snooping device 27
  - Scenario 4: DHCP client option 12 27
  - Scenario 5: DHCP auto-provisioning on a Layer 2 device 28
- Configuration notes and feature limitations for DHCP auto-provisioning 28
  - High Availability and 802.1BR considerations 29
  - Upgrade considerations 29
  - How DHCP client-based auto-provisioning and flash image update works 30
  - Validating the IP address and lease negotiation 30
  - Flash image download and update 30

Auto-provisioning download and update 31
Disabling or re-enabling auto-provisioning 31
Dynamic DHCP options configuration processing 31
Verifying dynamic DHCP options for a switch 33
Verifying dynamic DHCP options for a router 35

DHCP Servers 37
DHCP Servers 37
Configuration considerations for DHCP servers 38
Configuring the DHCP server and creating an address pool 39
Default DHCP server settings 42
DHCP server options 42
Disabling or re-enabling the DHCP server on the management port 43
Setting the wait time for ARP ping response 44
DHCP option 82 support 44
Enabling relay agent echo (option 82) 44
Configuring the IP address of the DHCP server 45
Configuring the boot image 45
Deploying an address pool configuration to the server 45
Specifying default routers available to the client 46
Specifying DNS servers available to the client 46
Configuring the domain name for the client 46
Configuring the lease duration for the address pool 47
Specifying addresses to exclude from the address pool 47
Configuring the NetBIOS server for DHCP clients 47
Configuring the subnet and mask of a DHCP address pool 48
Configuring a next-bootstrap server 48
Configuring the TFTP server 48
Configuring a vendor type and configuration value for a DHCP client 49
Configuring X Window System Display Manager IP addresses (option 49) 49
Configuring vendor details and vendor specific information (option 43 and option 60) 50
Enabling static IP to MAC address mapping 51
Configuring Avaya IP telephony (options 176 and 242) 51
Configuring WPAD (option 252) 52
Displaying DHCP server information 53

DHCPv4 57
DHCPv4 overview 57
DHCP Assist configuration 57
How DHCP Assist works 58
Configuring DHCP Assist 60
Dynamic ARP Inspection overview 61
ARP poisoning 61
How Dynamic ARP Inspection works 62
Configuration notes and feature limitations for DAI 63
Configuring Dynamic ARP Inspection 63
Enabling or disabling DAI syslog messages 64
Displaying ARP information 65
Configuring DAI to support Multi-VRF 67
Enabling trust on a port for a specific VRF 67
DHCP snooping 68

How DHCP snooping works....68
System reboot and the binding database....69
Configuration notes and feature limitations for DHCP snooping....69
Configuring DHCP snooping....70
Displaying DHCPv4 snooping information....71
Configuring DHCPv4 snooping for Multi-VRF....72
DHCP relay agent information and option 82 insertion....73
Configuration notes for DHCP option 82....74
DHCP option 82 sub-options....75
DHCP option 82 configuration....76
IP Source Guard....79
Configuration notes and feature limitations for IP Source Guard....80
Enabling IP Source Guard on a port or range of ports....81
Defining static IP source bindings....82
Enabling IP Source Guard per-port-per-VLAN....82
Enabling IP source guard on a VLAN....83
Enabling IP Source Guard on a VE....83
Enabling IP Source Guard on a Multi-VRF instance....84
Displaying learned IP addresses....85
DHCPv6....87
DHCPv6 overview....87
DHCP relay agent for IPv6....87
Configuring a DHCPv6 relay agent....87
DHCPv6 relay agent include options....88
Specifying the IPv6 DHCP relay include options....89
DHCPv6 Relay Agent Prefix Delegation Notification....89
DHCPv6 Relay Agent Prefix Delegation Notification limitations....90
Upgrade and downgrade considerations....91
Configuring DHCPv6 Relay Agent Prefix Delegation Notification....91
Enabling DHCPv6 Relay Agent Prefix Delegation Notification on an interface....91
Assigning the administrative distance to DHCPv6 static routes....92
Displaying DHCPv6 relay agent and prefix delegation information....92
Clearing the DHCPv6 delegated prefixes and packet counters....94
DHCPv6 snooping....94
How DHCPv6 snooping works....94
Configuration notes and feature limitations for DHCPv6 snooping....95
Configuring DHCPv6 snooping....96
Configuring DHCPv6 snooping for Multi-VRF....97
Displaying DHCPv6 snooping information....98

Preface

- Document Conventions 7
- Command Syntax Conventions 8
- Document Feedback 8
- Ruckus Product Documentation Resources 8
- Online Training Resources 9
- Contacting Ruckus Customer Services and Support 9

Document Conventions

The following table lists the text conventions that are used throughout this guide.

TABLE 1 Text Conventions

Convention	Description	Example
`monospace`	Identifies command syntax examples	`device(config)# interface ethernet 1/1/6`
bold	User interface (UI) components such as screen or page names, keyboard keys, software buttons, and field names	On the **Start** menu, click **All Programs**.
italics	Publication titles	Refer to the *Ruckus Small Cell Release Notes* for more information.

Notes, Cautions, and Warnings

Notes, cautions, and warning statements may be used in this document. They are listed in the order of increasing severity of potential hazards.

NOTE
A NOTE provides a tip, guidance, or advice, emphasizes important information, or provides a reference to related information.

ATTENTION
An ATTENTION statement indicates some information that you must read before continuing with the current action or task.

CAUTION
A CAUTION statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.

DANGER
A DANGER statement indicates conditions or situations that can be potentially lethal or extremely hazardous to you. Safety labels are also attached directly to products to warn of these conditions or situations.

Command Syntax Conventions

Bold and italic text identify command syntax components. Delimiters and operators define groupings of parameters and their logical relationships.

Convention	Description
bold text	Identifies command names, keywords, and command options.
italic text	Identifies a variable.
[ ]	Syntax components displayed within square brackets are optional.
	Default responses to system prompts are enclosed in square brackets.
{ **x** | **y** | **z** }	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
x | **y**	A vertical bar separates mutually exclusive elements.
< >	Nonprinting characters, for example, passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, *member*[*member*...].
\	Indicates a "soft" line break in command examples. If a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

Document Feedback

Ruckus is interested in improving its documentation and welcomes your comments and suggestions.

You can email your comments to Ruckus at ruckus-docs@arris.com.

When contacting us, include the following information:

- Document title and release number
- Document part number (on the cover page)
- Page number (if appropriate)

For example:

- Ruckus SmartZone Upgrade Guide, Release 5.0
- Part number: 800-71850-001 Rev A
- Page 7

Ruckus Product Documentation Resources

Visit the Ruckus website to locate related documentation for your product and additional Ruckus resources.

Release Notes and other user documentation are available at https://support.ruckuswireless.com/documents. You can locate the documentation by product or perform a text search. Access to Release Notes requires an active support contract and a Ruckus Support Portal user account. Other technical documentation content is available without logging in to the Ruckus Support Portal.

White papers, data sheets, and other product documentation are available at https://www.ruckuswireless.com.

Online Training Resources

To access a variety of online Ruckus training modules, including free introductory courses to wireless networking essentials, site surveys, and Ruckus products, visit the Ruckus Training Portal at https://training.ruckuswireless.com.

Contacting Ruckus Customer Services and Support

The Customer Services and Support (CSS) organization is available to provide assistance to customers with active warranties on their Ruckus products, and customers and partners with active support contracts.

For product support information and details on contacting the Support Team, go directly to the Ruckus Support Portal using https://support.ruckuswireless.com, or go to https://www.ruckuswireless.com and select **Support**.

What Support Do I Need?

Technical issues are usually described in terms of priority (or severity). To determine if you need to call and open a case or access the self-service resources, use the following criteria:

- Priority 1 (P1)—Critical. Network or service is down and business is impacted. No known workaround. Go to the **Open a Case** section.
- Priority 2 (P2)—High. Network or service is impacted, but not down. Business impact may be high. Workaround may be available. Go to the **Open a Case** section.
- Priority 3 (P3)—Medium. Network or service is moderately impacted, but most business remains functional. Go to the **Self-Service Resources** section.
- Priority 4 (P4)—Low. Requests for information, product documentation, or product enhancements. Go to the **Self-Service Resources** section.

Open a Case

When your entire network is down (P1), or severely impacted (P2), call the appropriate telephone number listed below to get help:

- Continental United States: 1-855-782-5871
- Canada: 1-855-782-5871
- Europe, Middle East, Africa, Central and South America, and Asia Pacific, toll-free numbers are available at https://support.ruckuswireless.com/contact-us and Live Chat is also available.
- Worldwide toll number for our support organization. Phone charges will apply: +1-650-265-0903

We suggest that you keep a physical note of the appropriate support number in case you have an entire network outage.

Self-Service Resources

The Ruckus Support Portal at https://support.ruckuswireless.com offers a number of tools to help you to research and resolve problems with your Ruckus products, including:

- Technical Documentation—https://support.ruckuswireless.com/documents

- Community Forums—https://forums.ruckuswireless.com/ruckuswireless/categories
- Knowledge Base Articles—https://support.ruckuswireless.com/answers
- Software Downloads and Release Notes—https://support.ruckuswireless.com/#products_grid
- Security Bulletins—https://support.ruckuswireless.com/security

Using these resources will help you to resolve some issues, and will provide TAC with additional data from your troubleshooting analysis if you still require assistance through a support case or RMA. If you still require help, open and manage your case at https://support.ruckuswireless.com/case_management.

About This Document

- Supported hardware and software.....11
- What's new in this document.....11

Supported hardware and software

This guide supports the following product families for FastIron 08.0.61:

- ICX 7250
- ICX 7450
- ICX 7750
- ICX 7150

What's new in this document

The following table describes information added or modified in this guide for FastIron 08.0.61.

TABLE 2 Summary of enhancements in FastIron release 08.0.61

Feature	Description	Location
Dynamic DHCP options configuration processing	DHCP options that are configured manually or obtained dynamically from the DHCP server can be differentiated.	Dynamic DHCP options configuration processing on page 31 Verifying dynamic DHCP options for a switch on page 33 Verifying dynamic DHCP options for a router on page 35
Auto-deployment of Layer 3 image and monitoring	Previously, migrating to a FastIron Layer 3 router image caused some manageability and reachability capabilities to be lost. These issues are resolved, and the same level of auto-provisioning is available in the Layer 3 router image.	DHCP client on page 15, especially the following sections: *DHCP over default Virtual Ethernet port (Layer 3 devices)* *Default Virtual Ethernet port creation (Layer 3 devices)* *DHCP client in continuous discovery* *DHCP client as a new device* *DHCP auto-provisioning*.
IP source guard on VLAN	IP source guard can be enabled on a switch or a router for a range of ports in a VLAN or on the entire VLAN.	Enabling IP source guard on a VLAN on page 83
Updated content for defect fix	Added more details regarding configuration notes and feature limitations for IP Source Guard.	Configuration notes and feature limitations for IP Source Guard on page 80
Updated content for defect fix	A FastIron device configured as a DHCP server can support up to 500 DHCP clients.	DHCP server options on page 42

Dynamic Host Configuration Protocol Overview

- DHCP overview..... 13

DHCP overview

The Dynamic Host Configuration Protocol (DHCP) is based on the Bootstrap Protocol (BOOTP) and provides several configuration parameters stored in DHCP server databases to DHCP clients upon request.

DHCP enables the automatic configuration of client systems. DHCP removes the need to configure devices individually. Clients can set network properties by connecting to the DHCP server instead. This protocol consists of two components; a protocol to deliver host-specific configuration parameters from a DHCP server to a host, and a mechanism to allocate leased or permanent IP addresses to hosts. DHCP is built on a client-server model, where designated DHCP server hosts allocate network addresses and deliver configuration parameters to dynamically configured hosts.

DHCP Clients

- DHCP client....15
- BootP and DHCP relay parameters....19
- Configuring an IP helper address....19
- Configuring the BOOTP and DHCP reply source address....20
- Changing the IP address used for stamping BootP and DHCP requests....20
- Changing the maximum number of hops to a BootP relay server....21
- DHCP auto-provisioning....21
- Auto-provisioning using the bootfile.bin option....22
- DHCP auto-provisioning using the manifest file option....23
- DHCP auto-provisioning options....24
- Disabling or re-enabling the DHCP client....24
- DHCP auto-provisioning on Layer 2 and Layer 3 devices....25
- Configuration notes and feature limitations for DHCP auto-provisioning....28
- Disabling or re-enabling auto-provisioning....31
- Dynamic DHCP options configuration processing....31
- Verifying dynamic DHCP options for a switch....33
- Verifying dynamic DHCP options for a router....35

DHCP client

A host on an IP network can use BOOTP or DHCP to obtain its IP address from a BOOTP or DHCP server. To obtain the address, the client sends a BOOTP or DHCP request.

The request is a subnet directed broadcast and is addressed to UDP port 67. A limited IP broadcast is addressed to IP address 255.255.255.255 and is not forwarded by the Ruckus Layer 3 switch or other IP routers. When the BOOTP or DHCP client and server are on the same network, the server receives the broadcast request and replies to the client. However, when the client and server are on different networks, the server does not receive the client request, because the Layer 3 switch does not forward the request.

You can configure the Layer 3 switch to forward BOOTP or DHCP requests. To do so, configure a helper address on the interface that receives the client requests, and specify the BOOTP or DHCP server IP address as the address you are helping the BOOTP or DHCP requests to reach. Refer to Configuring an IP helper address on page 19. Instead of the server IP address, you can specify the subnet directed broadcast address of the IP subnet the server is in.

The DHCP client supports the dynamic IP address allocation method, where an IP address is assigned to a client for a limited period of time (or until the client explicitly relinquishes the address). Permanent IP address allocation to the hosts and statically assigned IP addresses are not supported.

Ruckus devices support a DHCP client on physical ports, LAG ports, Virtual Ethernet ports, and Control Bridge (CB) ports (802.1BR-enabled). The DHCP client is not supported on tunnel ports, stacking ports when stacking is enabled, or PE ports in 802.1BR-enabled Ruckus devices.

NOTE
On a Layer 3 device, DHCP over a Virtual Ethernet port is supported only for the default Virtual Ethernet port. The DHCP client is disabled on other VIrtual Ethernet ports.

NOTE
On a Layer 3 device, DHCP client support for PE ports on 802.1BR-enabled Ruckus devices includes the ability to participate in the initial DHCP IP discovery phase to create a default Virtual Ethernet port. However, because PE ports are considered Layer 2 switching ports, they cannot be assigned an IP address. Refer to "Default Virtual Ethernet port creation" in this document for more information.

The DHCP client is enabled by default at bootup on all Ruckus devices.

DHCP over default Virtual Ethernet port (Layer 3 devices)

The following enhancements mimic the behavior of a Layer 2 device when it is running the Layer 3 image:

- The ICX device is managed even during cable movement from one in-band interface port to another.
- Network devices that are connected downstream through an ICX device are managed no matter what ports are connected, as long as the downstream ports belong to the default Virtual Ethernet port.
- Using DHCP, acquiring IP or upgrade configuration is zero-touch.
- By default, the ICX device allows traffic to pass across all ports (reachability).
- A single MAC adress per system is used for IP discovery, which allows the same IP address to be used all the time.

Default Virtual Ethernet port creation (Layer 3 devices)

DHCP server is reachable through a physical port, and, if option 43 VSI is configured on the DHCP server, DHCP server exchange option 43 Vendor Specific Info (VSI), “Create default VE” [not case sensitive], is sent through a DHCPACK message. A Ruckus device configured as a DHCP client matches the VSI string and creates the default Virtual Ethernet port.

NOTE
To create a Virtual Ethernet port, at least one port must be a member of the default VLAN of the device.

If Virtual Ethernet port creation is successful, the IP address that is acquired through the physical port is released, and an IP address will be re-acquired through the default Virtual Ethernet port.

NOTE
The index of the default Virtual Ethernet port is the first available index. For example, on a device with no startup configuration, the default Virtual Ethernet port will have an index of 1.

If default Virtual Ethernet port creation fails, the IP address acquired will be assigned to the physical interface port or ports connecting the DHCP server if the connecting ports are Layer 3 ports.

Possible Reasons for Failure of Virtual Ethernet Port creation. The member ports of the default VLAN are queried to check for certain configured items. If any of the items are found, default Virtual Ethernet creation fails without other conditions being checked. These configured items result in failure:

- **IP routing**
- **vrf**
- **ip policy**
- **route-only**
- **rpf-mode**
- **ip-mac**

DHCP client in continuous discovery mode (Layer 2 and Layer 3 devices)

Beginning with release 08.0.61, the DHCP-client discovery process starts automatically when the system boots up and runs in a continuous manner.

DHCP Discovery is attempted 5 times based on the exponential back-off algorithm, as per RFC 2131. Retries occur at these intervals: x+4 seconds, where x is the starting system time, x+8 seconds, x+16 seconds, x+32 seconds, and x+64 seconds. After the DHCP client reaches the maximum retransmission delay of 64 seconds, it waits 2 seconds and then restarts the discovery process. The five-interval cycle repeats continuously.

NOTE
Discovery intervals may vary by +1 or -1 seconds, depending on system performance.

DHCP client as a new device

When the DHCP client device boots up without an IP address with the Layer 2 switch software version, the client initiates DHCP discovery, which is a subnet-directed broadcast. Refer to "DHCP client in continuous discovery mode" for more information.

The DHCP discovery broadcast is received by the DHCP servers present in the network. There are three possible responses to this message:

- No response
- Single response
- More than one response

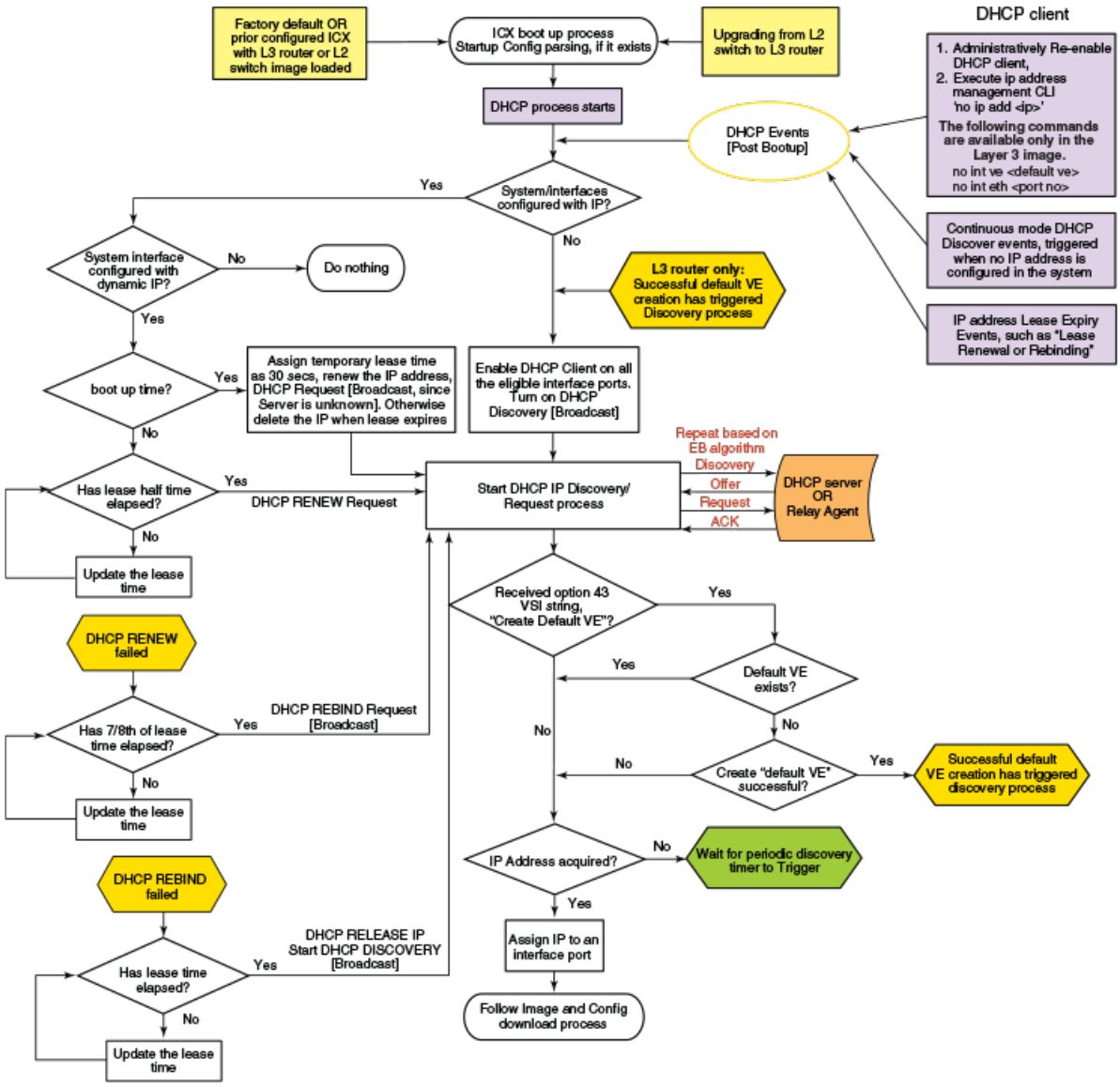
If the client does not receive a DHCP server response, there is a possibility that the client could be disabled on the device. If the client receives a response from the server (refer to "DORA process"), the client starts the DHCP request and obtains the IP address lease. If the client receives a response from more than one server, the client acknowledges the first response received, which is the default behavior.

NOTE
The DORA process is the standard Discover, Offer, Request, Acknowledge process used by DHCP to allocate IP addresses dynamically to clients through a lease period. Refer to the following graphic for a description of the ICX implementation.

In the Layer 3 software image, when the DHCP client device boots up without any IP address, the client initiates the DHCP discovery on all ports. DHCP discovery packets are sent from all DHCP client-eligible ports in the device. The default discovery mechanism is similar to the switch version.

The following flowchart illustrates this discovery mechanism.

FIGURE 1 DHCP client device bootup with no IP address



DHCP client behavior after reboot

If the DHCP client device reboots with a previously obtained IP address, the DHCP client sends the DHCP request packet, which is a subnet-directed broadcast packet from all the operationally up ports of the device. Once the DHCP server responds positively to the request, the previously obtained IP address is leased seamlessly. If the DHCP server responds in the negative, the previously obtained IP address will be released, and the DHCP process restarts.

If the software version is Layer 3, when the DHCP client comes up after a reboot with a previously obtained IP address, the DHCP client sends the DHCP request packets only on the ports where the DHCP client was enabled previously on the device.

BootP and DHCP relay parameters

The following parameters control the Layer 3 switch forwarding of BootP and DHCP requests:

- **Helper address** - The BootP/DHCP server IP address. You must configure the helper address on the interface that receives the BootP/DHCP requests from the client. The Layer 3 switch cannot forward a request to the server unless you configure a helper address for the server.
- **Gateway address** - The Layer 3 switch places the IP address of the interface that received the BootP/DHCP request in the request packet Gateway Address field (sometimes called the Router ID field). When the server responds to the request, the server sends the response as a unicast packet to the IP address in the Gateway Address field. (If the client and server are directly attached, the Gateway ID field is empty, and the server replies to the client using a unicast or broadcast packet, depending on the server.)

By default, the Layer 3 switch uses the lowest-numbered IP address on the interface that receives the request as the Gateway address. You can override the default by specifying the IP address you want the Layer 3 switch to use.

- **Hop count** - Each router that forwards a BootP/DHCP packet increments the hop count by one. Routers also discard a forwarded BootP/DHCP request instead of forwarding the request if the hop count is greater than the maximum number of BootP/DHCP hops allowed by the router. By default, a Ruckus Layer 3 switch forwards a BootP/DHCP request if its hop count is four or less but discards the request if the hop count is greater than four. You can change the maximum number of hops the Layer 3 switch allows to a value from 1 through 15.

  NOTE
  The BootP/DHCP hop count is not the TTL parameter.

Configuring an IP helper address

To forward a client broadcast request for a UDP application when the client and server are on different networks, you must configure a helper address on the interface connected to the client.

Specify the server IP address or the subnet directed broadcast address of the server's IP subnet as the helper address. You can configure up to 16 helper addresses on each interface. You can configure a helper address on an Ethernet port or a virtual interface.

1. Enter the global configuration mode by issuing the **configure terminal** command.

   ```
   device# configure terminal
   ```

2. Enter the interface configuration mode.

   ```
   device(config)# interface ethernet 1/1/2
   ```

3. Add a helper address for the server.

   ```
   device(config-if-1/1/2)# ip helper-address 1 10.95.7.6
   ```

   The commands in the example above add a helper address for server 10.95.7.6 to the port. If the port receives a client request for any of the applications that the Layer 3 switch is enabled to forward, the Layer 3 switch forwards the client request to the server.

4. By default, an IP helper does not forward client broadcast requests to a server within the network. To forward a client broadcast request when the client and server are on the same network, configure an IP helper with the unicast option on the interface connected to the client.

```
device(config-if-1/1/2)# ip helper-address 1 10.10.10.1 unicast
```

   The previous example configures an IP helper unicast option on unit 1, slot 1, port 2. The IP helper with unicast parameter forwards the client request to the server 10.10.10.1, which is within the network.

Configuring the BOOTP and DHCP reply source address

You can configure the device so that a BOOTP/DHCP reply to a client contains the server IP address as the source address instead of the router IP address.

1. Enter the global configuration mode by issuing the configure terminal command.

```
device# configure terminal
```

2. Enter the **ip helper-use-responder-ip** command.

```
device(config)# ip helper-use-responder-ip
```

Changing the IP address used for stamping BootP and DHCP requests

When a Layer 3 switch forwards a BootP or DHCP request, the Layer 3 switch "stamps" the Gateway Address field.

The default value the Layer 3 switch uses to stamp the packet is the lowest-numbered IP address configured on the interface that received the request. If you want the Layer 3 switch to use a different IP address to stamp requests received on the interface, use either of the following methods to specify the address.

The BootP/DHCP stamp address is an interface parameter. You can change the parameter on the interface that is connected to the BootP/DHCP client.

1. Enter the global configuration mode by issuing the configure terminal command.

```
device# configure terminal
```

2. Enter the interface configuration mode.

```
device(config)# interface ethernet 1/1/1
```

3. Change the BootP or DHCP stamp address for requests received on port 1/1/1 to 10.157.22.26.

```
device(config-if-1/1/1)# ip bootp-gateway 10.157.22.26
```

   The previous example changes the BootP or DHCP stamp address for requests received on port 1/1/1 to 10.157.22.26. The Layer 3 switch will place this IP address in the Gateway Address field of BootP or DHCP requests that the Layer 3 switch receives on port 1/1/1 and forwards to the BootP or DHCP server.

The following example changes the BootP or DHCP stamp address.

```
device# configure terminal
device(config)# interface ethernet 1/1/1
device(config-if-1/1/1)# ip bootp-gateway 10.157.22.26
```

Changing the maximum number of hops to a BootP relay server

Each BootP or DHCP request includes a Hop Count field. The Hop Count field indicates how many routers the request has passed through.

When the Layer 3 switch receives a BootP or DHCP request, the Layer 3 switch looks at the value in the Hop Count field.

- If the hop count value is equal to or less than the maximum hop count the Layer 3 switch allows, the Layer 3 switch increments the hop count by one and forwards the request.
- If the hop count is greater than the maximum hop count the Layer 3 switch allows, the Layer 3 switch discards the request.

You can change the maximum number of hops the Layer 3 switch allows for forwarded BootP or DHCP requests.

NOTE
The BootP and DHCP hop count is not the TTL parameter.

1. Enter the global configuration mode by issuing the **configure terminal** command.

   ```
   device# configure terminal
   ```

2. Modify the maximum number of BootP or DHCP.

   ```
   device(config)# bootp-relay-max-hops 10
   ```

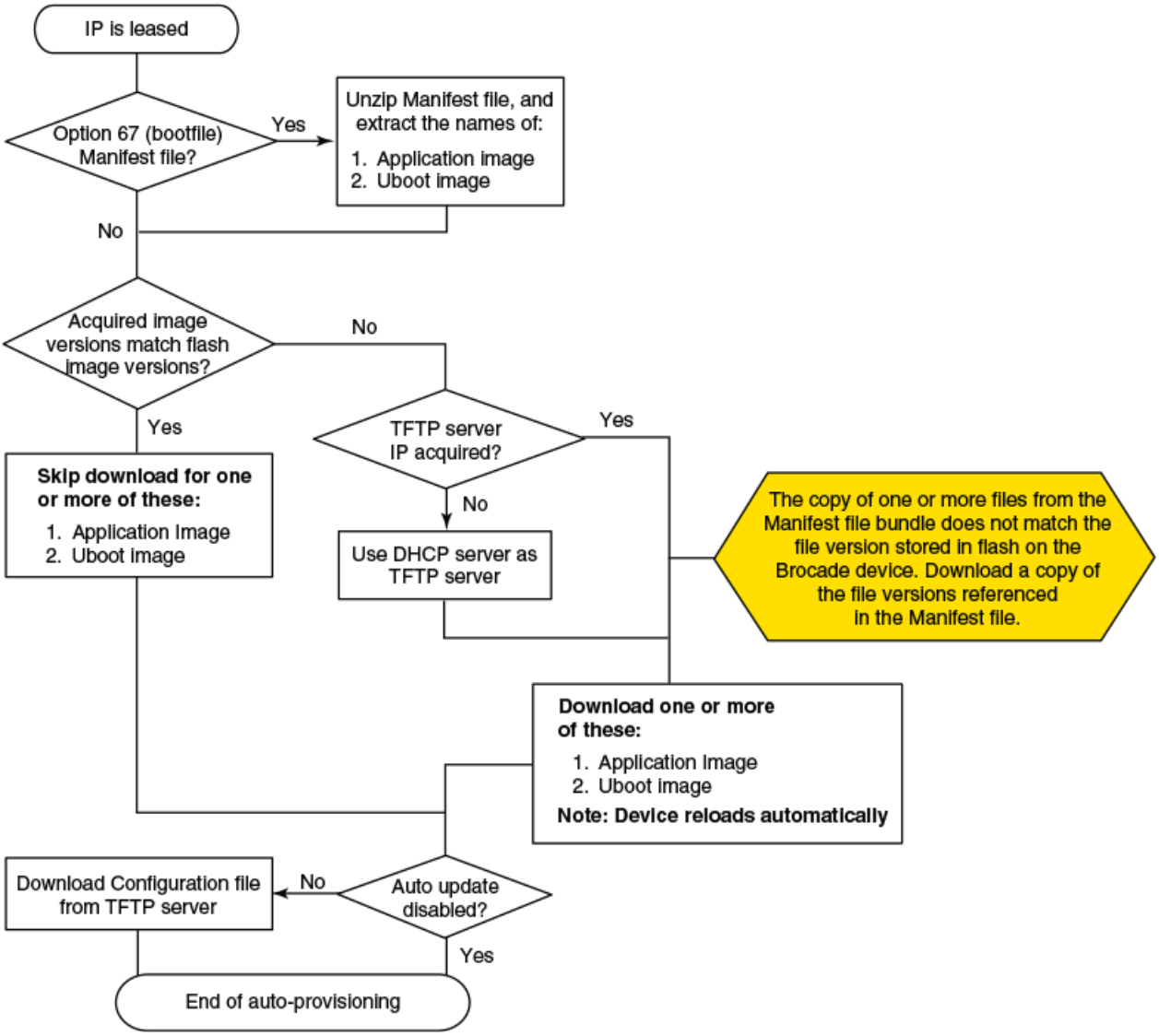
   The example allows the Layer 3 switch to forward BootP or DHCP requests that have passed through ten previous hops before reaching the Layer 3 switch. Requests that have traversed 11 hops before reaching the switch are dropped. Since the hop count value initializes at zero, the hop count value of an ingressing DHCP Request packet is the number of Layer 3 routers that the packet has already traversed.

DHCP auto-provisioning

DHCP auto-provisioning allows Layer 2 and Layer 3 devices to automatically obtain leased IP addresses through a DHCP server, negotiate address lease renewal, and obtain flash image and configuration files. The DHCP client and auto-provisioning are enabled by default on all DHCP client-eligible ports. Auto-provisioning allows clients to boot up with the latest image and configuration without manual intervention. Refer to the DHCP server section for details on DHCP server configuration and options.

NOTE
DHCP auto-provisioning is platform independent and has no difference in behavior or configuration across platforms.

FIGURE 2 DHCP client-based auto-provisioning



Auto-provisioning using the bootfile.bin option

You can configure the image name with a .bin extension on the server.

DHCP auto-provisioning using the bootfile.bin occurs as follows.

1. Once a lease is obtained from the server, the device uses the information from the DHCP server to contact the TFTP server to update the image file.
2. The device compares the file name of the requested flash image with the image stored in flash. In a stacking configuration, the device compares the file name with the image stored in the Active Controller only.

3. If the .bin file names match, then the DHCP client skips the flash image download. If auto-provisioning is enabled, the DHCP client proceeds with downloading the configuration files. If the .bin file names are different, the DHCP client downloads the new image from a TFTP server, and then writes the downloaded image to flash. In a stacking configuration, the device copies the flash image to flash in all stack member units.
4. The code determines which flash (primary or secondary) to use based on how the device is booted.
5. In a stacking configuration, the member units use the same flash as the Active Controller. Once the flash is updated with the newer flash image, the device is reloaded and all member units in a stacking configuration are reloaded as well. If auto-provisioning is enabled, the DHCP client then proceeds to download the configuration files.
6. If the DHCP client detects that the new image is older than the current running image, the device continues to reload after a syslog notification that the device is downgrading and may lose the configuration. The following example shows a syslog notification.

```
Downloaded boot-image ICXR07030F2b1.bin is downgraded version of  ICXR08030F2b1.bin.
Device is downgrading and the configuration may be lost.
```

DHCP auto-provisioning using the manifest file option

Support for auto-provisioning using the manifest file has been introduced in FastIron release 8.0.40.

The bundle of Image file, boot loader and PoE firmware can be configured as a .txt file on the DHCP server using option 67. Auto-provisioning using the manifest file occurs as follows.

1. Once a lease is obtained from the server, the device uses the information from the DHCP server to contact the TFTP server to update the image file.

   The manifest file is downloaded.
2. After downloading the manifest file, the device unzips the file and compares the file name of the requested flash image (SPR08040q054.bin) and boot image (spz10106b002.bin) with the images stored in flash. In a stacking configuration, the device compares the file name with the image stored in the Active Controller only.
3. If the flash image matches, the DHCP client skips the flash image download. If auto-provisioning is enabled, the DHCP client proceeds with downloading the configuration files.
4. If the flash image is different, the device downloads the new flash image from the TFTP server and checks for the boot image. If the boot image matches, the DHCP client skips the boot image. If the boot image does not match, the DHCP client downloads the new boot image from the TFTP server, and then writes the downloaded image to flash. In a stacking configuration, the device copies the flash and boot image to flash in all stack member units.
5. The code determines which flash (primary or secondary) to use based on how the device is booted.
6. In a stacking configuration, the member units use the same flash as the Active Controller. Once the flash is updated with the newer flash image, the device is reloaded and all member units in a stacking configuration are reloaded as well. If auto-configuration is enabled, after reload the DHCP client then proceeds to download the configuration files.
7. If the DHCP client detects that the new image is older than the current running image, the device continues to reload after a syslog notification that the device is downgrading and may lose the configuration. The following is an example of the syslog notification.

```
Downloaded boot-image ICXR07030F2b1.bin is downgraded version of ICXR08030F2b1.bin.
Device is downgrading and the configuration may be lost.
```

DHCP auto-provisioning options

The following options are supported by the client for auto-provisioning.

TABLE 3 DHCP auto-upgrade supported options

DHCP option	Description
001	Subnet mask
003	Router IP (default route)
006	Domain name server
012	Host name
015	Domain name
043	Vendor-specific information
066	TFTP server name
067	Boot file (image)
150	TFTP server IP address

Disabling or re-enabling the DHCP client

The DHCP client is enabled by default. You can disable or re-enable DHCP client on a switch or a router.

1. On a switch, enter the global configuration mode by issuing the **configure terminal** command.

```
device# configure terminal
```

2. Enter the **no ip dhcp-client enable** command to disable the DHCP client.

```
device(config)# no ip dhcp-client enable
```

3. On a switch, enter the **ip dhcp-client enable** command to re-enable the DHCP client.

```
device(config)# ip dhcp-client enable
```

4. On a router, enter the **ip dhcp-client disable** command to disable the DHCP client service on all physical interface and virtual interface level.

```
device(config)# ip dhcp-client disable
```

5. On a router, enter the **no ip dhcp-client disable** command to re-enable the DHCP client service on all physical interface and virtual interface level.

```
device(config)# no ip dhcp-client disable
```

6. On a router, enter the interface configuration mode.

```
device(config)# interface ethernet 2/1/1
```

7. Enter the **no ip dhcp-client enable** command to disable the DHCP client.

```
device(config-if-e1000-2/1/1)# no ip dhcp-client enable
```

8. On a router, enter the **ip dhcp-client enable** command at the interface configuration level to re-enable the DHCP client.

```
device(config-if-e1000-2/1/1)# ip dhcp-client enable
```

9. On a router, enter the **ip dhcp-client enable** command at the virtual interface level to re-enable the DHCP client.

```
device(config-if-ve1)# ip dhcp-client enable
```

DHCP auto-provisioning on Layer 2 and Layer 3 devices

DHCP auto-provisioning enhancements have been introduced for Layer 2 and Layer 3 devices.

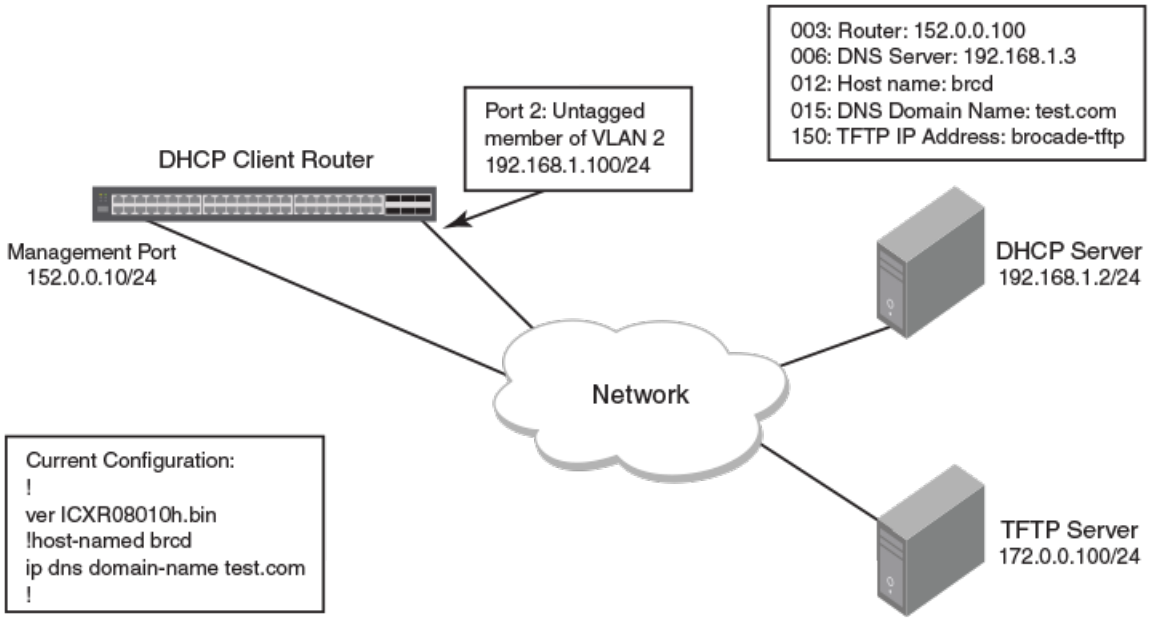
- If the non-default VLAN has multiple untagged ports connected to different DHCP servers, the first port that received the IP address offer will be considered and the other port will not receive an IP address. This behavior applies for default VLANs, too.
- After an image update and device reload, the option 3 (router) installs the default route to maintain the connectivity with the TFTP or DHCP servers. In releases prior to FastIron 8.0.40, option 3 was supported only on Layer 2 devices. The default route added by the DHCP client device from option 3 (router) will be of the lowest metric (254). If the device has a default route, the DHCP provided route is also appended to the routing table.

TABLE 4 Differences between switch and router image DHCP clients

Layer 2 DHCP client	Layer 3 DHCP client
IP address is configured on the switch (globally)	IP address is configured on the specific client port
IP default gateway is configured as “Default gateway X.X.X.X (option 3)	Default route is configured as “IP route” with distance metric 254

The following scenarios illustrate DHCP auto-provisioning in different environments.

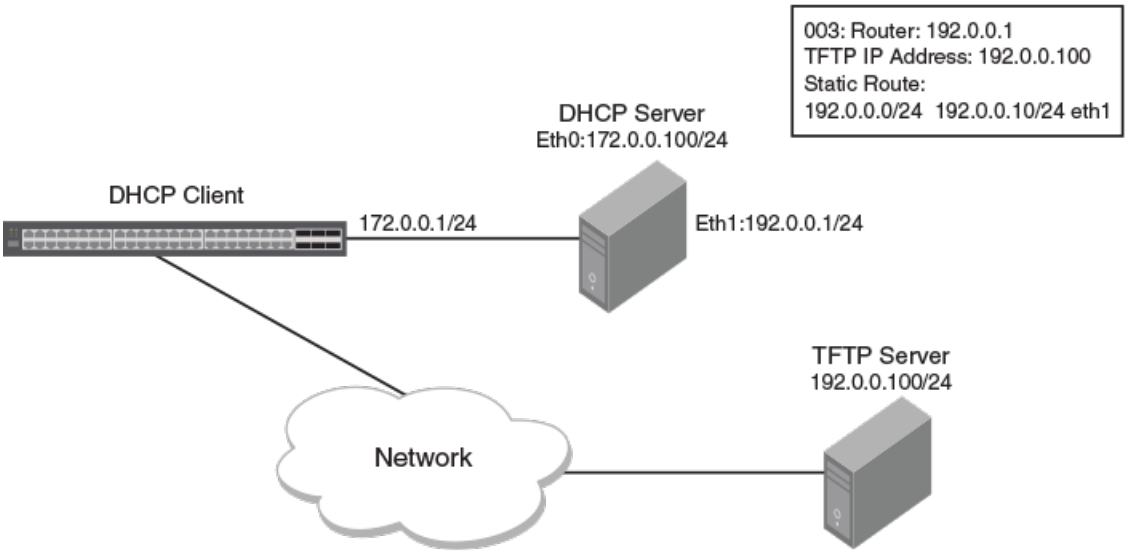
Scenario 1: DHCP auto-provisioning on a Layer 3 device



In this scenario, the DHCP client and server are part of the same network, but the TFTP server is part of a different network. Here the DHCP client device needs a default route for TFTP server reachability.

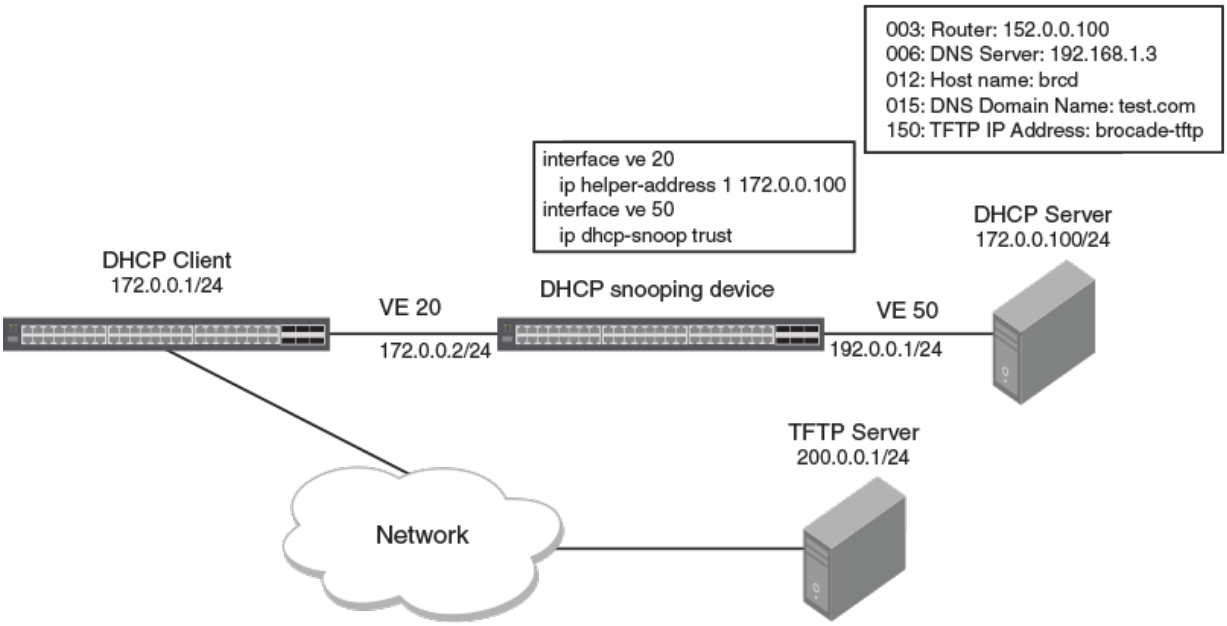
1. The FastIron router (DHCP client) connected to the DHCP server is booted.
2. The client obtains a dynamic IP address lease from the DHCP server through the untagged member port 2 of the VLAN 2 (which is a non-default VLAN) along with other DHCP server options.
3. Once DHCP server options are enabled, the router option 3 is processed and installs the default route onto the device. Options 6,12, 15, and 150 are processed as well.
4. If auto-provisioning is enabled and the image file comparison is successful, the client downloads the new image using the TFTP server IP address specified in the DHCP server.
5. If auto-provisioning is enabled, the client downloads the configuration file after connecting to the TFTP server and applies the running configuration on the device.

Scenario 2: DHCP auto-provisioning with a TFTP server in a different network



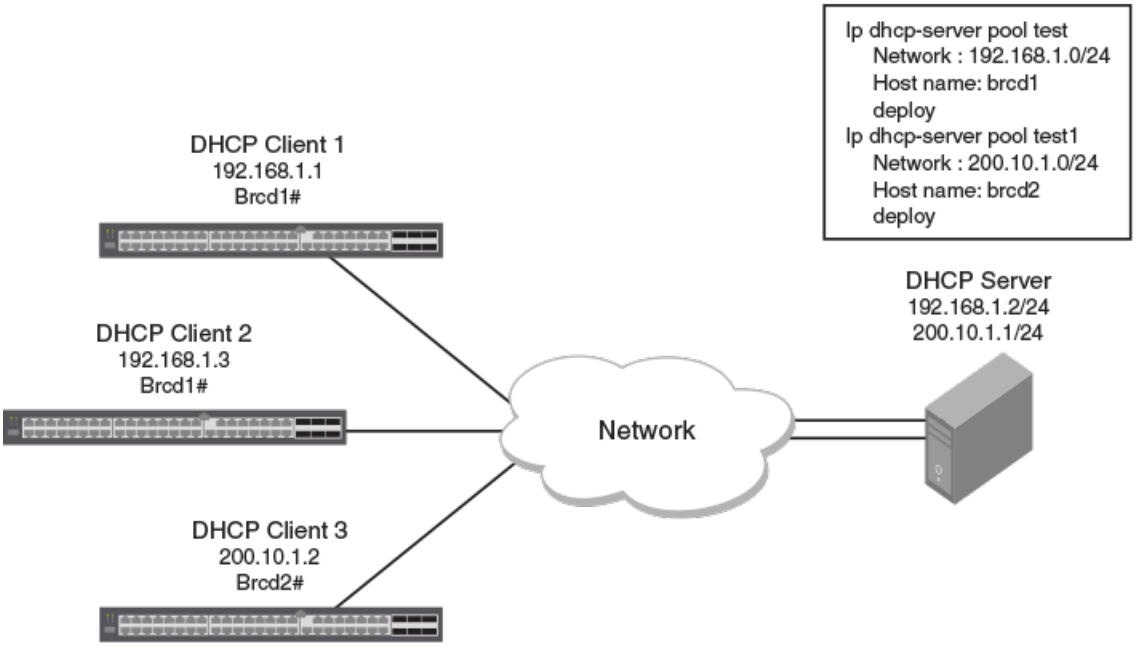
In this scenario, the DHCP client and server are connected in the same network, but the TFTP server is connected in a different network through the DHCP server. Here the DHCP client device needs a default route to reach the TFTP server. The steps are the same as in scenario 1, except that the TFTP server will be reachable after the new image update as the router option 3, which is the default gateway IP address 192.0.0.1, is installed.

Scenario 3: DHCP client connected through a DHCP snooping device



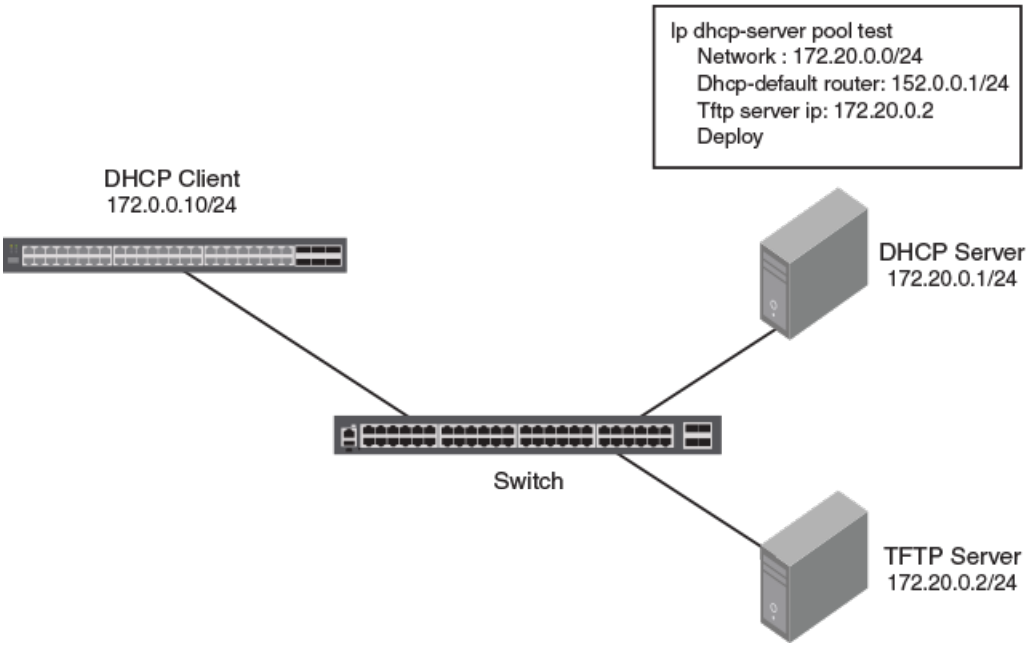
In this scenario, the DHCP client and server are connected through ports on which DHCP snooping or relay agent are enabled and are part of non-default VLANs. The working scenario is the same as Scenario 1.

Scenario 4: DHCP client option 12



In this scenario, the DHCP clients 1 and 2 are connected to the DHCP server in the same subnet. Subsequently, both receive the same host name. The DHCP client 3 is connected to the DHCP server in a different subnet and it is assigned with the host name of the second pool.

Scenario 5: DHCP auto-provisioning on a Layer 2 device



In this scenario, auto-provisioning on a Layer 2 device occurs as follows:

1. The DHCP client device is powered on.
2. The client sends the DHCP discovery packets on all DHCP client-eligible ports that are up.
3. The client obtains the dynamic IP address from the DHCP server along with option 3.
4. Once the new router image is brought up, the client tries to connect to the TFTP server using the default route.

Configuration notes and feature limitations for DHCP auto-provisioning

The following configuration notes and feature limitations apply to the DHCP auto-provisioning feature.

- For Layer 2 devices, the DHCP auto-provisioning feature is available for default VLANs and management VLANs.
- Although the DHCP server may provide multiple addresses, only one IP address is installed at a time.
- This feature is not supported together with DHCP snooping.
- POE firmware upgrade is not be supported when DHCP auto-provisioning occurs using the manifest file.
- The DHCP client does not initiate auto-provisioning after a stack switchover. You must disable and re-enable the DHCP client after a stack switchover for auto-provisioning to start.
- The **show ip** command does not display the image file name if the bootfile on the DHCP server is configured as manifest.txt, when the Layer 2 switch acts as a DHCP client.

- When the Layer 2 switch acts as a DHCP client, the **show ip** command does not display the image file name if the bootfile on the DHCP server is configured as manifest.txt.
- During the DHCP auto-provisioning process, the client accepts either the TFTP server name or the TFTP server IP address. If the server name is configured, the client ignores the server IP address.
- During auto-provisioning using the manifest.txt file, if the flash images are the same, the boot image download is skipped.
- The DHCP server accepts more than one default router in the address pool if the image is a Layer 2 image.
- The DHCP client contacts the TFTP server to obtain the hostnameMAC-config.cfg file five times only if the TFTP server is busy, or if the TFTP server is not reachable. If the TFTP server is reachable, the DHCP client contacts the TFTP server only once.
- In a stacking configuration, the DHCP client flash image download waits five minutes for all member units to join and update. Then the DHCP client downloads the new image from the TFTP server using the TFTP server IP address (option 150), if it is available. If the TFTP server IP address is not available, the DHCP client requests the TFTP file from the DHCP server.
- If the **enable aaa console** command is configured, the DHCP client does not request the configuration files.

The following configuration rules apply to DHCP auto-provisioning:

- To enable flash image update (**ip dhcp-client auto-update enable** command), you must also enable the auto-configuration (**ip dhcp-client enable** command).
- The image file name to be updated must have the extension .bin or .txt.
- The DHCP option 067 bootfile name is used for an image update if it has the extension .bin or .txt.
- The DHCP option 067 bootfile name is used for the configuration download if it does not have the extension .bin or .txt.
- If the DHCP option 067 bootfile name is not configured or does not have the extension .bin or .txt then auto-provisioning does not occur.
- In releases prior to FastIron 8.0.40, while updating the image using option 67, the image types (Layer 2 or Layer 3) should match. For example, if the DHCP client with a Layer 3 image downloads an updated Layer 2 image using option 067, the configuration download fails.

High Availability and 802.1BR considerations

In an ICX stack, after switchover between active and standby devices, the DHCP process re-acquires IP addresses and follows the upgrade process.

DHCP is supported on 802.1BR-enabled devices as a normal stacking device. In a Campus Fabric (SPX) configuration, the DHCP client is able to send packets through all CB and PE ports. PE ports can be members of the VE.

Upgrade considerations

When upgrading from FastIron 08.0.60 or previous releases to FastIron 08.0.61 or later, if rules to create default VE are met, the following occur automatically: the default VE is created, the DHCP client is enabled over the default VE, and it acquires the IP address.

How DHCP client-based auto-provisioning and flash image update works

Auto-provisioning is enabled by default. To disable this feature, refer to Disabling or re-enabling the DHCP client on page 24 and Disabling or re-enabling auto-provisioning on page 31 respectively.

FIGURE 3 DHCP auto-provisioning: Boot file and configuration downloads

Validating the IP address and lease negotiation

The following steps describe the IP address validation and lease negotiation process.

1. At bootup, the device automatically checks its configuration for an IP address.
2. If the device does not have a static IP address, it requests the lease of an address from the DHCP server:
   - If the server responds, it leases an IP address to the device for the specified lease period.
   - If the server does not respond (after four tries) the DHCP client process is ended.
3. If the device has a dynamic address, the device asks the DHCP server to validate that address. If the server does not respond, the device continues to use the existing address until the lease expires. If the server responds, and the IP address is outside of the DHCP address pool or has been leased to another device, it is automatically rejected, and the device receives a new IP address from the server. If the existing address is valid, the lease continues.

   NOTE
   The lease time interval is configured on the DHCP server, not on the client device. The **ip dhcp-client lease** command is set by the system, and is non-operational to a user.

4. If the existing address is static, the device keeps it and the DHCP client process is ended.
5. For a leased IP address, when the lease interval reaches the renewal point, the device requests a renewal from the DHCP server:
   - If the device is able to contact the DHCP server at the renewal point in the lease, the DHCP server extends the lease. This process can continue indefinitely.
   - If the device is unable to reach the DHCP server after four attempts, it continues to use the existing IP address until the lease expires. When the lease expires, the dynamic IP address is removed and the device contacts the DHCP server for a new address.

Flash image download and update

NOTE
The flash image download and update process only occurs when the client device reboots, or when the DHCP client has been disabled and then re-enabled.

Once a lease is obtained from the server, the device compares the file name of the requested flash image with the image stored in flash. In a stacking configuration, the device compares the file name with the image stored in the Active Controller only.

- If the .bin file names match, then the DHCP client skips the flash image download. If auto-provisioning is enabled, the DHCP client proceeds with downloading the configuration files.
- If the .bin file names are different, then the DHCP client downloads the new image from a TFTP server and then writes the downloaded image to flash. In a stacking configuration, the device copies the flash image to flash in all stack member units.

The code determines which flash (primary or secondary) to use based on how the device is booted. In a stacking configuration, the member units use the same flash as the active controller. Once the flash is updated with the newer flash image, the device is reloaded, and any member units in a stacking configuration are reloaded as well. If auto-provisioning is enabled, the DHCP client then proceeds to download the configuration files.

Auto-provisioning download and update

During auto-provisioning, the device requests the configuration files from the TFTP server in the following order.

1. bootfile name provided by the DHCP server (if configured).
2. hostnameMAC-config.cfg (for example: ICX001p-Switch0000.005e.4d00-config.cfg).
3. hostnameMAC.cfg (for example: ICX002p-Switch0000.005e.4d00.cfg).
4. A new file format has been introduced based on the host name as part of DHCP option 12 support. For example fi_router.cfg.
5. When the DHCP client switch looks for the configuration file in the TFTP server, a configuration file in the format such as <icx>-<switch | router>.cfg will be ignored. Instead the following file format is expected.

Old format: ICX7750-router.cfg	**New format:** ICX7750.cfg

   < ICX7750>.cfg appends the existing configuration.
6. ruckus.cfg (applies to all devices), (for example: ruckus.cfg appends the existing configuration).

If the device successfully contacts the TFTP server and the server has the configuration file, the files are merged. If there is a conflict, the server file takes precedence. If the device is unable to contact the TFTP server, or if the files are not found on the server, the TFTP part of the configuration download process ends.

Disabling or re-enabling auto-provisioning

DHCP auto-provisioning is enabled by default. You can disable or re-enable DHCP auto-provisioning on a switch or a router.

1. On a switch or a router enter the global configuration mode by issuing the **configure terminal** command.

   ```
   device# configure terminal
   ```

2. Enter the **no ip dhcp-client auto-update enable** command to disable DHCP auto-provisioning.

   ```
   device(config)# no ip dhcp-client auto-update enable
   ```

3. Enter the **ip dhcp-client auto-update enable** command to enable DHCP auto-provisioning after it has been disabled.

   ```
   device(config)# ip dhcp-client auto-update enable
   ```

Dynamic DHCP options configuration processing

The system can differentiate between manually configured DHCP options and DHCP options that were obtained dynamically from the server. Manually configured DHCP options are retained even when the dynamic IP address is released.

To help identify them, the keyword **dynamic** is appended to output for all dynamic DHCP options that are reflected in the running configuration.

NOTE
Only the IP address and the default gateway/default route are persistent across reloads (after the **write memory** is executed to save the configuration). The remaining DHCP options that are obtained from the DHCP server are relearned when the ICX device reboots.

It is not possible to manually configure the dynamic option. If you attempt to configure a dynamic option manually, an error is displayed stating “Manual configuration is not allowed for this option."

NOTE
If a static IP Address is configured manually for the device after obtaining a dynamic IP Address and DHCP options from the DHCP server, all DHCP options are released along with the dynamic IP Address.

Verifying dynamic DHCP options for a switch

You can identify dynamically obtained DHCP options for a switch.

1. On a switch enter the **show running-config** command. Examine the output to identify dynamically obtained options. These options have a “dynamic” tag appended to them in the running configuration.

```
device> show running-config

Current configuration:
!
ver 08.0.61b1T211
!
stack unit 1
  module 1 icx7250-24-port-management-module
  module 2 icx7250-sfp-plus-8port-80g-module
!
!
!
vlan 1 name DEFAULT-VLAN by port
!
!
!
hostname TestHostName dynamic
ip address 10.10.10.2 255.255.255.0 dynamic
ip dns domain-list ManualDomain.com
ip dns domain-list testStaticDomain.com
ip dns domain-list testDomain.com dynamic
ip dns server-address 20.20.20.8 20.20.20.9 20.20.20.5 10.10.10.5(dynamic)
ip default-gateway 10.10.10.1 dynamic
!
!
!
interface ethernet 1/1/21
 disable
!
interface ethernet 1/2/2
 speed-duplex 1000-full
!
interface ethernet 1/2/4
 speed-duplex 1000-full
!
interface ethernet 1/2/5
 speed-duplex 1000-full
!
interface ethernet 1/2/6
 speed-duplex 1000-full
!
interface ethernet 1/2/7
 speed-duplex 1000-full
!
interface ethernet 1/2/8
 speed-duplex 1000-full
!
!
!
lldp run
!
!
end
```

2. On a switch enter the **show configuration** command. Examine the output to identify dynamically obtained options. These options have a “dynamic” tag appended to them in the running configuration.

```
device> show configuration

Startup-config data location is flash memory
!
Startup configuration:
!
ver 08.0.61b1T211
!
stack unit 1
  module 1 icx7250-24-port-management-module
  module 2 icx7250-sfp-plus-8port-80g-module
!
!
vlan 1 name DEFAULT-VLAN by port
!
!
!
!
ip address 10.10.10.2 255.255.255.0 dynamic
ip dns domain-list ManualDomain.com
ip dns domain-list testStaticDomain.com
ip dns server-address 20.20.20.8 20.20.20.9 20.20.20.5
ip default-gateway 10.10.10.1 dynamic
!
!
!
interface ethernet 1/1/21
 disable
!
interface ethernet 1/2/2
 speed-duplex 1000-full
!
interface ethernet 1/2/4
 speed-duplex 1000-full
!
interface ethernet 1/2/5
 speed-duplex 1000-full
!
interface ethernet 1/2/6
 speed-duplex 1000-full
!
interface ethernet 1/2/7
 speed-duplex 1000-full
!
interface ethernet 1/2/8
 speed-duplex 1000-full
!
lldp run
!

end
```

Verifying dynamic DHCP options for a router

You can identify dynamically obtained DHCP options for a router.

1. On a router enter the **show running-config** command. Examine the output to identify dynamically obtained options. These options have a “dynamic” tag appended to them in the running configuration.

```
device> show running-config

Current configuration:
!
ver 08.0.61b1T213
!
stack unit 1
  module 1 icx7250-24-port-management-module
  module 2 icx7250-sfp-plus-8port-80g-module
!
!
vlan 1 name DEFAULT-VLAN by port
!
!
!
hostname TestHostName dynamic
ip dns domain-list ManualDomain.com
ip dns domain-list testDomain.com dynamic
ip dns domain-list testStaticDomain.com
ip dns server-address 20.20.20.8 20.20.20.9 10.10.10.5(dynamic) 20.20.20.5
ip route 0.0.0.0/0 10.10.10.1 distance 254 dynamic
!
!
interface ethernet 1/1/7
 ip address 10.10.10.2 255.255.255.0 dynamic
!
interface ethernet 1/1/21
 disable
!
interface ethernet 1/2/2
 speed-duplex 1000-full
!
interface ethernet 1/2/4
 speed-duplex 1000-full
!
interface ethernet 1/2/5
 speed-duplex 1000-full
!
interface ethernet 1/2/6
 speed-duplex 1000-full
!
interface ethernet 1/2/7
 speed-duplex 1000-full
!
interface ethernet 1/2/8
 speed-duplex 1000-full
!
!
lldp run
!
!
end
```

2. On a router enter the **show configuration** command. Examine the output to identify dynamically obtained options. These options have a “dynamic” tag appended to them in the running configuration.

```
device> show configuration

!
Startup-config data location is flash memory
!
Startup configuration:
!
ver 08.0.61b1T213
!
stack unit 1
  module 1 icx7250-24-port-management-module
  module 2 icx7250-sfp-plus-8port-80g-module
!
!
vlan 1 name DEFAULT-VLAN by port
!
!
!
ip dns domain-list ManualDomain.com
ip dns domain-list testStaticDomain.com
ip dns server-address 20.20.20.8 20.20.20.9 20.20.20.5
ip route 0.0.0.0/0 10.10.10.1 distance 254 dynamic
!
!
!
interface ethernet 1/1/7
 ip address 10.10.10.2 255.255.255.0 dynamic
!
interface ethernet 1/1/21
 disable
!
interface ethernet 1/2/2
 speed-duplex 1000-full
!
interface ethernet 1/2/4
 speed-duplex 1000-full
!
interface ethernet 1/2/5
 speed-duplex 1000-full
!
interface ethernet 1/2/6
 speed-duplex 1000-full
!
interface ethernet 1/2/7
 speed-duplex 1000-full
!
interface ethernet 1/2/8
 speed-duplex 1000-full
!
!
lldp run
!
!
end
```

DHCP Servers

- DHCP Servers....37
- DHCP server options....42
- Disabling or re-enabling the DHCP server on the management port....43
- Setting the wait time for ARP ping response....44
- DHCP option 82 support....44
- Enabling relay agent echo (option 82)....44
- Configuring the IP address of the DHCP server....45
- Configuring the boot image....45
- Deploying an address pool configuration to the server....45
- Specifying default routers available to the client....46
- Specifying DNS servers available to the client....46
- Configuring the domain name for the client....46
- Configuring the lease duration for the address pool....47
- Specifying addresses to exclude from the address pool....47
- Configuring the NetBIOS server for DHCP clients....47
- Configuring the subnet and mask of a DHCP address pool....48
- Configuring a next-bootstrap server....48
- Configuring the TFTP server....48
- Configuring a vendor type and configuration value for a DHCP client....49
- Configuring X Window System Display Manager IP addresses (option 49)....49
- Configuring vendor details and vendor specific information (option 43 and option 60)....50
- Enabling static IP to MAC address mapping....51
- Configuring Avaya IP telephony (options 176 and 242)....51
- Configuring WPAD (option 252)....52
- Displaying DHCP server information....53

DHCP Servers

All FastIron devices can be configured to function as DHCP servers.

DHCP introduces the concept of a lease on an IP address. The DHCP server can allocate an IP address for a specified amount of time or can extend a lease for an indefinite amount of time. DHCP provides greater control of address distribution within a subnet. This feature is crucial if the subnet has more devices than available IP addresses. In contrast to BOOTP, which has two types of messages that can be used for leased negotiation, DHCP provides seven types of messages.

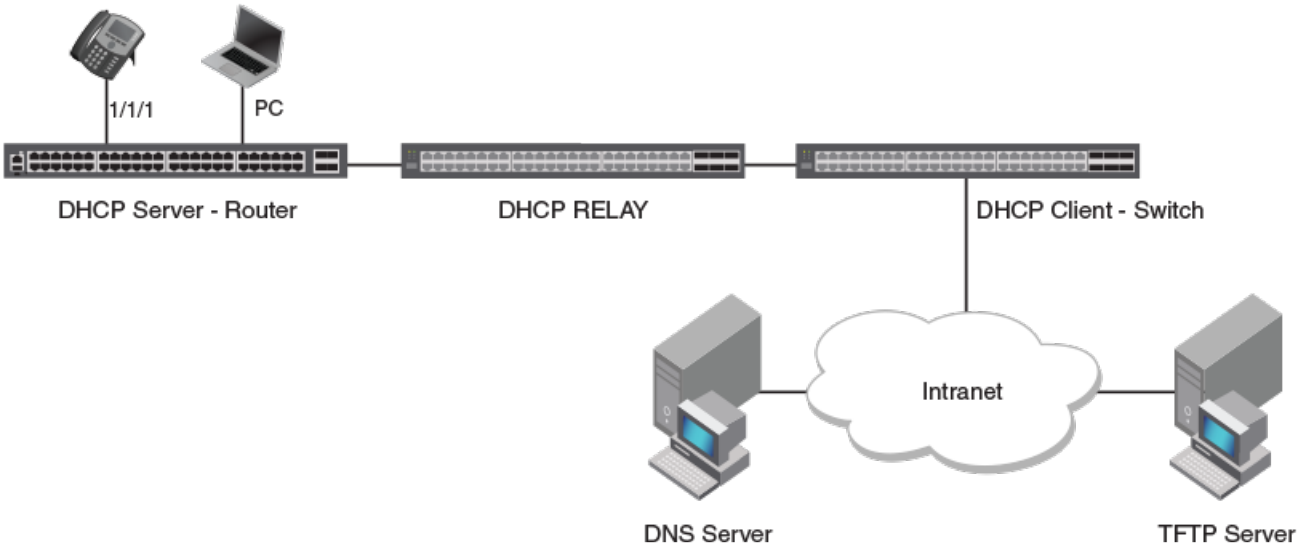
DHCP allocates temporary or permanent network IP addresses to clients. When a client requests the use of an address for a time interval, the DHCP server guarantees not to reallocate that address within the requested time and tries to return the same network address each time the client makes a request. The period of time for which a network address is allocated to a client is called a lease. The client may extend the lease through subsequent requests. When the client is done with the address, the address can be released back to the server. By asking for an indefinite lease, clients may receive a permanent assignment.

DHCP clients can be IP phones, desktops, or network devices, as illustrated in the following figure. The clients can be connected directly or through other networks using relays. The DHCP server provides information such as the DNS server name, TFTP server name, and also the image to pick for bootup to the DHCP client. Once the client obtains the IP address, TFTP server name and boot image name, the client can download the image from the TFTP server and boot with that image.

In some environments, it may be necessary to reassign network addresses due to exhaustion of the available address pool. In this case, the allocation mechanism reuses addresses with expired leases.

The DHCP server is disabled by default on all FastIron devices.

FIGURE 4 DHCP server usage



Configuration considerations for DHCP servers

The following configuration considerations apply to DHCP servers, the DHCP binding database, and DHCP address pools:

- The DHCP server is supported in the Layer 2 and Layer 3 software images.
- The DHCP server is not supported on non-default VRF.
- In the event of a controlled or forced switchover, a DHCP client requests from the DHCP server the same IP address and lease assignment that it had before the switchover. After the switchover, the DHCP server will be automatically re-initialized on the new Active Controller or management module.
- For DHCP client hitless support in a stack, the **stack mac** command must be used to configure the MAC address, so that the MAC address does not change in the event of a switchover or failover. If **stack mac** is not configured, the MAC address/IP address pair assigned to a DHCP client will not match after a switchover or failover. Furthermore, in the Layer 3 router image, if the **stack mac** configuration is changed or removed and the management port has a dynamic IP address, when a DHCP client tries to renew its lease from the DHCP server, the DHCP server will assign a different IP address.
- If any address from the configured DHCP pool is used, for example, by the DHCP server or TFTP server, you must exclude the address from the network pool.
- Ensure that DHCP clients do not send DHCP request packets with a Maximum Transmission Unit (MTU) larger than 1500 bytes. Ruckus devices do not support DHCP packets with an MTU larger than 1500 bytes.

DHCP binding database

- The IP addresses that have been automatically mapped to the MAC addresses of hosts are found in the DHCP binding database in the DHCP server.

- An address conflict occurs when two hosts use the same IP address. During address assignment, the DHCP server checks for conflicts. If a conflict is detected, the address is removed from the pool. The address will not be assigned until the administrator resolves the conflict.

DHCP address pools

- A DHCP address pool can be configured with a name that is a symbolic string (such as "cabo") or an integer (such as 0).
- Configuring a DHCP address pool also puts the router into DHCP pool configuration mode, where the pool parameters can be configured.
- If the DHCP server address is part of a configured DHCP address pool, you must exclude the DHCP server address from the network pool.
- While in DHCP server pool configuration mode, the system will place the DHCP server pool in pending mode and the DHCP server will not use the address pool to distribute information to clients. To activate the pool, use the **deploy** command.
- DHCP options are supported on a per-pool basis as required by the DHCP clients to be serviced in the sub-network.
- DHCP defines a process by which the DHCP server knows the IP subnet in which the DHCP client resides, and the DHCP server can assign an IP address from a pool of valid IP addresses in that subnet.

  If the client is directly connected (the giaddr field is zero), the DHCP server matches the DHCP DISCOVER message with DHCP pools that contain the subnets configured on the receiving interface. If the client is not directly connected (the giaddr field of the DHCP DISCOVER message is not zero), the DHCP server matches the DHCP DISCOVER message with a DHCP pool that has the subnet that contains the IP address in the giaddr field.

Configuring the DHCP server and creating an address pool

Perform the following steps to configure the DHCP server. Before you can configure the various DHCP server options, you must create an address pool on your FastIron device.

1. Enter global configuration mode by issuing the **configure terminal** command.

   ```
   device# configure terminal
   ```

2. Enable the DHCP server.

   ```
   device(config)# ip dhcp-server enable
   ```

3. Create a DHCP server address pool.

   ```
   device(config)# ip dhcp-server pool cabo
   ```

4. Configure the DHCP server address pool.

   ```
   device(config-dhcp-cabo)# network 172.16.1.0/24
   device(config-dhcp-cabo)# domain-name ruckuswireless.com
   device(config-dhcp-cabo)# dns-server 172.16.1.2 172.16.1.3
   device(config-dhcp-cabo)# netbios-name-server 172.16.1.2
   device(config-dhcp-cabo)# lease 0 0 5
   ```

5. To disable DHCP, enter the **no ip ip dhcp-server enable** command.

   ```
   device(config)# no ip dhcp-server enable
   ```

6. Use the **clear ip dhcp-server binding** command to delete a specific lease or all lease entries from the lease binding database.

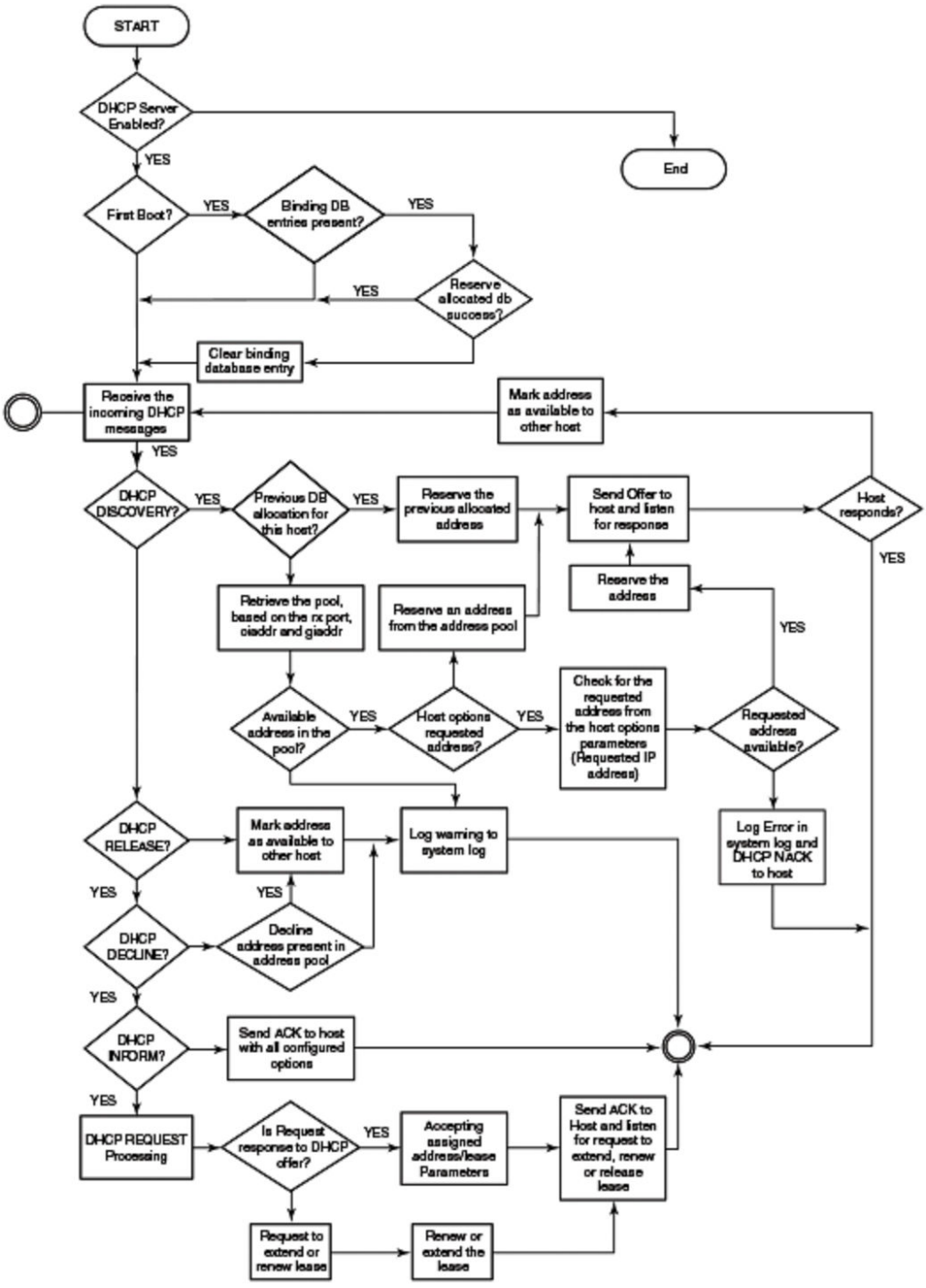
```
device(config)# clear ip dhcp-server binding *
```

   The asterisk used in the example above clears all the IP addresses.

DHCP server configuration

The following flowchart illustrates the DHCP server configuration procedure.

FIGURE 5 DHCP server configuration flowchart



Default DHCP server settings

TABLE 5 DHCP server default settings

Parameter	Default Value
DHCP server	Disabled
Lease database expiration time	86400 seconds
The duration of the lease for an assigned IP address	43200 seconds (one day)
Maximum lease database expiration time	86400 seconds
DHCP server with option 82	Disabled
DHCP server unknown circuit ID for option 82	Permit range lookup
IP distribution mechanism	Linear

DHCP server options

A FastIron device configured as a DHCP server can support up to 500 DHCP clients.

The list of supported DHCP options is shown in the following table:

TABLE 6 DHCP server options

Code	Option Name	Description
1	Subnet Mask	Specifies the client subnet mask (per RFC 950).
3	Router Option	Specifies a list of IP addresses for routers on the client subnet. Routers are listed in order of preference. **NOTE** Option 3 is not supported on non-default VRFs and management VRFs. **NOTE** Option 3 functions only when there is no previously configured route on the DHCP client. If the route received by the DHCP client from the DHCP server is already configured on the client, the following syslog message is displayed: DHCPC: Failed to configure default gateway.
6	Domain Name Server	Specifies a list of Domain Name System (RFC 1035) name servers available to the client. Servers are listed in order of preference.
12	Hostname	Configures the host name that can be assigned to the DHCP clients.
15	Domain name	Specifies the domain name the client should use when resolving host names using the Domain Name System.
47	NetBIOS over TCP/IP Name Server	Specifies a list of RFC1001/1002 NBNS name servers listed in order of preference.

TABLE 6 DHCP server options (continued)

Code	Option Name	Description
49	X Window System Display Manager	Configures the IP addresses of X Window System Display Managers which can be used by DHCP clients that support the X Window system.
66	TFTP server hostname or IP address	Configures the address or name of the TFTP server available to the client.
67	Boot File name	Specifies a boot image to be used by the client.
	Next Bootstrap Server	Configures the IP address of the next server to be used for startup by the client.
176 and 242	Avaya IP Telephone (46xx and 96xx) parameters	Configures the IP telephone parameters for Avaya IP phones running as DHCP clients.
252	Proxy-Auto Config (PAC)	Configures the PAC file location string for the Web Proxy Auto-Discovery WPAD-supported DHCP clients.
60	Vendor-Specific Information	Allows clients and servers to exchange vendor-specific information.

A DHCP server assigns and manages IPv4 addresses from multiple address pools, using dynamic address allocation. The DHCP server also contains the relay agent to forward DHCP broadcast messages to network segments that do not support these types of messages.

Disabling or re-enabling the DHCP server on the management port

By default, when the DHCP server is enabled on the FastIron device, the server responds to DHCP client requests received on the management port.

If required, you can prevent the response to DHCP client requests received on the management port by disabling DHCP server support on the port. When the DHCP server is disabled, DHCP client requests that are received on the management port are discarded.

1. Enter global configuration mode by issuing the **configure terminal** command.

```
device# configure terminal
```

2. Disable the DHCP server functionality on the management port.

```
device(config)# no ip dhcp-server mgmt
```

3. Enable the DHCP server functionality on the management port, as required.

```
device(config)# ip dhcp-server mgmt
```

Setting the wait time for ARP ping response

You can set the number of seconds to wait for a response to an ARP ping packet on the DHCP server.

At startup, the server reconciles the lease binding database by sending an ARP ping packet out to every client. If there is no response to the ARP ping packet within a set amount of time (set in seconds), the server deletes the client from the lease binding database. The minimum setting is 5 seconds and the maximum is 30 seconds.

NOTE
Do not alter the default value unless it is necessary. Increasing the value of this timer may increase the time to get console access after a reboot.

1. Enter global configuration mode by issuing the **configure terminal** command.

```
device# configure terminal
```

2. Specify the number of seconds to wait for a response to an ARP ping packet.

```
device(config)# ip dhcp-server arp-ping-timeout 20
```

The following example configures a wait ARP ping packet timeout response to 20 seconds.

```
device# configure terminal
device(config)# ip dhcp-server arp-ping-timeout 20
```

DHCP option 82 support

The DHCP relay agent information option (DHCP option 82) enables a DHCP relay agent to include information about itself when forwarding client-originated DHCP packets to a DHCP server. The DHCP server uses this information to implement IP address or other parameter-assignment policies.

In a metropolitan Ethernet-access environment, the DHCP server can centrally manage IP address assignments for a large number of subscribers. If DHCP option 82 is disabled, a DHCP policy can only be applied per subnet, rather than per physical port. When DHCP option 82 is enabled, a subscriber is identified by the physical port through which it connects to the network.

Enabling relay agent echo (option 82)

Complete the following steps to activate DHCP option 82.

This option enables the DHCP server to echo relay agent information in all replies.

1. Enter global configuration mode by issuing the **configure terminal** command.

```
device# configure terminal
```

2. Activate DHCP option 82.

```
device(config)# ip dhcp-server relay-agent-echo enable
```

Configuring the IP address of the DHCP server

Complete the following steps to specify the IP address of the selected DHCP server.

1. Enter global configuration mode by issuing the **configure terminal** command.

```
device# configure terminal
```

2. Specify the server identifier.

```
device(config)# ip dhcp-ser server-identifier 10.1.1.144
```

Configuring the boot image

The boot image specifies a boot image name to be used by the DHCP client.

In this task example, the DHCP client should use the boot image called "ICX". This variable can have an extension of .bin, .txt or .cfg.

1. Enter global configuration mode by issuing the **configure terminal** command.

```
device# configure terminal
```

2. Create and enter DHCP server pool configuration mode.

```
device(config)# ip dhcp-server pool cabo
```

3. Specify a boot image name to be used by the DHCP client.

```
device(config-dhcp-cabo)# bootfile icx
```

Deploying an address pool configuration to the server

Complete the following steps to send an address pool configuration to the DHCP server.

1. Enter global configuration mode by issuing the **configure terminal** command.

```
device# configure terminal
```

2. Create and enter DHCP server pool configuration mode.

```
device(config)# ip dhcp-server pool cabo
```

3. Deploy the address pool to the DHCP server.

```
device(config-dhcp-cabo)# deploy
```

Specifying default routers available to the client

Complete the following steps to specify the IP addresses of the default routers for a client.

1. Enter global configuration mode by issuing the **configure terminal** command.

```
device# configure terminal
```

2. Create and enter DHCP server pool configuration mode.

```
device(config)# ip dhcp-server pool cabo
```

3. Specify the IP addresses of the default routers for the client.

```
device(config-dhcp-cabo)# dhcp-default-router address [10.2.1.141, 10.2.2.140]
```

Specifying DNS servers available to the client

Complete the following steps to specify the DNS servers available to the client.

1. Enter global configuration mode by issuing the **configure terminal** command

```
device# configure terminal
```

2. Create and enter DHCP server pool configuration mode.

```
device(config)# ip dhcp-server pool cabo
```

3. Enter the dns server command followed by the IP addresses of the DNS servers that are available to the DHCP clients.

```
device(config-dhcp-cabo)# dns-server 10.2.1.143, 10.2.2.142
```

Configuring the domain name for the client

Complete the following steps to configure the domain name for the client.

1. Enter global configuration mode by issuing the **configure terminal** command.

```
device# configure terminal
```

2. Create and enter the DHCP server pool configuration mode.

```
device(config)# ip dhcp-server pool cabo
```

3. Specify the domain name for the client.

```
device(config-dhcp-cabo)# domain-name sierra
```

Configuring the lease duration for the address pool

Complete the following steps to specify the lease duration for the address pool.

You can set a lease duration for days, hours, or minutes, or any combination of the three.

1. Enter global configuration mode by issuing the **configure terminal** command.

```
device# configure terminal
```

2. Create and enter the DHCP server pool configuration mode.

```
device(config)# ip dhcp-server pool cabo
```

3. Set the lease duration for the address pool.

```
device(config-dhcp-cabo)# lease 1 4 32
```

In the example, the lease duration has been set to one day, four hours, and 32 minutes.

Specifying addresses to exclude from the address pool

Specifies addresses that should be excluded from the address pool.

You can specify a single address or a range of addresses that should be excluded from the address pool.

1. Enter global configuration mode by issuing the **configure terminal** command.

```
device# configure terminal
```

2. Create and enter DHCP server pool configuration mode.

```
device(config)# ip dhcp-server pool cabo
```

3. Specify the address that should be excluded from the address pool.

```
device(config-dhcp-cabo)# excluded-address 10.2.3.44
```

Configuring the NetBIOS server for DHCP clients

You can specify the IP address of NetBIOS WINS servers that are available to Microsoft DHCP clients.

1. Enter global configuration mode by issuing the **configure terminal** command.

```
device# configure terminal
```

2. Create and enter DHCP server pool configuration mode.

```
device(config)# ip dhcp-server pool cabo
```

3. Specify the NetBIOS server for the DHCP client.

```
device(config-dhcp-cabo)# netbios-name-server 192.168.1.55
```

Configuring the subnet and mask of a DHCP address pool

You can configure the subnet network and mask of the DHCP address pool.

1. Enter global configuration mode by issuing the **configure terminal** command.

```
device# configure terminal
```

2. Create and enter DHCP server pool configuration mode.

```
device(config)# ip dhcp-server pool cabo
```

3. Specify the subnet network and mask length of the DHCP address pool.

```
device(config-dhcp-cabo)# network 10.2.3.44/24
```

Configuring a next-bootstrap server

You can specify the IP address of the next server the client should use for bootup.

1. Enter global configuration mode by issuing the **configure terminal** command.

```
device# configure terminal
```

2. Create and enter DHCP server pool configuration mode.

```
device(config)# ip dhcp-server pool cabo
```

3. Specify the IP address of the server the client should use for bootup.

```
device(config-dhcp-cabo)# next-bootstrap-server 10.2.5.44
```

Configuring the TFTP server

You can specify the address or name of the TFTP server to be used by the DHCP clients.

NOTE
If DHCP options 66 (TFTP server name) and 150 (TFTP server IP address) are both configured, the DHCP client ignores option 150 and tries to resolve the TFTP server name (option 66) using DNS.

1. Enter global configuration mode by issuing the **configure terminal** command.

```
device# configure terminal
```

2. Create and enter DHCP server pool configuration mode.

```
device(config)# ip dhcp-server pool cabo
```

3. Configure a TFTP server by specifying its IP address or server name.

```
device(config-dhcp-cabo)# tftp-server 10.7.5.48
device(config-dhcp-cabo)# tftp-server tftp.domain.com
```

   The first example configures a TFTP server by specifying its IP address, while the second example configures a TFTP server by specifying its server name.

Configuring a vendor type and configuration value for a DHCP client

You can specify the vendor type and configuration value for the DHCP client. The value can be represented in ASCII characters, a hexadecimal string, or an IP address.

1. Enter global configuration mode by issuing the **configure terminal** command.

```
device# configure terminal
```

2. Create and enter DHCP server pool configuration mode.

```
device(config)# ip dhcp-server pool cabo
```

3. Specify the vendor type and configuration value for the DHCP client.

```
device(config-dhcp-cabo)# vendor class ascii waikiki
```

Configuring X Window System Display Manager IP addresses (option 49)

Option 49 of RFC 2132 specifies a list of IP addresses of systems that are running the X Window System Display Manager and are available to the client.

The X Window client is a DHCP client in a network that solicits configuration information by broadcasting a DHCP discovery packet on bootup or when the DHCP client is enabled. The DHCP server provides the IP addresses of systems running the X Window System Display Managers available in the network in their preferred order as part of the DHCP offer message.

On receipt of a discovery packet from the client, a DHCP offer message must be sent back. Option 49 must be added with the IP addresses of systems running the X Window System Display Manager in the network, along with other mandatory options. You can configure a maximum of three IP addresses in a DHCP server pool.

NOTE
Option 49 is ignored if the client is a non-X Window client.

1. Enter global configuration mode.

```
device# configure terminal
```

2. Configure an address pool in the DHCP server and enter DHCP server pool configuration mode.

```
device(config)# ip dhcp-server pool cabo
```

3. Enter the **xwindow-manager** command along with the IP addresses of the X Window System Display Managers separated by spaces.

```
device(config-dhcp-cabo)# xwindow-manager 10.38.12.1 10.38.12.3 10.38.12.5
```

The following example configures the IP addresses of systems running the X Window System Display Manager in the DHCP configuration pool.

```
device# configure terminal
device(config)# ip dhcp-server pool cabo
device(config-dhcp-cabo)# xwindow-manager 10.38.12.1 10.38.12.3 10.38.12.5
```

Configuring vendor details and vendor specific information (option 43 and option 60)

Ruckus devices running as DHCP servers can be configured with option 43 and option 60.

Configuring the DHCP option 60 helps in identifying the incoming DHCP client. If the vendor class identifier (VCI) advertised by the DHCP client matches with the DHCP server, the server makes a decision to exchange the vendor-specific information (VSI) configured as part of DHCP option 43.

The Ruckus ICX DHCP server can recognize the DHCP client device using the VCI (option 60) and pass specific information to this device type only (using option 43). However, the DHCP server can be configured to always pass additional information using option 43 (regardless of the client).

1. Enter global configuration mode.

```
device# configure terminal
device(config)#
```

2. Create a DHCP server pool.

```
device(config)# ip dhcp-server pool ruckus
```

NOTE
Save the configuration to retain the configuration through warm or cold reboots.

3. Add option 60 using the **vendor-class** command.

```
device(ip dhcp-server pool ruckus)# vendor-class ascii “Ruckus CPE”
```

NOTE
If the **ascii** option contains a space, you must enter it with double quotes as shown in the previous example.

4. Add the option 43 line using the **option** command.

```
device(ip dhcp-server pool ruckus)# option 43 ascii 192.168.10.1,192.168.20.01,192.168.30.1
```

or

```
device(ip dhcp-server pool ruckus)# option 43 hex 0108c0a80a01c0a81401
```

5. Deploy the configuration using the **deploy** command.

```
device(ip dhcp-server pool ruckus)# deploy
```

The following example configures option 60 and option 43 (hex) for a Ruckus Access Point (AP).

```
device# configure terminal
device(config)# ip dhcp-server pool ruckus
device(ip dhcp-server pool ruckus)# vendor-class ascii "Ruckus CPE"
device(ip dhcp-server pool ruckus)# option 43 hex 010cc0a80a01c0a81401c0a81e01
device(ip dhcp-server pool ruckus)# deploy
```

The following example configures option 60 and option 43 (ASCII) for a Ruckus AP.

```
device# configure terminal
device(config)# ip dhcp-server pool ruckus
device(ip dhcp-server pool ruckus)# vendor-class ascii "Ruckus CPE"
device(ip dhcp-server pool ruckus)# option 43 ascii 192.168.10.1,192.168.20.01,192.168.30.1
device(ip dhcp-server pool ruckus)# deploy
```

Enabling static IP to MAC address mapping

Based on the client MAC address, you can statically configure the IP address to the MAC address in the DHCP server.

This configuration is useful when you want to have selected clients assigned with particular IP addresses from the server. Whenever a DHCP discover message is received from these clients, based on the static configuration, the IP address will be assigned with the other required parameters.

1. Enter global configuration mode.

```
device# configure terminal
device(config)#
```

2. Create a DHCP server pool.

```
device(config)# ip dhcp-server pool cabo
```

3. Enter the **static-mac-ip-mapping** command followed by the IP address and MAC address for mapping.

```
device(config-dhcp-cabo)# static-mac-ip-mapping 10.10.10.29 0010.9400.0005
```

The following example enables the static MAC address to IP address mapping.

```
device# configure terminal
device(config)# ip dhcp-server pool cabo
device(config-dhcp-cabo)# static-mac-ip-mapping 10.10.10.29 0010.9400.0005
```

Configuring Avaya IP telephony (options 176 and 242)

Avaya IP telephones use site-specific options 176 and 242 as a method to obtain parameters from the DHCP server.

On receipt of a discovery packet from the Avaya IP telephone client, a DHCP offer message must be sent back. Options 176 and 242 must be added with the details of IP telephony voice and data servers present in the network, along with mandatory options.

- Option 176 is used for voice server representation.
- Option 242 is used for data servers.

NOTE
Options 176 and 242 are ignored for non-Avaya IP telephone clients.

1. Enter global configuration mode.

```
device# configure terminal
```

2. Configure an address pool in the DHCP server and enter DHCP server pool configuration mode.

```
device(config)# ip dhcp-server pool cabo
```

3. Enter the **ip-telephony data** command followed by the supported parameters. The parameters you can add for IP telephony data are **mcipadd**, **mcport**, **httpsrvr**, **l2qaud**, **l2qsig**, **l2qvlan**, **tftpsrvr**, **tlssrvr**, and **vlantest**.

   The following example specifies the MCIP address and MCPORT of the data server.

```
device(config-dhcp-cabo)# ip-telephony data mcipadd 1.1.1.2 mcport 1719
```

4. Enter the **ip-telephony voice** command followed by the supported parameters. The parameters you can add for IP telephony voice are **mcipadd**, **mcport**, **httpsrvr**, **l2qaud**, **l2qsig**, **l2qvlan**, **tftpsrvr**, **tlssrvr**, and **vlantest**.

   The following example specifies the MCIP address and MCPORT of the voice server.

```
device(config-dhcp-cabo)# ip-telephony voice mcipadd 1.1.1.2 mcport 1719
```

5. Deploy the DHCP address pool.
6. Enter the **show ip dhcp-server address-pools** command to verify the configured IP telephony options.

```
device(config)# show ip dhcp-server address-pools

Showing all address pool(s):
                    Pool Name:  test
 Time elapsed since last save:  00d:00h:01m:21s
Total number of active leases:  1
           Address Pool State:  active
      Pool Configured Options:
                         lease:  1 0 0
ip-telephony-voice-server: MCIPADD=192.168.42.1,MCPORT=1719,TFTPSRVR=192.168.42.1
ip-telephony-data-server: MCIPADD=192.168.42.1,MCPORT=1719,TFTPSRVR=192.168.42.1
                     network:  50.50.50.0 255.255.255.0
```

Configuring WPAD (option 252)

The Web Proxy Auto-Discovery (WPAD) protocol is used by web browsers to locate a Proxy Auto-Config (PAC) file automatically.

The WPAD protocol can use a DNS or DHCP server to locate a PAC file. DHCP detection involves the URL being pushed to the user in the DHCP assignment, while DNS detection is based on an informed guess, using known information about the DNS. A web browser that supports both methods checks the DHCP assignment first, and then attempts the DNS method. If the browser is unable to load a PAC file through the DHCP or DNS methods, it will allow direct Internet access.

NOTE
The PAC file must have the file name wpad.dat for the DNS method to function.

1. Enter global configuration mode.

```
device# configure terminal
```

2. Configure an address pool in the DHCP server and enter DHCP server pool configuration mode.

```
device(config)# ip dhcp-server pool cabo
```

3. Enter the **wpad** command followed by the full network location of the PAC file.

```
device(config-dhcp-cabo)# wpad http://172.26.67.243:8080/wpad.dat
```

4. Enter the **show ip dhcp-server address-pools** command to view the configured network location of the PAC file.

```
device(config)# show ip dhcp-server address-pools

Showing all address pool(s):
                    Pool Name:  test
 Time elapsed since last save:  00d:00h:01m:21s
Total number of active leases:  1
           Address Pool State:  active
      Pool Configured Options:
                        lease:  1 0 0
                        wpad: http://172.26.67.243:8080/wpad.dat
                      network:  50.50.50.0 255.255.255.0
```

Displaying DHCP server information

The following DHCP show commands can be entered from any level of the CLI.

Use one of the commands to view DHCP server information. The commands do not need to be entered in the specified order.

- Display a specific active lease, or all active leases.

```
device# show ip dhcp-server binding
Bindings from all pools:
IP Address Client-ID/ Lease expiration Type
Hardware address
192.168.1.2 0000.005d.a440 0d:0h:29m:31s Automatic
192.168.1.3 0000.00e1.26c0 0d:0h:29m:38s Automatic
```

- Display information about a specific address pool or all address pools.

```
device# show ip dhcp-server address-pools
Showing all address pool(s):

                       Pool Name:  dhcp
    Time elapsed since last save:  00d:00h:00m:00s
   Total number of active leases:  0
              Address Pool State:  pending

         Pool Configured Options:
                           lease:  1 0 0
                         network:  10.10.10.0 255.255.255.0
option   3 (Default-Router     ):  ip 10.10.10.1
option   6 (Domain Server      ):  ip 192.168.1.100
option  15 (Domain Name        ):  ascii example.com
option  44 (NETBIOS Name Srv   ):  ip 192.168.1.101
option  60 (Vendor Class Id    ):  hex 00
option  67 (Bootfile-Name      ):  ascii example.bin
option 150 (TFTP Server Addr   ):  ip 192.168.1.103
option 176 (IP Tele-VoiceSrvr  ):  MCIPADD=10.10.10.1,MCPORT=5,HTTPSRVR=20.20.20.1,L2QAUD=5,
option 242 (IP Tele-DataSrvr   ):  MCIPADD=10.10.10.1,
```

- Display the lease binding database that is stored in flash memory.

```
device# show ip dhcp-server flash
Address Pool Binding:
```

```
IP Address Client-ID/ Lease expiration Type
Hardware address
192.168.1.2 0000.005d.a440 0d:0h:18m:59s Automatic
192.168.1.3 0000.00e1.26c0 0d:0h:19m:8s Automatic
```

- Display information about active leases, deployed address pools, undeployed address pools, and server uptime.

```
device# show ip dhcp-server summary
DHCP Server Summary:
Total number of active leases: 2
Total number of deployed address-pools: 1
Total number of undeployed address-pools: 0
Server uptime: 0d:0h:8m:27s
```

- Display DHCP configuration information on a Layer 2 device.

```
device(config)# show ip
Switch IP address: 10.44.16.116
Subnet mask: 255.255.255.0
Default router address: 10.44.16.1
TFTP server address: 10.44.16.41
Configuration filename: foundry.cfg
Image filename: None
```

- Display IP address information for a Layer 2 device.

```
device(config)# show ip address
IP Address Type Lease Time Interface
10.44.16.116 Dynamic 174 0/1/1
```

- Display IP address information for a Layer 3 device.

```
device(config)# show ip address
IP Address Type Lease Time Interface
10.44.3.233 Dynamic 672651 0/1/2
10.0.0.1 Static N/A 0/1/15
```

- Display the Layer 2 device configuration using the **show run** command.

```
device(config)# show run
Current configuration:
!
ver 08.0.40
!
module 1 icx-24-port-base-module
!
!ip dns domain-list englab.ruckuswireless.com
ip dns domain-list companynet.com
ip dns server-address 10.31.2.10
ip route 0.0.0.0/0 10.25.224.1
!ipv6 raguard policy p1
!ipv6 dns server-address 200::1 8000::60 7000::61
!!
end
```

- Display the Layer 3 device configuration using the **show run** command.

```
device(config)# show run
Current configuration:
!
ver 08.0.40
!
module 1 icx7750-20-qxg-port-management-module
module 2 icx7750-qsfp-6port-qsfp-240g-module
!
vlan 1 name DEFAULT-VLAN by port
!
ip dns server-address 10.44.3.111
```

```
interface ethernet 0/1/2
ip address 10.44.3.233 255.255.255.0 dynamic
ip dhcp-client lease 691109
interface ethernet 0/1/15
ip address 10.0.0.1 255.0.0.0
ip helper-address 1 10.44.3.111
!
end
```

DHCPv4

- DHCPv4 overview 57
- DHCP Assist configuration 57
- Dynamic ARP Inspection overview 61
- DHCP snooping 68
- DHCP relay agent information and option 82 insertion 73
- IP Source Guard 79

DHCPv4 overview

The Dynamic Host Configuration Protocol for DHCPv4 enables DHCP servers to pass configuration parameters such as IPv4 addresses to IPv4 hosts.

On FastIron devices, you can configure Dynamic ARP Inspection, DHCPv4 snooping, and IP Source Guard together. The Ruckus implementation of these features provides enhanced network security by filtering untrusted DHCP packets.

The Dynamic Host Configuration Protocol (DHCP) is based on the Bootstrap Protocol (BOOTP) and provides configuration parameters such as IP addresses, default routes, DNS server addresses, access control, QoS policies, and security policies stored in DHCP server databases to DHCP clients upon request. DHCP enables the automatic configuration of client systems. DHCP removes the need to configure devices individually. Clients can set network properties by connecting to the DHCP server instead. This protocol consists of two components; a protocol to deliver host-specific configuration parameters from a DHCP server to a host, and a mechanism to allocate network addresses to hosts.

DHCP is built on a client-server model, where designated DHCP server hosts allocate network addresses and deliver configuration parameters to dynamically configured hosts.

DHCP Assist configuration

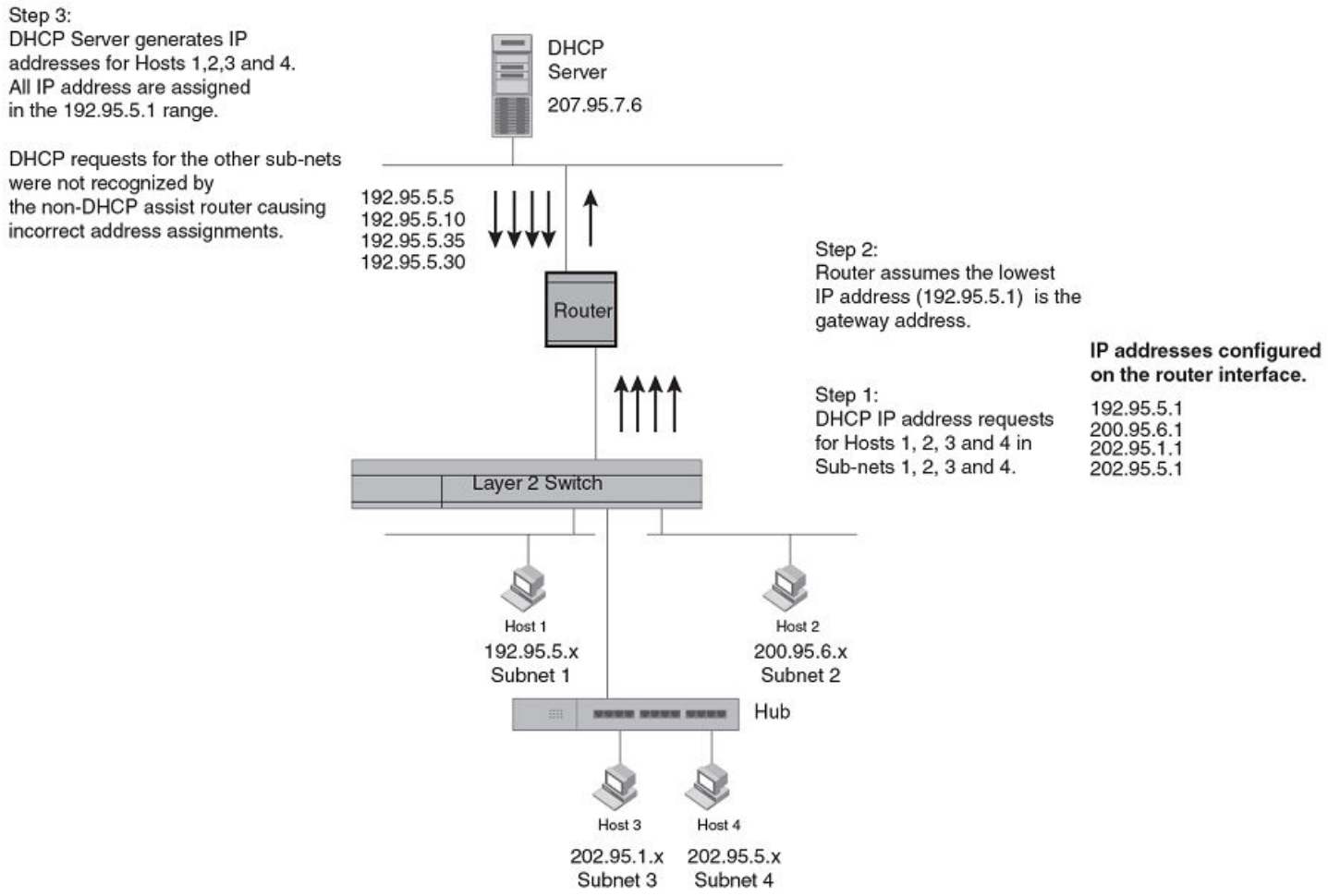
DHCP Assist allows a Ruckus Layer 2 switch to assist a router that is performing multi-netting on its interfaces as part of its DHCP relay function.

DHCP Assist ensures that a DHCP server that manages multiple IP subnets can readily recognize the requester IP subnet, even when that server is not on the client local LAN segment. The Ruckus Layer 2 switch does so by stamping each request with its IP gateway address in the DHCP discovery packet.

NOTE
Ruckus Layer 2 switches provide BOOTP/DHCP assistance by default on an individual port basis. Refer to Changing the IP address used for stamping BOOTP and DHCP requests in the *Ruckus FastIron Layer 3 Routing Configuration Guide*.

By allowing multiple subnet DHCP requests to be sent on the same wire, you can reduce the number of router ports required to support secondary addressing, as well as reduce the number of DHCP servers required by allowing a server to manage multiple subnet address assignments.

FIGURE 6 DHCP requests in a network without DHCP Assist on the Layer 2 switch



In a network operating without DHCP Assist, hosts can be assigned IP addresses from the wrong subnet range because a router with multiple subnets configured on an interface cannot distinguish among DHCP discovery packets received from different subnets.

In the example depicted, a host from each of the four subnets supported on a Layer 2 switch requests an IP address from the DHCP server. These requests are sent transparently to the router. Because the router is unable to determine the origin of each packet by subnet, it assumes the lowest IP address or the "primary address" is the gateway for all ports on the Layer 2 switch and stamps the request with that address.

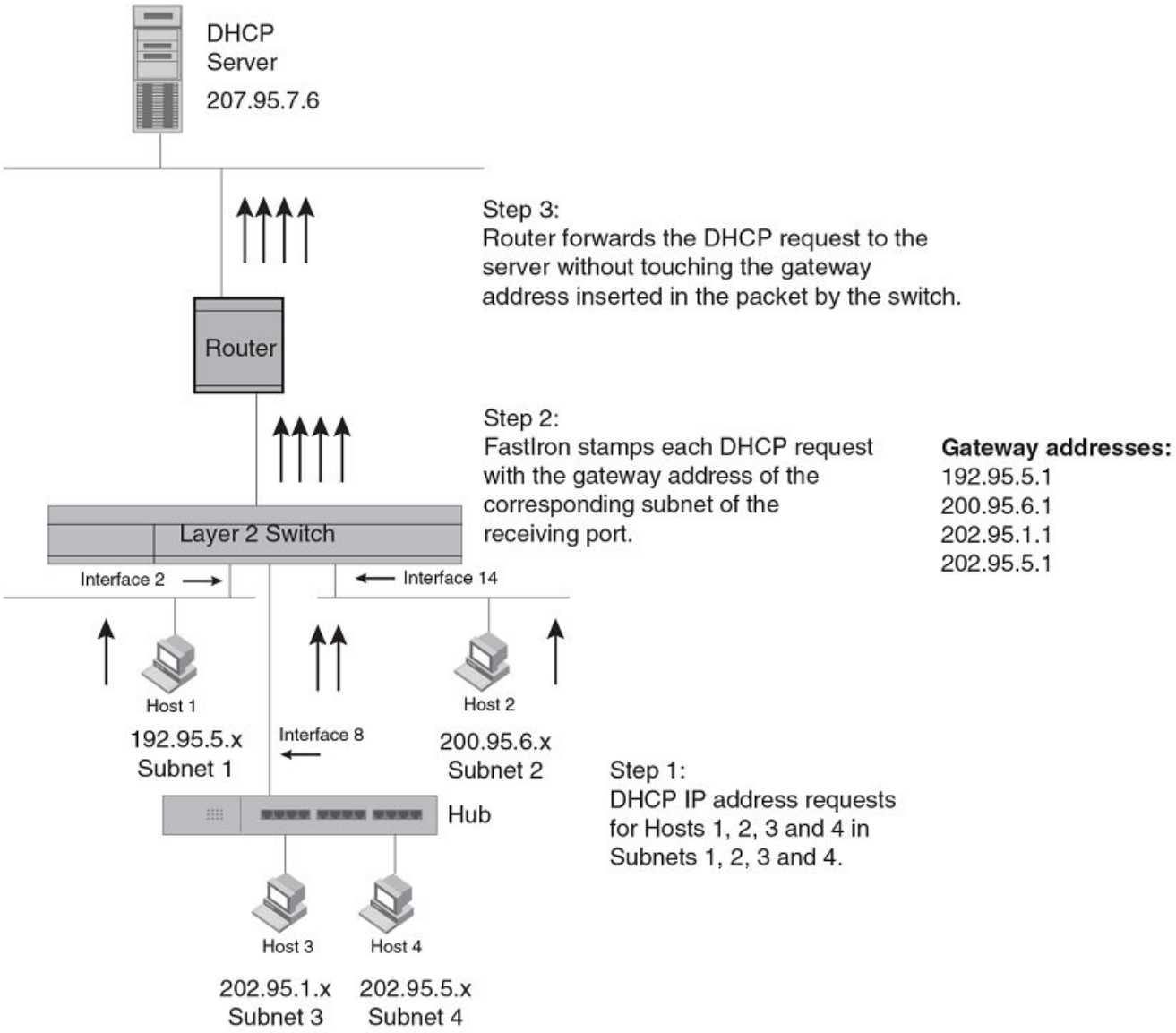
When the DHCP request is received at the server, it assigns all IP addresses within that range only.

With DHCP Assist enabled on a Ruckus Layer 2 switch, correct assignments are made because the Layer 2 switch provides the stamping service.

How DHCP Assist works

Upon initiation of a DHCP session, the client sends out a DHCP discovery packet for an address from the DHCP server. When the DHCP discovery packet is received at a Ruckus Layer 2 switch with the DHCP Assist feature enabled, the gateway address configured on the receiving interface is inserted into the packet. This address insertion is also referred to as stamping.

FIGURE 7 DHCP requests in a network with DHCP Assist operating on a FastIron switch

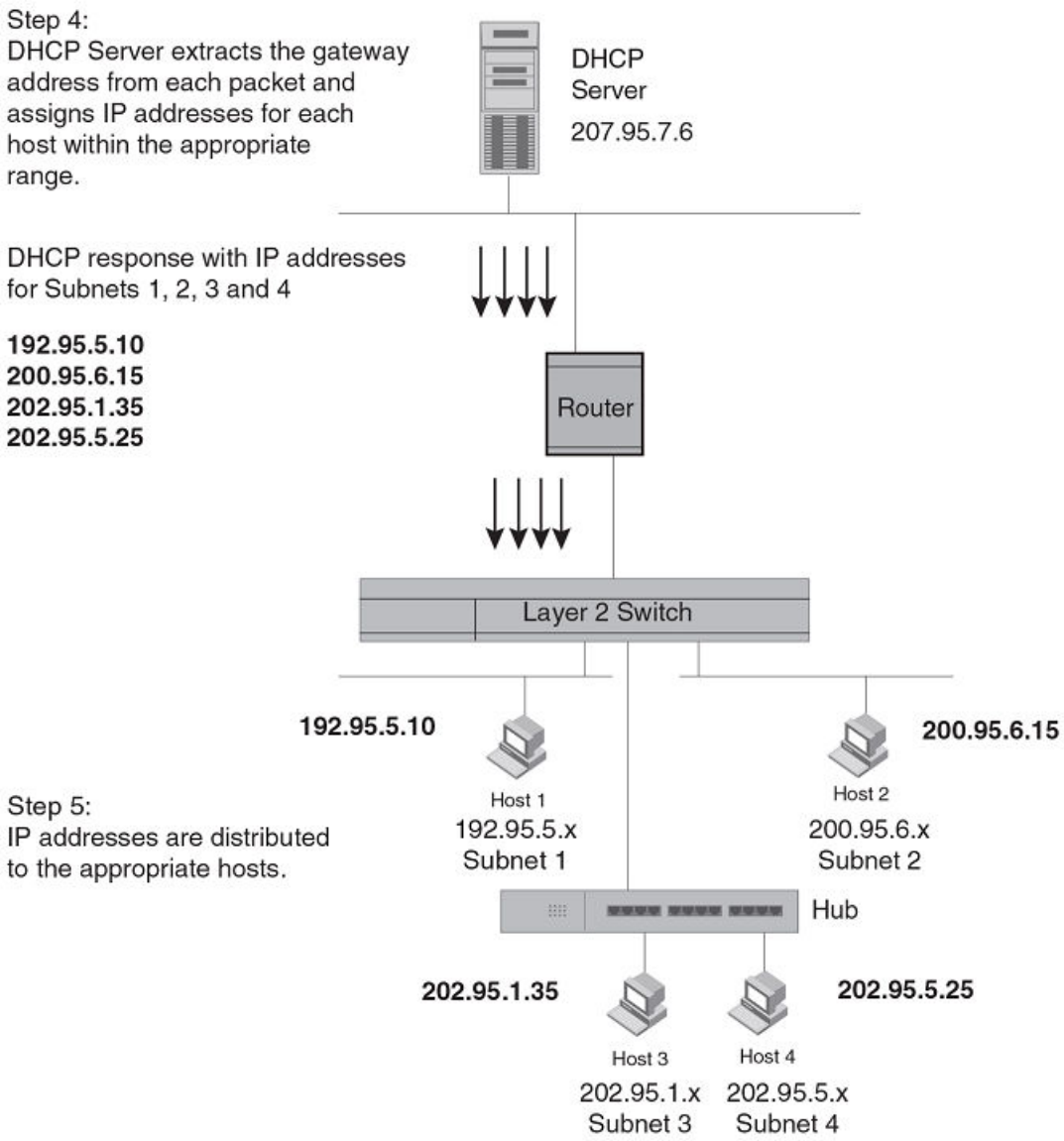


When the stamped DHCP discovery packet is then received at the router, it is forwarded to the DHCP server. The DHCP server then extracts the gateway address from each request and assigns an available IP address within the corresponding IP subnet. The IP address is then forwarded back to the workstation that originated the request.

NOTE
When DHCP Assist is enabled on any port, Layer 2 broadcast packets are forwarded by the CPU. Unknown unicast and multicast packets are still forwarded in hardware, although selective packets such as IGMP, are sent to the CPU for analysis. When DHCP Assist is not enabled, Layer 2 broadcast packets are forwarded in hardware.

NOTE
The DHCP relay function of the connecting router must be turned on.

FIGURE 8 DHCP offers are forwarded back toward the requesters



Configuring DHCP Assist

You can associate a gateway list with a port. You must configure a gateway list when DHCP Assist is enabled on a Ruckus Layer 2 switch.

The gateway list contains a gateway address for each subnet that will be requesting addresses from a DHCP server. The list allows the stamping process to occur. Each gateway address defined on the Layer 2 switch corresponds to an IP address of the Ruckus router interface or other router involved.

When multiple IP addresses are configured for a gateway list, the Layer 2 switch inserts the addresses into the discovery packet in a round-robin fashion. Up to 32 gateway lists can be defined for each Layer 2 switch.

1. Enter global configuration mode by issuing the **configure terminal** command.

```
device# configure terminal
```

2. Configure the required gateway lists. Up to eight addresses can be defined for each gateway list in support of ports that are multihomed.

```
device(config)# dhcp-gateway-list 1 10.95.5.1
device(config)# dhcp-gateway-list 2 10.95.6.1
device(config)# dhcp-gateway-list 3 10.95.1.1 10.95.5.1
```

3. Enter interface configuration mode and associate gateway list 1 with interface 1/1/2.

```
device(config)# interface ethernet 1/1/2
device(config-if-e1000-1/1/2)# dhcp-gateway-list 1
```

4. Associate gateway list 2 with interface 1/1/8.

```
device(config)# interface ethernet 1/1/8
device(config-if-e1000-1/1/8)# dhcp-gateway-list 2
```

5. Associate gateway list 3 with interface 1/1/14

```
device(config)# interface ethernet 1/1/14
device(config-if-e1000-1/1/14)# dhcp-gateway-list 3
```

Dynamic ARP Inspection overview

For enhanced network security, you can configure the Ruckus device to inspect and keep track of Dynamic Host Configuration Protocol (DHCP) assignments.

Dynamic ARP Inspection (DAI) enables the Ruckus device to intercept and examine all ARP request and response packets in a subnet and discard packets with invalid IP-to-MAC address bindings. DAI can prevent common man-in-the-middle (MiM) attacks such as ARP cache poisoning, and disallow misconfiguration of client IP addresses.

DAI allows only valid ARP requests and responses to be forwarded and supports Multi-VRFs with overlapping address spaces.

ARP poisoning

ARP provides IP communication within a Layer 2 broadcast domain by mapping an IP address to a MAC address. Before a host can talk to another host, it must map the IP address to a MAC address first. If the host does not have the mapping in its ARP table, it creates an ARP request to resolve the mapping. All computers on the subnet receive and process the ARP requests, and the host whose IP address matches the IP address in the request sends an ARP reply.

An ARP poisoning attack can target hosts, switches, and routers connected to the Layer 2 network by poisoning the ARP caches of systems connected to the subnet and by intercepting traffic intended for other hosts on the subnet. For instance, a malicious host can reply to an ARP request with its own MAC address, thereby causing other hosts on the same subnet to store this information in their ARP tables or replace the existing ARP entry. Furthermore, a host can send gratuitous replies without having received any ARP requests. A malicious host can also send out ARP packets claiming to have an IP address that actually belongs to another host (for example, the default router). After the attack, all traffic from the device under attack flows through the attacker computer and then to the router, switch, or host.

How Dynamic ARP Inspection works

Dynamic ARP Inspection (DAI) allows only valid ARP requests and responses to be forwarded.

A Ruckus device on which DAI is configured does the following:

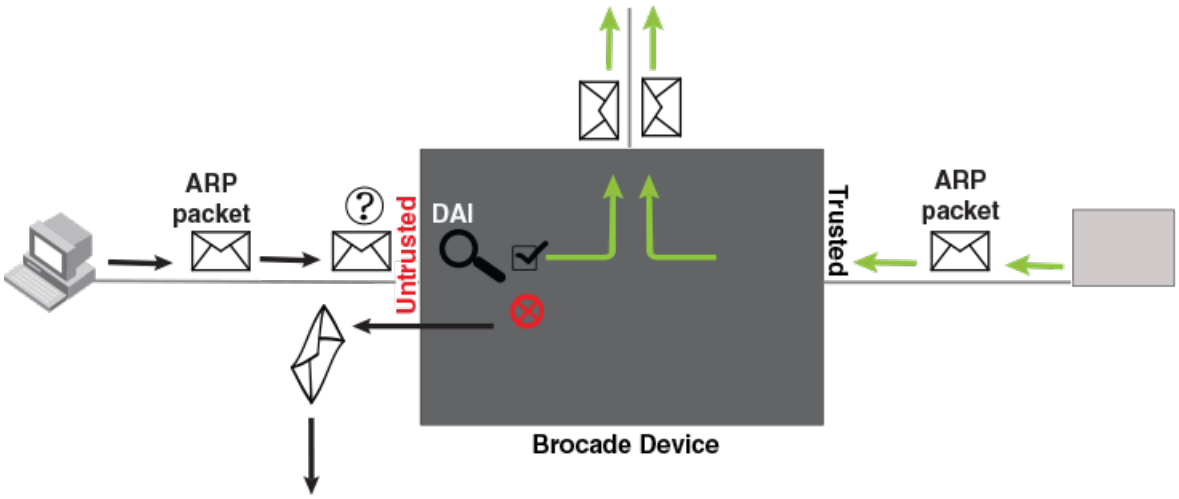
- Intercepts ARP packets received by the system CPU
- Inspects all ARP requests and responses received on untrusted ports
- Verifies that each of the intercepted packets has a valid IP-to-MAC address binding before updating the local ARP table, or before forwarding the packet to the appropriate destination
- Drops invalid ARP packets.

When you enable DAI on a VLAN, by default, all member ports are untrusted. You must manually configure trusted ports. In a typical network configuration, ports connected to host ports are untrusted. You configure ports connected to other switches or routers as trusted.

DAI inspects ARP packets received on untrusted ports, as shown in the following figure. DAI carries out the inspection based on IP-to-MAC address bindings stored in a trusted binding database. For the Ruckus device, the binding database is the ARP table and the DHCP snooping table, which supports DAI, DHCP snooping, and IP Source Guard. To inspect an ARP request packet, DAI checks the source IP address and source MAC address against the ARP table. For an ARP reply packet, DAI checks the source IP, source MAC, destination IP, and destination MAC addresses. DAI forwards the valid packets and discards those with invalid IP-to-MAC address bindings.

When ARP packets reach a trusted port, DAI lets them through, as shown in the following figure.

FIGURE 9 Dynamic ARP Inspection at work



ARP and DHCP snoop entries

DAI uses the IP-to-MAC mappings in the ARP table to validate ARP packets received on untrusted ports. DAI relies on the following entries:

- Dynamic ARP - Normal ARP learned from trusted ports.
- Static ARP - Statically configured IP/MAC/port mapping.
- Inspection ARP - Statically configured IP-to-MAC mapping, where the port is initially unspecified. The actual physical port mapping will be resolved and updated from validated ARP packets.

- DHCP-Snooping ARP - Information collected from snooping DHCP packets when DHCP snooping is enabled on VLANs. DHCP snooping entries are stored in a different table and are not part of the ARP table.

The status of an ARP entry is either pending or valid:

- Valid - The mapping is valid, and the port is resolved. This is always the case for static ARP entries.
- Pending - For normal dynamic ARP entries before they are resolved. Their status changes to valid when they are resolved, and the port is mapped. Refer to System reboot and the binding database on page 69.

Configuration notes and feature limitations for DAI

The following configuration notes and limitations apply when configuring DAI:

- There is a limit on the number of static ARP inspection entries that can be configured. This is determined by the system-max parameter **max-static-inspect-arp-entries**. The maximum value is 1024. The default value is 512. Changing the system max values requires a system reload.
- ACLs are supported on member ports of a VLAN on which DHCP snooping and Dynamic ARP Inspection (DAI) are enabled.
- DAI is supported on a VLAN without a VE, or on a VE with or without an assigned IP address.
- DAI is supported on LAG ports.

Configuring Dynamic ARP Inspection

Dynamic ARP Inspection is disabled by default and the trust setting of ports is untrusted by default.

The following prerequisites apply while configuring Dynamic ARP Inspection:

- You must first configure static ARP and static inspection ARP entries for hosts on untrusted ports. Otherwise, when DAI checks ARP packets from these hosts against entries in the ARP table, it will not find any entries for them, and the Ruckus device will not allow or learn ARP from an untrusted host.
- To run Dynamic ARP Inspection, you must first enable support for ACL filtering based on VLAN membership or VE port membership. Enter the following commands to enable ACL-per-port-per-VLAN.

```
device# configure terminal
device(config)# enable ACL-per-port-per-vlan
device(config)# write memory
device(config)# exit
device# reload
```

NOTE
You must save the configuration with the **write memory** command and reload the software to place the change into effect.

To configure DAI, follow these steps.

1. Enter global configuration mode.

```
device# configure terminal
```

2. Configure an ARP inspection entry.

```
device(config)# arp 10.20.20.12 0000.0002.0003 inspection
```

   This command defines an ARP inspection entry in the static ARP table and maps the device IP address 10.20.20.12 with its MAC address, 0000.0002.0003. The ARP entry will be moved to the ARP table once the DAI receives a valid ARP packet with the matching IP and MAC addresses on a device port. Until then, the ARP entry will remain in Pend (pending) status.

3. **NOTE**
   Dynamic ARP Inspection must be enabled to use static ARP inspection entries.

   Enable Dynamic ARP Inspection on an existing VLAN.

```
device(config)# ip arp inspection vlan 2
```

   The command enables DAI on VLAN 2. ARP packets from untrusted ports in VLAN 2 will undergo DAI.

4. Enable trust on any ports that will bypass DAI.
   a) To enable trust on a port, enter interface configuration mode.

```
device(config)# interface ethernet 1/1/4
```

   b) Enable trust on the port.

```
device(config-if-e10000-1/1/4)# arp inspection trust
```

   These commands change the CLI to the interface configuration level of port 1/1/4 and set the trust setting of port 1/1/4 to trusted.

5. Enable DHCP snooping to populate the DHCP snooping IP-to-MAC address binding database. Refer to text on DHCP snooping for more information.

The following example configures a dynamic ARP inspection table entry, enables DAI on VLAN 2, and designates port 1/1/4 as trusted.

```
device# configure terminal
device(config)# enable ACL-per-port-per-vlan
device(config)# write memory
device(config)# exit
device# reload
device# configure terminal
device(config)# arp 10.20.20.12 0000.0002.0003 inspection
device(config)# ip arp inspection vlan 2
device(config)# interface ethernet 1/1/4
device(config-if-e10000-1/1/4)# arp inspection trust
```

Enabling or disabling DAI syslog messages

You can enable or disable syslog messages for Dynamic ARP Inspection.

Syslog messages are enabled by default on FastIron devices. Follow these steps to disable DAI messages.

1. Enter global configuration mode.

```
device# configure terminal
```

2. Enter the **ip arp inspection syslog disable** command to disable syslog messages.

```
device(config)# ip arp inspection syslog disable
```

3. To re-enable DAI syslog messages, use the **no** form of the command.

```
device(config)# no ip arp inspection syslog disable
```

The following example disables the syslog messages for DAI.

```
device# configure terminal
device(config)# ip arp inspection syslog disable
```

Displaying ARP information

You can use various show commands to view information about ARP.

Use the following commands to view ARP-related information. The commands do not need to be entered in the specified order, and can be used to view the ARP table as well as ARP inspection status and trusted or untrusted ports.

1. Display the ARP table.

```
device# show arp
Total number of ARP entries: 2
Entries in default routing instance:
No.   IP Address       MAC Address    Type     Age  Port             Status
1     10.1.1.100       0000.0000.0100 Dynamic  0    1/1/1*2/1/25     Valid
2     10.37.69.129     02e0.5215.cae3 Dynamic  0    mgmt1            Valid
```

   The output of this command displays all ARP entries in the system.

2. Display the ARP inspection status for a VLAN and the trusted and untrusted port.

```
device# show ip arp inspection vlan 2
IP ARP inspection VLAN 2: Disabled
  Trusted Ports :   ethernet 1/1/4
  Untrusted Ports : ethernet 2/1/1 to 2/1/3 ethernet 4/1/1 to 4/1/24 ethernet 6/1/1 to 6/1/4
ethernet 8/1/1 to 8/1/4
```

   This command displays DAI information for VLAN 2. DAI is disabled on the VLAN, and port 1/1/4 is the only trusted port.

3. Display ARP inspection entries.

   The following example displays ARP inspection entries with a specific Ethernet port.

```
device# show ip arp inspection entries e 1/3/2
Total Entries: 1
     IP Address   Mac Address      Port   vlan  VRF            Entry Type
     27.0.0.1     cc4e.246e.eb00   1/3/2  2700  default-vrf    arp_entry
```

   The following example displays ARP inspection entries with a specific IP address.

```
device# show ip arp inspection entries ip 27.0.0.1
     IP Address  Mac Address      Port    vlan    VRF          Entry Type
     27.0.0.1    cc4e.246e.eb00   1/3/2   2700    default-vrf  arp table entry
```

   The following example displays ARP inspection entries with a specific LAG.

```
device# show ip arp inspection entries lag 2
Total Entries: 263
     IP Address      Mac Address    Port   vlan  VRF            Entry Type
     27.1.0.1        0010.2710.04ed lg2    2701  default-vrf    dhcp snoop entry
     27.1.0.2        0010.2710.04ec lg2    2701  default-vrf    dhcp snoop entry
     27.1.0.3        0010.2710.04eb lg2    2701  default-vrf    dhcp snoop entry
     27.1.0.4        0010.2710.04ea lg2    2701  default-vrf    dhcp snoop entry
     27.1.0.5        0010.2710.04e9 lg2    2701  default-vrf    dhcp snoop entry
     27.1.0.6        0010.2710.04e8 lg2    2701  default-vrf    dhcp snoop entry
     27.1.0.7        0010.2710.04f1 lg2    2701  default-vrf    dhcp snoop entry
     27.1.0.8        0010.2710.04f0 lg2    2701  default-vrf    dhcp snoop entry
     27.1.0.9        0010.2710.04ef lg2    2701  default-vrf    dhcp snoop entry
     27.1.0.10       0010.2710.04ee lg2    2701  default-vrf    dhcp snoop entry
```

   The following example displays ARP inspection entries with a specific VLAN.

```
device# show ip arp inspection entries vlan 2702
Total Entries: 13
     IP Address      Mac Address    Port  vlan  VRF            Entry Type
     27.2.0.12       0010.2720.04e8 lg2   2702  default-vrf    dhcp snoop entry
     27.2.0.13       0010.2720.04e9 lg2   2702  default-vrf    dhcp snoop entry
     27.2.0.47       0010.2720.050b lg2   2702  default-vrf    dhcp snoop entry
     27.2.0.48       0010.2720.050c lg2   2702  default-vrf    dhcp snoop entry
     27.2.0.49       0010.2720.050d lg2   2702  default-vrf    dhcp snoop entry
     27.2.0.53       0010.2720.0511 lg2   2702  default-vrf    dhcp snoop entry
     27.2.0.54       0010.2720.0512 lg2   2702  default-vrf    dhcp snoop entry
     27.2.0.55       0010.2720.0513 lg2   2702  default-vrf    dhcp snoop entry
     27.2.0.56       0010.2720.0514 lg2   2702  default-vrf    dhcp snoop entry
     27.2.0.57       0010.2720.0515 lg2   2702  default-vrf    dhcp snoop entry
     27.2.0.141      0010.2720.0569 lg2   2702  default-vrf    dhcp snoop entry
     27.2.0.153      0010.2720.0575 lg2   2702  default-vrf    dhcp snoop entry
     27.2.0.162      0010.2720.057e lg2   2702  default-vrf    dhcp snoop entry
```

   The following example displays ARP inspection entries with a specific VLAN.

```
device# show ip arp inspection entries vlan 2702
Total Entries: 13
     IP Address      Mac Address    Port  vlan  VRF            Entry Type
     27.2.0.12       0010.2720.04e8 lg2   2702  default-vrf    dhcp snoop entry
     27.2.0.13       0010.2720.04e9 lg2   2702  default-vrf    dhcp snoop entry
     27.2.0.47       0010.2720.050b lg2   2702  default-vrf    dhcp snoop entry
     27.2.0.48       0010.2720.050c lg2   2702  default-vrf    dhcp snoop entry
     27.2.0.49       0010.2720.050d lg2   2702  default-vrf    dhcp snoop entry
     27.2.0.53       0010.2720.0511 lg2   2702  default-vrf    dhcp snoop entry
     27.2.0.54       0010.2720.0512 lg2   2702  default-vrf    dhcp snoop entry
     27.2.0.55       0010.2720.0513 lg2   2702  default-vrf    dhcp snoop entry
     27.2.0.56       0010.2720.0514 lg2   2702  default-vrf    dhcp snoop entry
     27.2.0.57       0010.2720.0515 lg2   2702  default-vrf    dhcp snoop entry
     27.2.0.141      0010.2720.0569 lg2   2702  default-vrf    dhcp snoop entry
     27.2.0.153      0010.2720.0575 lg2   2702  default-vrf    dhcp snoop entry
     27.2.0.162      0010.2720.057e lg2   2702  default-vrf    dhcp snoop entry
```

Configuring DAI to support Multi-VRF

DAI supports Multi-VRF (Virtual Routing and Forwarding) instances. You can deploy multiple VRFs on a Ruckus Ethernet switch. Each VLAN having a Virtual Ethernet (VE) interface is assigned to a VRF.

You can enable DAI on individual VLANs and assign any interface as the ARP inspection trusted interface. If an interface is a tagged port in this VLAN, you can turn on the trusted port per VRF, so that traffic intended for other VRF VLANs will not be trusted.

1. Enter global configuration mode by issuing the **configure terminal** command.

```
device# configure terminal
```

2. **NOTE**
   DAI requires that the ACL-per-port-per-VLAN setting be enabled.

   Enable the ACL-per-port-per-VLAN setting. You must save the setting and reload for it to take effect.

```
device(config)# enable acl-per-port-per-vlan
Reload required. Please write memory and then reload or power cycle.
device(config)# write memory
device(config)# exit
device# reload
```

   This example enables ACL-per-port-per-VLAN, saves the change, and reloads the device to make the change active.

3. Return to global configuration mode, and configure DAI on a VLAN.

```
device# configure terminal
device(config)# ip arp inspection vlan 2
```

   This example configures DAI on VLAN 2.

4. To add a static ARP inspection entry for a specific VRF, enter the VRF CLI context.

```
device(config)# vrf one-ipv4
```

5. Add a static ARP inspection entry for the VRF.

```
device(config-vrf-one-ipv4)# arp 5.5.5.5 00a2.bbaa.0033 inspection
```

   This example creates a static ARP inspection entry for the VRF named "one-ipv4."

Enabling trust on a port for a specific VRF

The default trust setting for a port is untrusted. Leave the trust settings for ports that are connected to host ports as untrusted.

The VRF must already exist.

1. Enter global configuration mode by issuing the **configure terminal** command.

```
device# configure terminal
```

2. Enter interface configuration mode.

```
device(config)# interface ethernet 1/1/4
```

3. Set the trust setting to **trust** for the specific VRF.

```
device(config-if-e10000-1/1/4)# arp inspection trust vrf vrf2
```

   This example configures the VRF named "vrf2" as a trusted VRF on port 1/1/4.

DHCP snooping

DHCP snooping enables the Ruckus device to filter untrusted DHCP packets in a subnet. DHCP snooping can ward off MiM attacks, such as a rogue DHCP server sending false DHCP server reply packets with the intention of misdirecting other users. DHCP snooping can also stop unauthorized DHCP servers and prevent errors stemming from user misconfiguration of DHCP servers.

DHCP snooping is often used with Dynamic ARP Inspection and IP Source Guard.

How DHCP snooping works

When enabled on a VLAN, DHCP snooping stands between untrusted ports (those connected to host ports) and trusted ports (those connected to DHCP servers). A VLAN with DHCP snooping enabled forwards DHCP request packets from clients and discards DHCP server reply packets on untrusted ports. DHCP server reply packets on trusted ports to DHCP clients are forwarded, as shown in the following figures.

FIGURE 10 DHCP snooping at work on an untrusted port

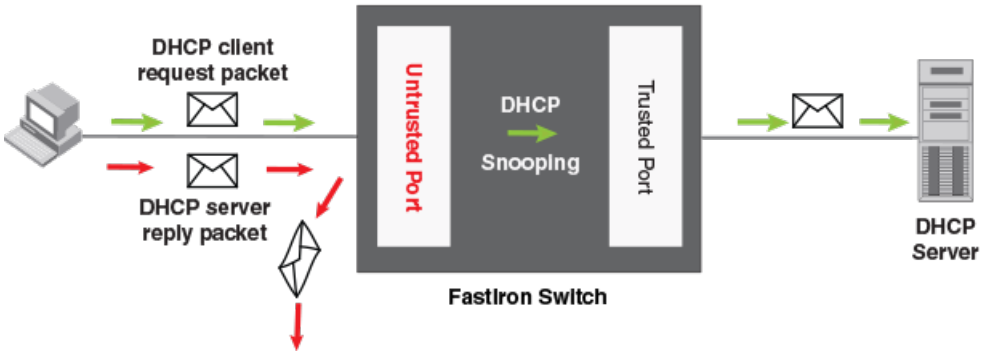
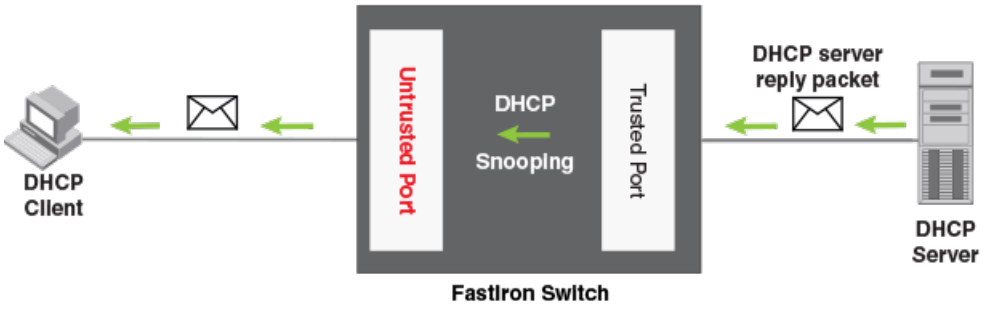


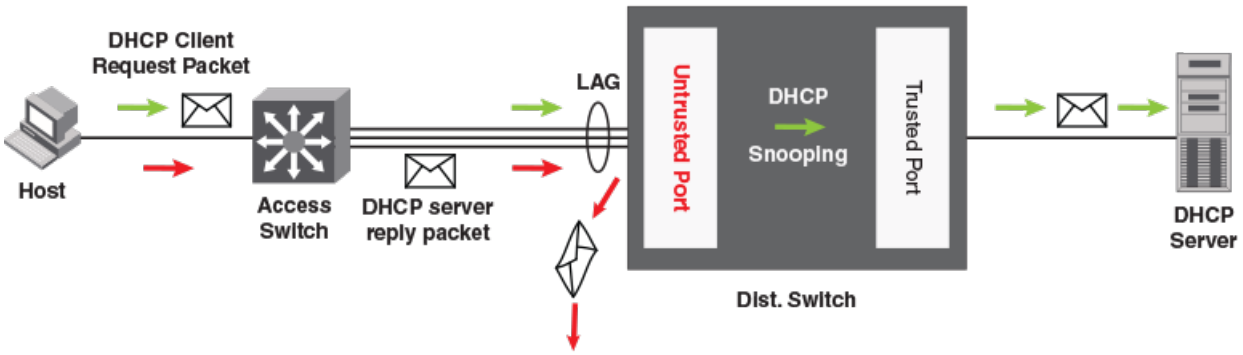
FIGURE 11 DHCP snooping at work on a trusted port



DHCP snooping deployment over a LAG

The following figure shows DHCP snooping deployment over a LAG. The LAG is between an access switch and distribution switch.

FIGURE 12 DHCP snooping deployment over a LAG



DHCP binding database

DHCP server reply packets are forwarded to DHCP clients on trusted ports. The DHCP server reply packets collect client IP-to-MAC address binding information, which is saved in the DHCP binding database. This information includes MAC addresses, IP addresses, lease time, VLAN numbers, and port numbers.

Beginning with FastIron release 8.0.30b, the DHCP binding database in the Ruckus device is decoupled from the ARP database. For more information, refer to ARP and DHCP snoop entries on page 62.

The lease time is refreshed when the client renews its IP address with the DHCP server; otherwise, the Ruckus device removes the entry when the lease time expires.

Client IP-to-MAC address mappings

Client IP addresses need not be on directly connected networks, as long as the client MAC address is learned on the client port and the client port is on the same VLAN as the DHCP server port. In this case, the system learns the client IP-to-MAC port mapping. Therefore, a VLAN with DHCP snooping enabled does not require a VE interface.

In earlier releases, in the Layer 3 software image, DHCP snooping did not learn the secure IP-to-MAC address mapping for a client, if the client port was not a Virtual Ethernet (VE) interface with an IP subnet address. In other words, the client IP address had to match one of the subnets of the client port in order for DHCP to learn the address mapping.

System reboot and the binding database

To allow DAI and DHCP snooping to work smoothly across a system reboot, the binding database is saved to a file in the system flash memory after an update to the binding database with a 30-second delay. The flash file is written and read only if DHCP snooping is enabled.

Configuration notes and feature limitations for DHCP snooping

The following limitations and restrictions apply to DHCP snooping:

- DHCP snooping is supported on LAG ports.
- DHCP snooping is supported on MCT clients. DHCP snooping is not supported on the MCT peer for the MCT VLAN.

- There is a limit on the maximum number of DHCP snooping entries that the device can learn. This is determined by the system-max parameter **max-dhcp-snoop-entries**. The maximum value is 3072 and the default value is 1024. This value is also applicable to the flash file where DHCP snooping entries are stored.
- DHCP snooping is not supported along with DHCP auto-configuration.
- You cannot apply MAC address filters on a VLAN member on which DHCP snooping is already enabled and vice versa.
- ACLs are supported on member ports of a VLAN on which DHCP snooping and Dynamic ARP Inspection (DAI) are enabled. Refer to Client IP-to-MAC address mappings on page 69.
- DHCP snooping supports DHCP relay agent information (DHCP option 82). Refer to DHCP relay agent information and option 82 insertion on page 73 for more information.
- For default VLAN ID changes, DHCP snooping and Dynamic ARP Inspection should be re-applied on the new default VLAN.

Configuring DHCP snooping

DHCP snooping should be enabled on VLANs, after which the trust setting of ports connected to a DHCP server must be changed to trusted. DHCP packets for a VLAN with DHCP snooping enabled are inspected.

To run DHCP snooping, you must first enable support for ACL filtering based on VLAN membership or VE port membership. Enter the following commands at the global configuration level.

```
device(config)# enable ACL-per-port-per-vlan
device(config)# write memory
device(config)# exit
device# reload
```

NOTE
You must save the configuration and reload the software for the changes to take effect.

NOTE
DHCP snooping is disabled by default and the trust setting of ports is untrusted by default. DHCP snooping must be enabled on the client and the DHCP server VLANs.

1. Enter global configuration mode by issuing the **configure terminal** command.

   ```
   device# configure terminal
   ```

2. Enable DHCP snooping on a VLAN.

   ```
   device(config)# ip dhcp snooping vlan 2
   ```

3. Change the trust setting of the ports that are connected to the DHCP server to trusted at the interface configuration level.

   ```
   device(config-if-e10000-1/1/1)# dhcp snooping trust
   ```

4. If required, disable the learning of DHCP clients on ports at the interface configuration level. Disabling the learning of DHCP clients can be configured on a range of ports as well.

   ```
   device(config-if-e10000-1/1/1)# dhcp snooping client-learning disable
   ```

5. Clear the DHCP binding database. You can remove all entries in the database or for a specific IP address only.

   The first command removes all entries from the DHCP binding database and the second removes entries for a specific IP address.

```
device# clear dhcp

device# clear dhcp 10.10.102.4
```

The following example configures VLAN 2 and VLAN 20, and changes the CLI to the global configuration level to enable DHCP snooping on the two VLANs.

```
device(config)# vlan 2
device(config-vlan-2)# untagged ethe 1/1/3 to 1/1/4
device(config-vlan-2)# router-interface ve 2
device(config-vlan-2)# exit
device(config)# ip dhcp snooping vlan 2
device(config)# vlan 20
device(config-vlan-20)# untagged ethe 1/1/1 to 1/1/2
device(config-vlan-20)# router-interface ve 20
device(config-vlan-20)# exit
device(config)# ip dhcp snooping vlan 20
```

On VLAN 2, client ports 1/1/3 and 1/1/4 are untrusted. By default all client ports are untrusted. Thus, only DHCP client request packets received on ports 1/1/3 and 1/1/4 are forwarded. On VLAN 20, ports 1/1/1 and 1/1/2 are connected to a DHCP server. DHCP server ports are set to trusted.

```
device(config)# interface ethernet 1/1/1
device(config-if-e10000-1/1/1)# dhcp snooping trust
device(config-if-e10000-1/1/1)# exit
device(config)# interface ethernet 1/1/2
device(config-if-e10000-1/1/2)# dhcp snooping trust
device(config-if-e10000-1/1/2)# exit
```

Thus, DHCP server reply packets received on ports 1/1/1 and 1/1/2 are forwarded, and client IP/MAC binding information is collected. The example also sets the DHCP server address for the local relay agent.

```
device(config)# interface ve 2
device(config-vif-2)# ip address 10.20.20.1/24
device(config-vif-2)# ip helper-address 1 10.30.30.4
device(config-vif-2)# interface ve 20
device(config-vif-20)# ip address 10.30.30.1/24
```

Displaying DHCPv4 snooping information

You can use various show commands to view information about DHCPv4 snooping.

Use one of the following commands to view DHCPv4 snooping information. The commands do not need to be entered in the specified order.

1. Display the DHCP snooping status for a VLAN and the trusted and untrusted ports in the VLAN.

```
device# show ip dhcp snooping vlan 2
IP DHCP snooping VLAN 2: Enabled
```

2. Display the DHCP snooping binding database.

   The following example displays the DHCP snooping binding database.

```
device# show ip dhcp snooping info
Dhcp snooping Info
Total learnt entries 10
Learnt DHCP Snoop Entries
IP Address      Mac Address    Port           Virtual Port   vlan  lease VRF
10.1.1.20       0000.0000.0001 1/1/1*2/1/25    v100           100   200   default-vrf
10.1.1.21       0000.0000.0002 1/1/1*2/1/25    v100           100   200   default-vrf
10.1.1.22       0000.0000.0003 1/1/1*2/1/25    v100           100   200   default-vrf
10.1.1.23       0000.0000.0004 1/1/1*2/1/25    v100           100   200   default-vrf
10.1.1.24       0000.0000.0005 1/1/1*2/1/25    v100           100   200   default-vrf
10.1.1.25       0000.0000.0006 1/1/1*2/1/25    v100           100   200   default-vrf
10.1.1.26       0000.0000.0007 1/1/1*2/1/25    v100           100   200   default-vrf
10.1.1.27       0000.0000.0008 1/1/1*2/1/25    v100           100   200   default-vrf
10.1.1.28       0000.0000.0009 1/1/1*2/1/25    v100           100   200   default-vrf
10.1.1.29       0000.0000.000a 1/1/1*2/1/25    v100           100   200   default-vrf
```

   The following example displays the IP DHCP snooping flash entries.

```
device# show ip dhcp snooping flash
Dhcp snooping Info
Total learnt entries 10
SAVED DHCP ENTRIES IN FLASH
  IP Address    Mac Address    Port           Virtual Port   vlan  lease VRF
1  10.1.1.20    0000.0000.0001 1/1/1*2/1/25   v100           100   170   default-vrf
2  10.1.1.21    0000.0000.0002 1/1/1*2/1/25   v100           100   170   default-vrf
3  10.1.1.22    0000.0000.0003 1/1/1*2/1/25   v100           100   170   default-vrf
4  10.1.1.23    0000.0000.0004 1/1/1*2/1/25   v100           100   170   default-vrf
5  10.1.1.24    0000.0000.0005 1/1/1*2/1/25   v100           100   170   default-vrf
6  10.1.1.25    0000.0000.0006 1/1/1*2/1/25   v100           100   170   default-vrf
7  10.1.1.26    0000.0000.0007 1/1/1*2/1/25   v100           100   170   default-vrf
8  10.1.1.27    0000.0000.0008 1/1/1*2/1/25   v100           100   170   default-vrf
9  10.1.1.28    0000.0000.0009 1/1/1*2/1/25   v100           100   170   default-vrf
10 10.1.1.29    0000.0000.000a 1/1/1*2/1/25   v100           100   170   default-vrf
```

Configuring DHCPv4 snooping for Multi-VRF

DHCP supports Multi-VRF (Virtual Routing and Forwarding) instances. You can deploy multiple VRFs on a Ruckus Ethernet switch. Each VLAN with a Virtual Ethernet (VE) interface is assigned to a VRF.

You can enable DHCP snooping on individual VLANs and assign any interface as the DHCP trust interface. If an interface is a tagged port in this VLAN, you can turn on the trust port per VRF, so that traffic intended for other VRF VLANs is not trusted

1. Enter global configuration mode by issuing the **configure terminal** command.

```
device# configure terminal
```

2. To configure DHCP snooping to support a Multi-VRF instance, enable the ACL-per-port-per-VLAN setting.

```
device(config)# enable acl-per-port-per-vlan
Reload required. Please write memory and then reload or power cycle.
```

3. Configure DHCP IPv4 snooping on a specific VLAN.

```
device(config)# ip dhcp snooping vlan 2
```

4. Set the port as a trusted port. The trust port setting for DHCP snooping can be specified per VRF.

```
device(config)# interface ethernet 1/1/4
device(config-if-e10000-1/1/4)# ip dhcp snooping trust vrf vrf2
```

   The default trust setting for a port is untrusted. For ports that are connected to host ports, leave their trust settings as untrusted.

5. Configure the IP helper address on the client port if the client and server are in the same VLAN and the client and server ports are Layer 3 interfaces with IP addresses.

```
device(config)# interface ve 2
device(config-vif-2)# ip helper-address 1 10.1.1.2
```

   If the client and server are in different VLANs, configure the server port as the trust port.

6. Clear any entry specific to a VRF instance, as required.

```
device(config)# clear dhcp 3.3.3.5 vrf one
```

DHCP relay agent information and option 82 insertion

DHCP relay agent information, also known as DHCP option 82, enables a DHCP relay agent to insert information about a client's identity into a DHCP client request being sent to a DHCP server. This option can be used to assist DHCP servers to implement dynamic address policy.

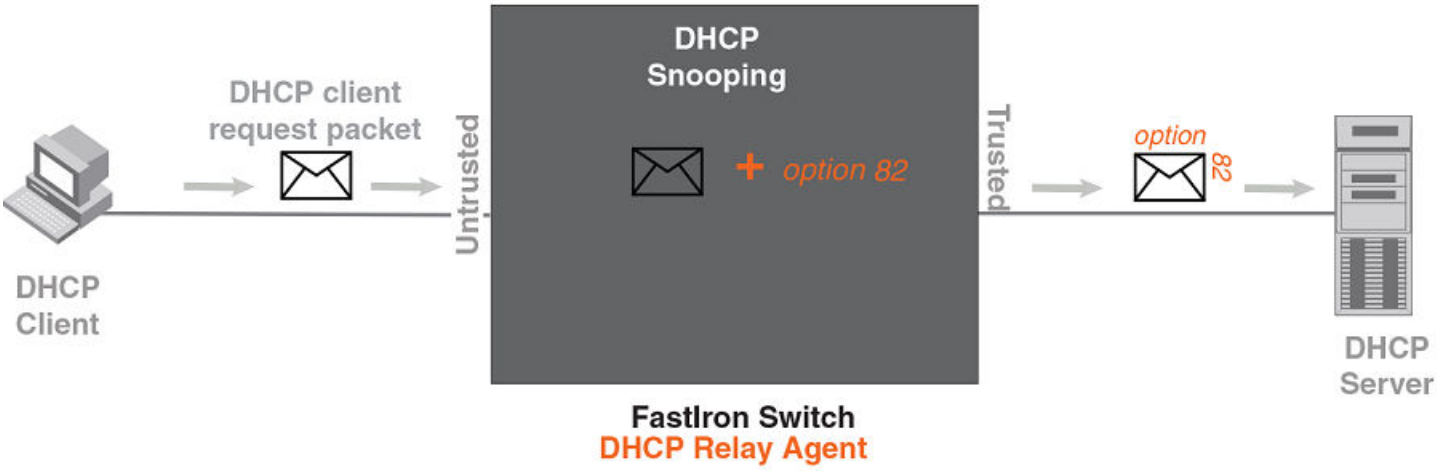
The Ruckus device inserts DHCP option 82 when relaying DHCP request packets to DHCP servers. When DHCP server reply packets are forwarded back to DHCP clients, and sub-option 2 as RID (remote ID) matches the local port MAC address, then DHCP option 82 is deleted. The vlan/port information is used to forward the DHCP reply.

DHCP packets are processed as follows:

- Before relaying a DHCP discovery packet or DHCP request packet from a client to a DHCP server, the FastIron switch adds agent information to the packet.
- Before relaying a DHCP reply packet from a DHCP server to a client, the FastIron switch removes relay agent information from the packet.

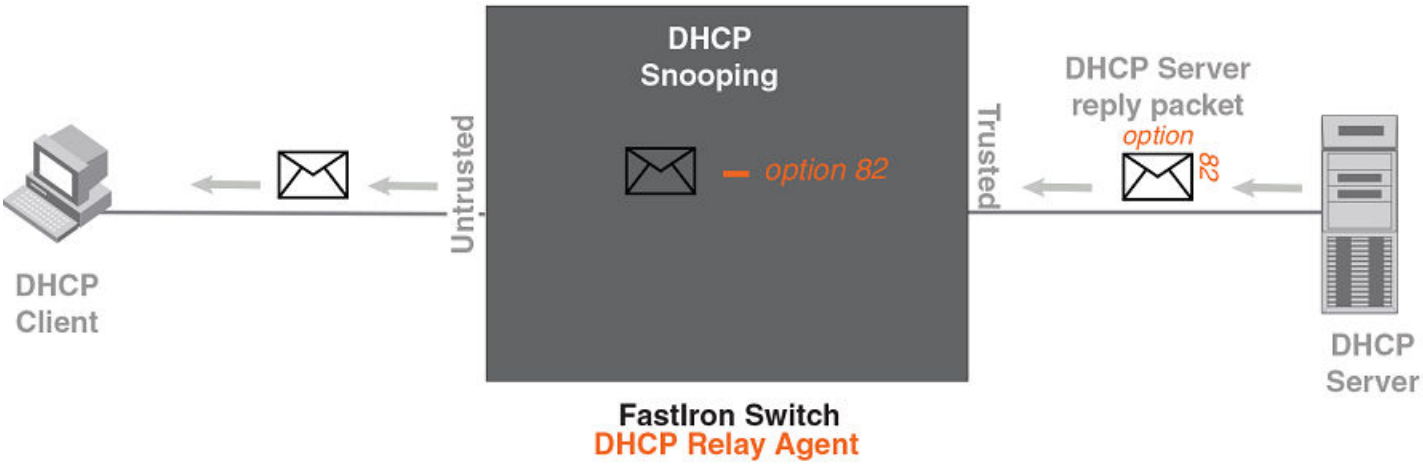
The DHCP relay agent (the FastIron switch) inserts DHCP option 82 attributes when relaying a DHCP request packet to a DHCP server.

FIGURE 13 DHCP option 82 attributes added to the DHCP packet



The FastIron switch deletes DHCP option 82 attributes before forwarding a server reply packet back to a DHCP client.

FIGURE 14 DHCP option 82 attributes removed from the DHCP packet



The DHCP option 82 insertion or deletion feature is available only when DHCP snooping is enabled on both client and server ports.

Configuration notes for DHCP option 82

- DHCP snooping and DHCP option 82 are supported on a per-VLAN basis.
- DHCP option 82 follows the same configuration rules and limitations described for DHCP snooping. For more information, refer to Configuration notes and feature limitations for DHCP snooping on page 69.

DHCP option 82 sub-options

The Ruckus implementation of DHCP option 82 supports the following sub-options:

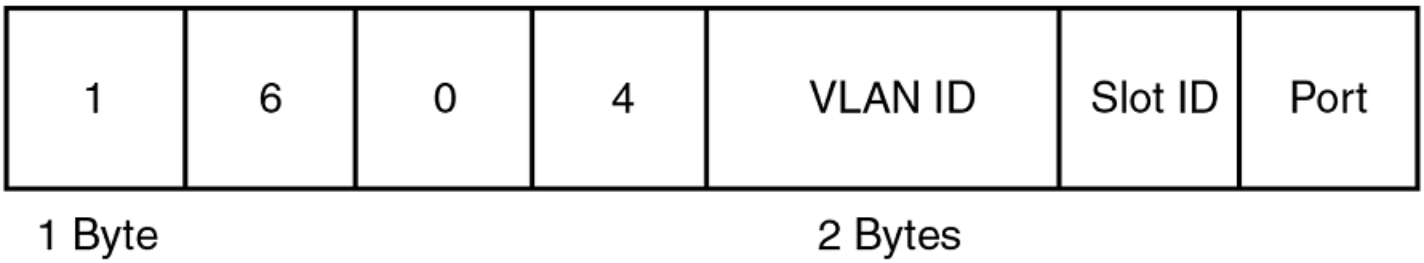
- Sub-option 1: Circuit ID
- Sub-option 2: Remote ID
- Sub-option 6: Subscriber ID

Sub-option 1: Circuit ID

The Circuit ID (CID) identifies the circuit or port from which a DHCP client request was sent. The FastIron switch uses this information to relay DHCP responses back to the proper circuit; for example, the port number on which the DHCP client request packet was received.

Ruckus FastIron devices support the general CID packet format. This simple format encodes the CID type, actual information length, VLAN ID, slot number, and port number. This format is compatible with the format used by other vendors' devices. The following figure illustrates the general CID packet format.

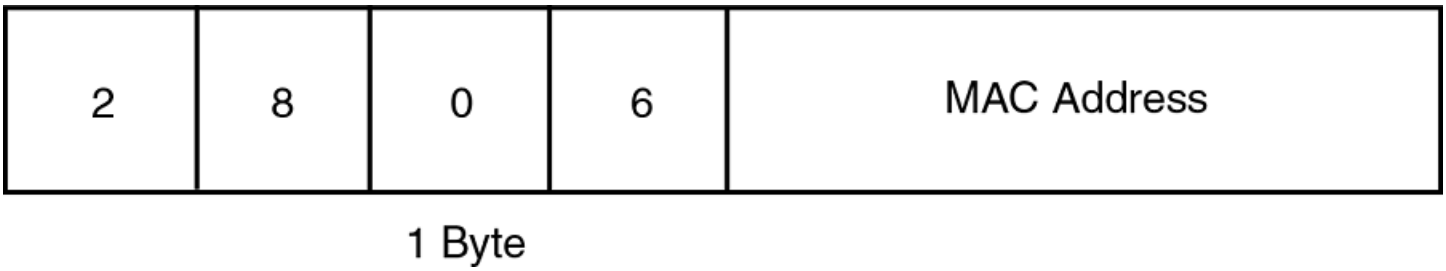
FIGURE 15 General CID packet format



Sub-option 2: Remote ID

The Remote ID (RID) identifies the remote host end of the circuit (the relay agent). Ruckus devices use the MAC address to identify itself as the relay agent. The following figure illustrates the RID packet format.

FIGURE 16 RID packet format



Sub-option 6: Subscriber ID

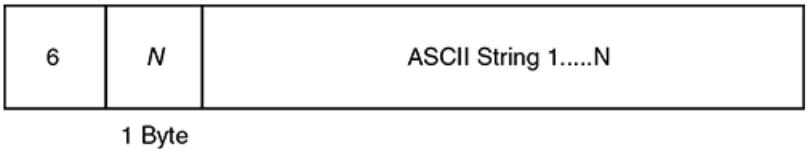
The Subscriber ID (SID) is a unique identification number that enables an Internet Service Provider (ISP) to perform the following actions:

- Identify a subscriber

- Assign specific attributes to that subscriber (for example, host IP address, subnet mask, and domain name server (DNS)
- Trigger accounting

The following figure illustrates the SID packet format.

FIGURE 17 SID packet format



The second byte (*N* in the figure) is the length of the ASCII string that follows. The FastIron switch supports up to 50 ASCII characters.

DHCP option 82 configuration

DHCP option 82 is enabled when you enable DHCP snooping on a VLAN. There are no additional configuration steps to enable DHCP option 82. Refer to Configuring DHCP snooping on page 70 to enable DHCP snooping.

When processing DHCP packets the FastIron switch applies the following default behavior when DHCP option 82 is enabled:

- Subjects all ports in the VLAN to DHCP option 82 processing
- Uses the general CID packet format
- Uses the standard RID packet format
- Replaces relay agent information received in DHCP packets with its own information
- Does not enable SID processing

When DHCP option 82 is enabled, you can optionally:

- Disable DHCP option 82 processing on individual ports in the VLAN
- Configure the device to drop or keep the relay agent information in a DHCP packet instead of replacing it with its own information
- Configure Subscriber ID (SID), Circuit ID (CID) or Remote ID (RID) processing.

Disabling or re-enabling DHCP option 82 processing on an interface

By default, when DHCP option 82 is enabled on a VLAN, DHCP packets received on all member ports of the VLAN are subject to DHCP option 82 processing. You can disable or re-enable this processing on one or more member ports of the VLAN.

Option 82 is automatically enabled when you enable DHCP snooping on the VLAN.

1. To disable Option 82, enter global configuration mode by issuing the **configure terminal** command.

```
device# configure terminal
```

2. Enter interface configuration mode.

```
device(config)# interface ethernet 1/1/4
```

3. Disable DHCP option 82 on the interface.

```
device(config-if-e1000-1/1/4)# no dhcp snooping relay information
```

4. Re-enable DHCP option 82, as required at the interface configuration level.

```
device(config-if-e1000-1/1/4)# dhcp snooping relay information
```

5. You can also re-enable DHCP option 82 after it has been disabled on a range of ports. First, specify the range of ports at the global configuration level and then enter the **dhcp snooping relay information** command.

```
device(config)# interface ethernet 1/1/1 to 1/1/5

device(config-mif-1/1/1-1/1/5)# dhcp snooping relay information
```

The following example disables DHCP option 82.

```
device# configure terminal
device(config)# interface ethernet 1/1/4
device(config-if-e1000-1/1/4)# no dhcp snooping relay information
```

The following example re-enables DHCP option 82 at the interface configuration level.

```
device# configure terminal
device(config)# interface ethernet 1/1/4
device(config-if-e1000-1/1/4)# dhcp snooping relay information
```

The following example re-enables DHCP option 82 on a range of ports.

```
device(config)# interface ethernet 1/1/1 to 1/1/5
device(config-mif-1/1/1-1/1/5)# dhcp snooping relay information
```

Changing the DHCP relay agent forwarding policy

When the device receives a message containing relay agent information, by default the device replaces the information with its own relay agent information. This behavior can be changed if required.

You can configure the device to keep the information instead of replacing it, or to drop (discard) messages that contain relay agent information.

1. Enter global configuration mode by issuing the **configure terminal** command.

```
device# configure terminal
```

2. Configure the device to keep the relay agent information contained in a DHCP message.

```
device(config)# ip dhcp relay information policy keep
```

3. Alternately, configure the device to drop the relay agent information contained in the DHCP message.

```
device(config)# ip dhcp relay information policy drop
```

4. Configure the device back to the default behavior if required.

```
device(config)# ip dhcp relay information policy replace
```

Configuring DHCP snooping relay information sub-options

You can configure DHCP relay agent sub-options such as the circuit-ID, remote-ID, or subscriber-ID options.

1. Enter global configuration mode.

```
device# configure terminal
```

2. Enable DHCP snooping and DHCP option 82 on a VLAN.

```
device(config)# ip dhcp snooping vlan 1
```

3. Enter interface configuration mode for port 1/1/4.

```
device(config)# interface ethernet 1/1/4
```

4. Enable interface 1/1/4 to insert the SID, CID, or RID information in the DHCP packets.

```
device(config-if-e1000-1/1/4)# dhcp snooping relay information subscriber-id Brcd01
```

   In the example above the SID is Brcd01.

The following example enables interface 1/1/4 to insert the CID information in the DHCP packets.

```
device(config-if-e1000-1/1/4)# dhcp snooping relay information circuit-id circuit01
```

The following example enables interface 1/1/4 to insert the RID information in the DHCP packets.

```
device(config-if-e1000-1/1/4)# dhcp snooping relay information remote-id remote01
```

Displaying DHCP option 82 information

You can use various show commands to view information about DHCP option 82 processing.

Use one of the following commands to view DHCP Option 82 processing. The commands do not need to be entered in the specified order.

1. Enter the **show ip dhcp relay information** command to display information about the Circuit ID, Remote ID, and forwarding policy for DHCP Option 82.

```
device# show ip dhcp relay information
Relay Information: Format: Circuit-ID : vlan-mod-port
                           Remote-ID : mac
                              Policy : keep
```

2. Enter the **show ip dhcp snooping vlan** command to display information about the trusted ports, untrusted ports, and ports on which DHCP Option 82 is disabled.

```
device# show ip dhcp snooping vlan 1
IP DHCP snooping VLAN 1: Enabled
  Trusted Ports :   ethe 3
  Untrusted Ports : ethe 1 to 2 ethe 4 to 24
  Relay Info. disabled Ports: ethe 10
```

3. Enter the **show interfaces ethernet** command.

```
device# show interfaces ethernet 1/1/1
GigabitEthernet1/1/1 is up, line protocol is up
Port up for 40 minutes 10 seconds
  Hardware is GigabitEthernet, address is 0000.0000.0002 (bia 0000.0000.0002)
  Configured speed auto, actual 1Gbit, configured duplex fdx, actual fdx
  Configured mdi mode AUTO, actual MDI
  Member of L2 VLAN ID 1, port is untagged, port state is FORWARDING
  BPDU guard is Disabled, ROOT protect is Disabled
  Link Error Dampening is Disabled
  STP configured to ON, priority is level0
  Flow Control is config enabled, oper enabled, negotiation disabled
  mirror disabled, monitor disabled
  Not member of any active trunks
  Not member of any configured trunks
  No port name
  IPG MII 96 bits-time, IPG GMII 96 bits-time
  IP MTU 1500 bytes
  300 second input rate: 0 bits/sec, 0 packets/sec, 0.00% utilization
  300 second output rate: 264 bits/sec, 0 packets/sec, 0.00% utilization
  0 packets input, 0 bytes, 0 no buffer
  Received 0 broadcasts, 0 multicasts, 0 unicasts
  0 input errors, 0 CRC, 0 frame, 0 ignored
  0 runts, 0 giants
  0 packets output, 0 bytes, 0 underruns
  Transmitted 0 broadcasts, 0 multicasts, 0 unicasts
  0 output errors, 0 collisions
     Relay Agent Information option: Enabled, Subscriber-ID: Ruckus001
```

The output shows the DHCP option 82 enabled on the device and the configured Subscriber ID to be Ruckus001.

NOTE
The port up or down time is required only for physical ports and not for loopback, ve, or tunnel ports.

Configuring the source IP address of a DHCP client packet on the DHCP relay agent

Enables the DHCP server to know the source subnet or network of a DHCP-client packet.

By default, a DHCP relay agent forwards a DHCP client packet with the source IP address set to the IP address of the outgoing interface to the DHCP server. You can configure ACLs on a DHCP server to provide or block DHCP services to particular subnets or networks. The **ip bootp-use-intf-ip** command configures a DHCP relay agent to set the source IP address of a DHCP client packet with the IP address of the incoming interface for the packet. This reveals the source subnet or network of a DHCP client packet to the DHCP server and enables the DHCP server to process or discard the DHCP traffic according to the configured ACLs.

Enter the **ip bootp-use-intf-ip** command in global configuration mode of the DHCP relay agent.

```
device(config)# ip bootp-use-intf-ip
```

IP Source Guard

You can use IP Source Guard together with Dynamic ARP Inspection on untrusted ports.

The Ruckus implementation of the IP Source Guard technology supports configuration on a port, specific VLAN memberships on a port (Layer 2 devices only), and specific ports on a Virtual Ethernet (VE) interface (Layer 3 devices only).

When IP Source Guard is first enabled, only DHCP packets are allowed, while all other IP traffic is blocked. IP Source Guard allows IP traffic when the system learns valid IP addresses. The system learns of a valid IP address from DHCP snooping.

When a new IP source entry binding on the port is created or deleted, the ACL is recalculated and reapplied in the hardware to reflect the change in IP source bindings. By default, if IP Source Guard is enabled without any IP source binding on the port, an ACL that denies all IP traffic is loaded on the port.

Configuration notes and feature limitations for IP Source Guard

The following configuration notes and feature limitations apply to IP Source Guard (IPSG):

- IPSG is supported on LAGs.
- If you change the default VLAN ID when IPSG is enabled on a LAG, the IPSG is not inherited. All IPSG configuration is lost for the VLAN if the default VLAN ID is changed.
- If removing a VLAN from a switch, you must first remove IPSG from the VLAN. This ensures that IPSG configurations do not remain for the VLAN.
- Before removing a physical port from a LAG, IPSG should first be disabled for the VLAN.
- IP Source Guard functions across reload.
- Ruckus ICX devices do not support IP Source Guard and dynamic ACLs on the same port.
- Ruckus devices support IP Source Guard with IPv4 ACLs (similar to ACLs for dot1x), as long as both features are configured at the port level or per-port-per-VLAN level. Ruckus devices do not support IP Source Guard and IPv4 ACLs on the same port if one is configured at the port level and the other is configured at the per-port-per-VLAN level.
- When IPSG is enabled on a LAG, IPSG entries learned on the LAG port will be flushed out upon removing the port from the LAG. When IPSG is enabled for the LAG under VLAN, IPSG entries learned on the LAG ports remain intact upon removing the port from the LAG.
- IP Source Guard and IPv6 ACLs are supported together on the same device, as long as they are not configured on the same port or virtual interface.
- IP Source Guard can be enabled on tagged ports or untagged ports in a VLAN or VE.
- Beginning 08.0.40a, IP Source Guard can be enabled with Flexible Authentication using the **authentication source-guard-protection enable** command. Refer to the *Ruckus FastIron Security Configuration Guide* for more information.
- A port on which IP Source Guard is enabled limits the support of clients, VLANs, and ACL rules per port. An IP Source Guard port supports a maximum of:
  - 520 clients per port
  - 64 VLANs
  - 520 rules per ACL

    NOTE
    When IPv4 ACLs and IP source guard are configured on the same port, both the rules will be clubbed together and the combined number of filters in that ACL must not exceed 1024.

- On certain Ruckus devices, such as ICX 7150 that have smaller TCAM, the IP source guard entries are limited to 256 entries. The scaling number of 256 per port in ICX 7150 and 520 per port in all other platforms is not guaranteed and depends on the number of free TCAM rules. Since IP source guard is programmed in the TCAM and if there are fewer TCAM rules, then the number of free TCAM rules will determine the number of IP source guard entries that are allowed.
- When IPSG and DHCP snooping are enabled on SPX Virtual (PE) ports and DHCP clients are learnt on the port, system performance may be degraded if more than 256 clients are learnt on the same port.
- You can enable IP Source Guard on a range of ports within a given slot only. Enabling IP Source Guard across multiple slots is not supported.

- The number of configured ACL rules affect the rate at which hardware resources are used when IP Source Guard is enabled. Use the **show access-list hw-usage on** command to enable hardware usage for an ACL, followed by the **show access-list** *access-list-id* command to determine the hardware usage for an ACL. Modifying the ACL rules ensures that more hardware resources are provided for IP Source Guard addresses. For example.

```
device# show access-list hw-usage on
   device# show access-list 100
   Extended IP access list 100 (hw usage : 2)
   deny ip any any (hw usage : 1)
```

- If you enable IP Source Guard in a network topology that has DHCP clients, you must also enable DHCP snooping. If you do not enable DHCP snooping, all IP traffic, including DHCP packets, are blocked.
- When you enable IP Source Guard in a network topology that does not have DHCP clients, you must create an IP source binding for each client that is allowed access to the network. Data packets are blocked if you do not create an IP source binding for each client.
- IP Source Guard protection enables concurrent support with MAC authentication.
- IP Source Guard is supported on a VE with or without an assigned IP address.
- IP Source Guard supports multi-VRF instances.

Enabling IP Source Guard on a port or range of ports

IP Source Guard is disabled by default. You can enable IP Source Guard on DHCP snooping untrusted ports.

To run IP Source Guard, you must first enable support for ACL filtering based on VLAN membership or VE port membership. Enter the following commands at the global configuration level.

```
device(config# enable ACL-per-port-per-vlan
device(config)# write memory
device(config)# exit
device# reload
```

NOTE
You must save the configuration and reload the software for the changes to take effect.

1. Enter global configuration mode by issuing the **configure terminal** command.

```
device# configure terminal
```

2. Enter interface configuration mode.

```
device(config)# interface ethernet 1/1/1
```

3. Enable IP Source Guard on the port.

```
device(config-if-e10000-1/1/1)# source-guard enable
```

4. To enable IP Source Guard on a range of ports, enter interface configuration mode and specify the range of ports.

```
device(config-if-e10000-1/1/1)# interface ethernet 1/1/21 to 1/1/25
```

When enabling IP Source Guard on a range of ports, you can choose only a range of ports within a given slot.

5. Enable IP Source Guard on the range of ports specified in the previous step.

```
device(config-mif-1/1/21-1/1/25)# source-guard enable
```

NOTE
If you try to configure IP Source Guard across different modules, the following error displays.

```
device(config)# interface ethernet 2/1/10 to 12/1/10
Error - cannot configure multi-ports on different slot
```

Defining static IP source bindings

You can manually enter valid IP addresses in the binding database.

Note that because static IP source bindings consume system resources, you should avoid unnecessary bindings.

1. Enter global configuration mode by issuing the **configure terminal** command.

```
device# configure terminal
```

2. Enter the **ip source binding** command followed by a valid IP address and the interface number. Entering the VLAN number is optional.

```
device(config)# ip source binding 10.10.10.1 ethernet 1/2/4 vlan 4
```

If you enter a VLAN number, the binding applies to that VLAN only. If you do not enter a VLAN number, the static binding applies to all VLANs associated with the port.

Enabling IP Source Guard per-port-per-VLAN

IP Source Guard can be enabled on a per-port-per-VLAN basis.

1. Enter the global configuration mode by issuing the **configure terminal** command.

```
device# configure terminal
```

2. Configure the port-based VLAN.

```
device(config)# vlan 12
```

3. Add ports Ethernet 5 through 8 as untagged ports.

```
device(config-vlan-12)# untag ethernet 5 to 8
```

4. Add ports Ethernet 23 through Ethernet 24 as tagged ports and exit the mode.

```
device(config-vlan-12)# tag ethernet 23 to 24
device(config-vlan-12)# exit
```

5. Enter interface configuration mode for port 23.

```
device(config)# interface ethernet 23
```

6. Enable IP Source Guard on port Ethernet 23, a member of VLAN 12.

```
device(config-if-e1000-23)# per-vlan vlan12
device(config-if-e1000-23-vlan-12)# source-guard enable
```

The following example configures IP Source Guard on a per-port-per-vlan.

```
device# configure terminal
device(config)# vlan 12
device(config-vlan-12)# untag ethernet 5 to 8
device(config-vlan-12)# tag ethernet 23 to 24
device(config-vlan-12)# exit
device(config)# interface ethernet 23
device(config-if-e1000-23)# per-vlan vlan12
device(config-if-e1000-23-vlan-12)# source-guard enable
```

Enabling IP source guard on a VLAN

You can enable IP source guard on a switch or a router for a range of ports in a VLAN or on the entire VLAN.

1. Enter the global configuration mode by issuing the **configure terminal** command.

```
device# configure terminal
```

2. Configure the port-based VLAN.

```
device(config)# vlan 12
```

3. Add ports Ethernet 1/1/5 through 1/1/8 as untagged ports.

```
device(config-vlan-12)# untagged ethernet 1/1/5 to 8
```

4. Add ports Ethernet 1/1/23 through Ethernet 1/1/24 as tagged ports.

```
device(config-vlan-12)# tagged ethernet 1/1/23 to 1/1/24
```

5. Enable source guard on the tagged ports.

```
device(config-vlan-12)# source-guard enable ethernet 1/1/23 to 1/1/24
```

The following example configures IP Source Guard on a VLAN.

```
device# configure terminal
device(config)# vlan 12
device(config-vlan-12)# untagged ethernet 1/1/5 to 1/1/8
device(config-vlan-12)# tagged ethernet 1/1/23 to 1/1/24
device(config-vlan-12)# source-guard enable ethernet 1/1/23 to 1/1/24
```

The following example configures IP Source Guard on a single port on a VLAN.

```
device# configure terminal
device(config)# vlan 12
device(config-vlan-12)# untagged ethernet 1/1/5 to 1/1/8
device(config-vlan-12)# tagged ethernet 1/1/23 to 1/1/24
device(config-vlan-12)# source-guard enable ethernet 1/1/23
```

The following example configures IP Source Guard on all ports on a VLAN.

```
device# configure terminal
device(config)# vlan 12
device(config-vlan-12)# untagged ethernet 1/1/5 to 1/1/8
device(config-vlan-12)# tagged ethernet 1/1/23 to 1/1/24
device(config-vlan-12)# source-guard enable
```

Enabling IP Source Guard on a VE

IP Source Guard can be enabled on a virtual interface.

1. Enter global configuration mode by issuing the **configure terminal** command.

```
device# configure terminal
```

2. Configure the port-based VLAN.

```
device(config)# vlan 2
```

3. Add port Ethernet 1 to VLAN 2.

```
device(config-vlan-2)# tagged ethe 2/1/36 ethe 12/1/38 to 12/1/39 ethe 17/2/2 ethe 55/1/32
```

4. Create a VE on the VLAN.

```
device(config-vlan-2)# router-interface ve 2
```

5. Enter the Virtual Interface mode.

```
device(config-vlan-2)# interface ve 2
```

6. Enable IP Source Guard on Ethernet 2/1/36.

```
device(config-vif-2)# source-guard enable ethe 2/1/36
```

The following example configures IP Source Guard on a virtual interface.

```
device# configure terminal
device(config)# vlan 2
device(config-vlan-2)# tagged ethe 2/1/36 ethe 12/1/38 to 12/1/39 ethe 17/2/2 ethe 55/1/32
device(config-vlan-2)# router-interface ve 2
device(config-vlan-2)# interface ve 2
device(config-vif-2)# source-guard enable ethernet 2/1/36
```

The following example configures IP Source Guard on untagged ports in a virtual interface.

```
device# configure terminal
device(config)# vlan 2
device(config-vlan-2)# untagged ethe 1/2/3 ethe 2/1/11 ethe 3/1/5 to 3/1/6 ethe 20/1/5 to 20/1/6 ethe 20/2/3
device(config-vlan-2)# router-interface ve 2
device(config-vlan-2)# interface ve 2
device(config-vif-2)# source-guard enable e 20/2/3
```

Enabling IP Source Guard on a Multi-VRF instance

You can use IP Source Guard together with Dynamic ARP Inspection on untrusted ports.

To configure IP Source Guard to support a VRF instance, you must first enable the ACL-per-port-per-VLAN setting.

```
device(config)# enable acl-per-port-per-vlan
Reload required. Please write memory and then reload or power cycle.
```

The Ruckus implementation of IP Source Guard supports configuration on a port, on specific VLAN memberships on a port (Layer 2 devices only), and on specific ports on a virtual interface (VE) (Layer 3 devices only).

1. Enter global configuration mode by issuing the **configure terminal** command.

```
device# configure terminal
```

2. Enter interface configuration mode.

```
device(config)# interface ethernet 1/1/1
```

3. Configure IP Source Guard on a port.

```
device(config-if-e1000-1/1/1)# source-guard enable
```

4. For Layer 2 devices, enable IP Source Guard per-port per-VLAN.

```
device(config-if-e1000-1/1/1)# per-vlan 2
device(config-if-e1000-1/1/1-vlan-2)# source-guard enable
```

5. For Layer 3 devices, enable IP Source Guard on a virtual interface.

```
device(config)# interface ve 30
device(config-vif-30)# source-guard enable ethernet 1/1/1
```

6. Manually enter valid IP addresses in the binding database.

```
device(config)# ip source binding 1.1.1.2 ethernet 1/1/1 vlan 2
```

   If the VLAN ID is not provided, this setting will be applied on the port.

Displaying learned IP addresses

To display the learned IP addresses for IP Source Guard ports, use the **show ip source-guard ethernet** command.

```
device# show ip source-guard e 1/1/48
Total IP Source Guard entries on port 1/1/48: 33
No    Interface           Type  Flter-mode       IP-address     Vlan   Static
--    ---------           ----  ----------       ----------     ----   -------
1     1/1/9*4/1/39          ip     active        15.15.15.127      1    Yes
2     1/1/9*4/1/39          ip     active          15.15.15.9      1     No
3     1/1/9*4/1/39          ip     active         15.15.15.10      1     No
4     1/1/9*4/1/39          ip     active         15.15.15.11      1     No
5     1/1/9*4/1/39          ip     active         15.15.15.12      1     No
6     1/1/9*4/1/39          ip     active         15.15.15.13      1     No
7     1/1/9*4/1/39          ip     active         15.15.15.14      1     No
8     1/1/9*4/1/39          ip     active         15.15.15.15      1     No
9     1/1/9*4/1/39          ip     active         15.15.15.16      1     No
10    1/1/9*4/1/39          ip     active         15.15.15.17      1     No
```

NOTE

All static source guard entries in the IP source guard table will be populated as "Yes".

DHCPv6

- DHCPv6 overview..... 87
- DHCP relay agent for IPv6..... 87
- Configuring a DHCPv6 relay agent..... 87
- DHCPv6 relay agent include options..... 88
- Specifying the IPv6 DHCP relay include options..... 89
- DHCPv6 Relay Agent Prefix Delegation Notification..... 89
- DHCPv6 snooping..... 94

DHCPv6 overview

The Dynamic Host Configuration Protocol for IPv6 (DHCP) enables DHCP servers to pass configuration parameters such as IPv6 network addresses to IPv6 nodes.

The DHCPv6 protocol offers the capability of automatic allocation of reusable network addresses and additional configuration flexibility.

On FastIron devices, you can configure DHCPv6 snooping, the DHCPv6 relay agent, DHCPv6 relay include options, and the DHCPv6 Relay Agent Prefix Delegation Notification.

DHCP relay agent for IPv6

A client locates a DHCPv6 server using a reserved, link-scoped multicast address. Direct communication between the client and server requires that they are attached by the same link. In some situations where ease-of-management, economy, and scalability are concerns, you can allow a DHCPv6 client to send a message to a DHCPv6 server using a DHCPv6 relay agent.

A DHCPv6 relay agent, which may reside on the client link, but is transparent to the client, relays messages between the client and the server. Multiple DHCPv6 relay agents can exist between the client and server. DHCPv6 relay agents can also receive relay-forward messages from other relay agents; these messages are forwarded to the DHCPv6 server specified as the destination.

When the relay agent receives a message, it creates a new relay-forward message, inserts the original DHCPv6 message, and sends the relay-forward message as the DHCPv6 server.

Configuring a DHCPv6 relay agent

You can enable the DHCPv6 relay agent function and specify the relay destination (the DHCP server) address on an interface.

1. Enter global configuration mode by issuing the **configure terminal** command.

```
device# configure terminal
```

2. Enter interface configuration mode.

```
device(config)# interface ethernet 1/2/3
```

3. Specify the relay destination (the DHCP server) address on the interface.

```
device(config-if-e10000-1/2/3)# ipv6 dhcp-relay destination 2001::2
```

   The IPv6 address is the destination address to which client messages are forwarded and which enables DHCPv6 relay service on the interface. You can configure up to 16 relay destination addresses on an interface.

4. Specify the outgoing interface parameter.

```
device(config-if-e10000-1/2/3)# ipv6 dhcp-relay destination fe80::224:38ff:febb:e3c0  outgoing-
interface ethernet 1/2/5
```

   Use the **outgoing-interface** parameter when the destination relay address is a link-local or multicast address. Specify the interface type as **ethernet**, **tunnel interface**, or **VE**. Specify the port-num as the port number.

The following example enables the DHCPv6 relay agent function and specifies the relay destination address (i.e. the DHCP server) on an interface.

```
device(config)# interface ethernet 1/2/3
device(config-if-e10000-1/2/3)# ipv6 dhcp-relay destination 2001::2
device(config-if-e10000-1/2/3)# ipv6 dhcp-relay destination fe80::224:38ff:febb:e3c0  outgoing-interface
ethernet 1/2/5
```

DHCPv6 relay agent include options

You can configure the DHCPv6 relay agent to include the client's remote ID, interface ID, or client link layer address as identifiers in the relay forward DHCPv6 messages.

In some network environments, it is useful for the relay agent to add information to the DHCPv6 message before relaying it. The information that the relay agent carries can also be used by the DHCP server to make decisions about the addresses, delegated prefixes, and configuration parameters that the client should receive. The DHCPv6 relay-forward message contains relay agent parameters that identify the client-facing interface on which the reply messages can be forwarded. You can use either one or all of the parameters as client identifiers.

The following options can be included in the relay-forward messages:

- Interface-ID option (18)
- Remote-ID option (37)
- Client link layer (MAC) address option (79)

The relay agent may send the interface-ID option (18) to identify the interface on which a client message was received. If the relay agent cannot use the address in the link-address field to identify the interface through which the response to the client will be relayed, the relay agent must include an interface-ID option in the relay-forward message. If the relay agent receives a relay-reply message with an interface-ID option, the relay agent relays the message to the client through the interface identified by the option. The server must also copy the interface-ID option from the relay-forward message into the relay-reply message the server sends to the relay agent in response to the relay-forward message.

The remote-ID option (37) may be added by the DHCP relay agent that terminates switched or permanent circuits and uses a mechanism to identify the remote host end of the circuit. The remote ID must be unique. A DHCPv6 relay agent can be configured to include a remote-ID option in the relay-forward DHCPv6 messages.

The client link layer (MAC) address option (79) can be used along with other identifiers to associate DHCPv4 and DHCPv6 messages from a dual-stack client, and is useful in environments where operators using an existing DHCPv4 system with the client link layer address as the customer identifier need to correlate DHCPv6 assignments using the same identifier.

NOTE
If you enable the client link layer (MAC) option and save the configuration, and then downgrade to a version of the software that does not support this feature, an error message displays. You must remove any configuration related to this option before the downgrade and add the configuration after the upgrade to prevent this error.

Specifying the IPv6 DHCP relay include options

You can specify either one or all of the IPv6 DHCP relay include options in the relay-forward message.

The options include the interface-ID, remote-ID, or link layer option. Perform the following steps to include the DHCPv6 relay options.

1. Enter global configuration mode by issuing the **configure terminal** command.

```
device# configure terminal
```

2. Enter interface configuration mode.

```
device(config)# interface ethernet 1/1/1
```

3. Enter the **ipv6 dhcp-relay include-options** command followed by the required options: **interface-ID**, **remote-ID** or **link-layer-option**.

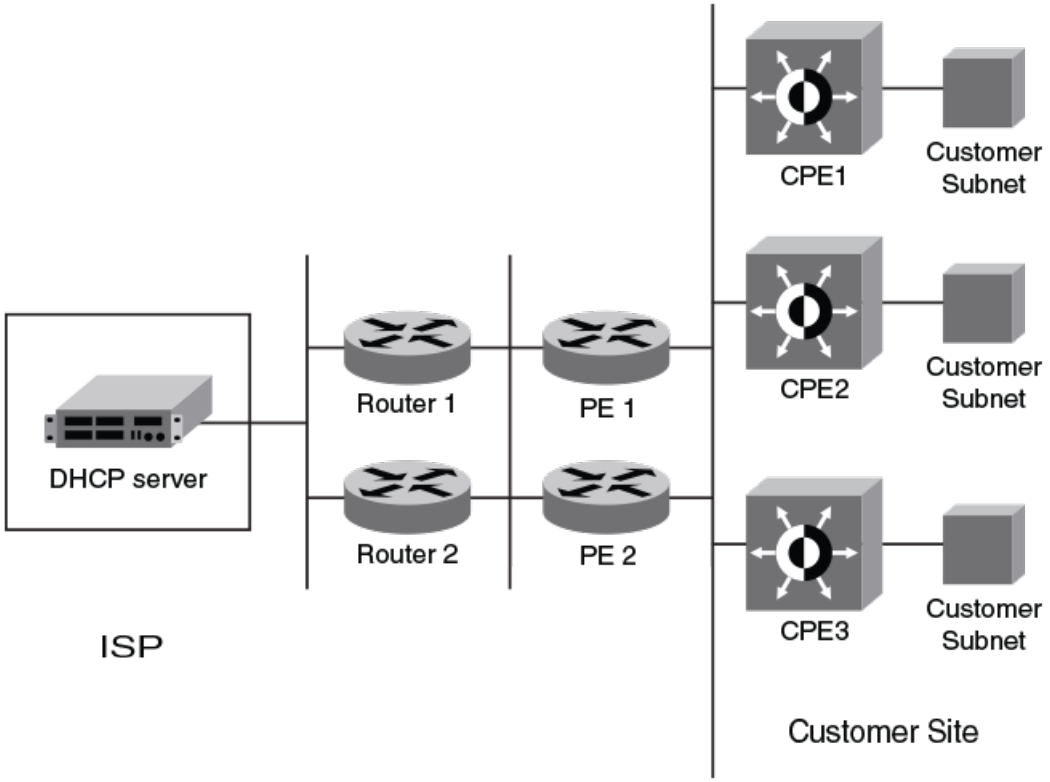
   The following example shows specifying the link layer option.

```
device(config-if-e1000-1/1/1)# ipv6 dhcp-relay include-options link-layer-option
```

DHCPv6 Relay Agent Prefix Delegation Notification

DHCPv6 Relay Agent Prefix Delegation Notification allows a DHCPv6 server to dynamically delegate IPv6 prefixes to a DHCPv6 client using the DHCPv6 Prefix Delegation (PD) option. DHCPv6 prefix delegation enables an Internet Service Provider (ISP) to automate the process of assigning prefixes to a customer premises equipment (CPE) network. The CPE then assigns IPv6 subnets from the delegated IPv6 prefix to its downstream customer interfaces.

FIGURE 18 DHCPv6 Relay Agent Prefix Delegation Notification



A route is added to the IPv6 route table on the provider edge router (PE) for the delegated prefix to be delegated to requesting routers. The DHCP server chooses a prefix for delegation and responds with it to the CPEx. to the external network, and to enable the correct forwarding of the IPv6 packets for the delegated IPv6 prefix. Adding the delegated prefix to the IPv6 route table ensures that the unicast Reverse Path Forwarding (uRPF) works correctly.

Because the PE is also a DHCPv6 relay agent (it relays DHCPv6 messages between the CPE and the DHCP server), it examines all DHCPv6 messages relayed between the CPE and the DHCP server and gathers information about a delegated prefix and then manages the advertisement of this delegated prefix to the external network.

DHCPv6 Relay Agent Prefix Delegation Notification limitations

The following limitations apply to DHCPv6 Relay Agent Prefix Delegation Notification.

- The PD notification fails when the DHCPv6 messages between a DHCPv6 server and a DHCPv6 client containing the PD option are not relayed by way of the DHCPv6 relay agent.
- If the delegated prefix is released or renewed by the client at the time when the DHCPv6 relay agent is down or rebooting, then this release or renewal of the delegated prefix will not be detected by the relay agent. In such a condition, there could be stale static routes in the routing table. You must clear the stale routes.
- If there is no sufficient disk space on a flash disk, then the system may not store all the delegated prefixes in the IPv6 route table.
- The DHCPv6 PD flash operation depends on the NTP clock synchronization. During system bootup, if the NTP is configured, the flash operation (dhcp6_delegated_prefixes_data flash file read/write) is delayed until the NTP is

synchronized. The NTP synchronization is needed for the correct updating of the prefix age. If the NTP is not configured, then the DHCP prefix delegation will still read the flash, but the prefix age may not be correct.

Upgrade and downgrade considerations

- When a router is upgraded to the version of software that supports this feature DHCPv6 Relay Agent Prefix Delegation Notification, the saved information about delegated prefixes will be examined and if the delegated prefix lifetime is not expired, then the prefix will be added to the IPv6 static route table.
- When a router is downgraded to the version of software that does not support DHCPv6 Relay Agent Prefix Delegation Notification, the saved information about delegated prefixes is retained and it cannot be used.

Configuring DHCPv6 Relay Agent Prefix Delegation Notification

You can set the number of delegated prefixes that can be learned at the global level. By default, DHCPv6 Relay Agent Prefix Delegation Notification is enabled when the DHCPv6 relay agent is enabled on an interface.

You can disable the DHCPv6 Relay Agent Prefix Delegation Notification at the system or the interface level by setting the IPv6 DHCP relay maximum delegated prefixes to 0 at the system or interface level as required.

Make sure that there is enough free space in the flash memory to save information about delegated prefixes in flash on both the Active and Standby management processor.

1. Enter global configuration mode by issuing the **configure terminal** command.

   ```
   device# configure terminal
   ```

2. Set the maximum number of prefixes that can be learned at the global level.

   ```
   device(config)# ipv6 dhcp-relay maximum-delegated-prefixes 500
   ```

   You can limit the maximum number of prefixes that can be learned at the global level. The range is from 0 through 512. The default value is 500. The DHCPv6 prefix delegation default for the ICX 7750 is 50.

The following example sets the maximum number of prefixes that can be learned at the global level to 500.

```
device# configure terminal
device(config)# ipv6 dhcp-relay maximum-delegated-prefixes 500
```

Enabling DHCPv6 Relay Agent Prefix Delegation Notification on an interface

The number of delegated prefixes that can be learned can be limited at the interface level.

1. Enter global configuration mode by issuing the **configure terminal** command.

   ```
   device# configure terminal
   ```

2. Enter interface configuration mode.

   ```
   device(config)# interface ethernet 1/1/1
   ```

3. Set the number of delegated prefixes that can be learned.

```
device(config-if-eth 1/1/1)# ipv6 dhcp-relay maximum-delegated-prefixes 100
```

   You can limit the maximum number of prefixes that can be delegated. The range is from 0 through 512. The default value is 100. The sum of all the delegated prefixes that can be learned at the interface level is limited by the system max.

The following example sets the number of delegated prefixes that can be learned to 100.

```
device# configure terminal
device(config)# interface ethernet 1/1/1
device(config-if-eth 1/1/1)# ipv6 dhcp-relay maximum-delegated-prefixes 100
```

Assigning the administrative distance to DHCPv6 static routes

You can assign the administrative distance to DHCPv6 static routes installed in the IPv6 route table for the delegated prefixes on the interface. This value must be set so that it does not replace the same IPv6 static route configured by the user.

1. Enter global configuration mode by issuing the **configure terminal** command.

```
device# configure terminal
```

2. Enter interface configuration mode.

```
device(config)# interface ethernet 1/1/1
```

3. Set the administrative distance value.

```
device(config-if-eth-1/1/1)# ipv6 dhcp-relay distance 25
```

   The value parameter is used to assign the administrative distance to DHCPv6 static routes on the interface. The range is from 1 to 255. The default value is 10. If the value is set to 255, then the delegated prefixes for this interface will not be installed in the IPv6 static route table.

The following example sets the administrative distance to the DHCPv6 static routes on the interface to 25.

```
device# configure terminal
device(config)# interface ethernet 1/1/1
device(config-if-eth-1/1/1)# ipv6 dhcp-relay distance 25
```

Displaying DHCPv6 relay agent and prefix delegation information

You can use various show commands to view information about DHCPv6 relay agent and prefix delegation information.

Use one of the following commands to view DHCPv6 relay agent and prefix delegation information. The commands do not need to be entered in the specified order.

1. Enter the **show ipv6 dhcp-relay options** command.

```
device# show ipv6 dhcp-relay options
DHCPv6 Relay Options Information:
Interface       Interface-Id     Remote-Id     Option-79
e 1/1/1            No                No             No
```

   The output of this command displays information about the relay options available to the prefixed delegates for a specific interface.

2. Enter the **show ipv6 dhcp-relay** command.

```
device(config)# show ipv6 dhcp-relay
Current DHCPv6 relay agent state: Enabled
DHCPv6 enabled interface(s): e 1/2/3
DHCPv6 Relay Agent Statistics:
 Total DHCPv6 Packets, Received:0, Transmitted:0
 Received DHCPv6 Packets: RELEASE:0,RELAY_FORWARD:0,RELAY_REPLY:0
                          OtherServertoClient:0,OtherClinettoServer:0
```

   The output of this command displays the DHCPv6 relay agent information configured on the device.

3. Enter the **show ipv6 dhcp-relay interface** command.

```
device(config)# show ipv6 dhcp-relay interface ethernet 1/1/1
DHCPv6 Relay Information for interface e 1/1/1:
Destinations:
 Destination                   OutgoingInterface
 2001::2                       NA
Options:
 Interface-Id: No       Remote-Id:No           Option-79:No
Prefix Delegation Information:
 Current:0 Maximum:100 AdminDistance:10
```

   The output of this command displays DHCPv6 relay information for a specific interface.

4. Enter the **show ipv6 dhcp-relay destinations** command.

```
device# show ipv6 dhcp-relay destinations
DHCPv6 Relay Destinations:
Interface e 1/2/3:
   Destination                   OutgoingInterface
   2001::2                       NA
   fe80::224:38ff:febb:e3c0      e 1/2/5
```

   The output of this command displays information about the delegated prefixes' configured destinations for a specific interface.

5. Enter the **show ipv6 dhcp-relay prefix-delegation-information** command.

```
device# show ipv6 dhcp-relay prefix-delegation-information
DHCPv6 Relay Prefix Delegation Notification Information:
  Interface  Current    Maximum    AdminDistance
  ve 100     20         20000      10
  ve 101     4000       20000      10
  ve 102     0          20000      10
  ve 103     0          20000      10
  ve 104     0          20000      10
  ve 105     0          20000      10
```

   The output of this command displays additional information about the DHCPv6 prefix delegation.

6. Enter the **show ipv6 dhcp-relay delegated-prefixes** command.

```
device# show ipv6 dhcp-relay delegated-prefixes interface ethernet 1/1/45

Prefix                        Client                Interface    ExpireTime
fc00:2000:6:7:1::/96          fe80::210:94ff:fe00:e   1/1/45     29d23h53m0s
```

   The output of this command displays information about the delegated prefixes.

Clearing the DHCPv6 delegated prefixes and packet counters

Use the clear commands to clear the DHCPv6 delegated prefixes and packet counters.

1. Clear the DHCPv6 delegated prefixes using the clear command at the privileged EXEC level.

   ```
   device# clear ipv6 dhcp-relay delegated-prefixes vrf VRF1
   ```

   This command clears the DHCPv6 delegated prefixes for VRF1. If you do not provide the VRF name, the information for the default VRF is cleared. You can also use the **all** or **interface** keywords. Optionally, you can also clear a specific DHCPv6 delegated prefix.

2. Clear all the DHCPv6 packet counters using the clear command at the privileged EXEC level.

   ```
   device# clear ipv6 dhcp-relay statistics
   ```

DHCPv6 snooping

In an IPv6 domain, a node can obtain an IPv6 address using the following mechanisms:

- IPv6 address auto-configuration using router advertisements
- The DHCPv6 protocol

In a typical man-in-the-middle (MiM) attack, the attacker can snoop or spoof the traffic act as a rogue DHCPv6 server. To prevent such attacks, DHCPv6 snooping helps to secure the IPv6 address configuration in the network.

DHCPv6 snooping enables the Ruckus device to filter untrusted DHCPv6 packets in a subnet on an IPv6 network. DHCPv6 snooping can ward off MiM attacks, such as a malicious user posing as a DHCPv6 server sending false DHCPv6 server reply packets with the intention of misdirecting other users. DHCPv6 snooping can also stop unauthorized DHCPv6 servers and prevent errors due to user misconfiguration of DHCPv6 servers.

How DHCPv6 snooping works

When enabled on a VLAN, DHCPv6 snooping stands between untrusted ports (those connected to host ports) and trusted ports (those connected to DHCPv6 servers). A VLAN with DHCPv6 snooping enabled forwards DHCPv6 request packets from clients and discards DHCPv6 server reply packets on untrusted ports, and it forwards DHCPv6 server reply packets on trusted ports to DHCPv6 clients, as shown in the following figures.

FIGURE 19 DHCPv6 snooping at work on an untrusted port

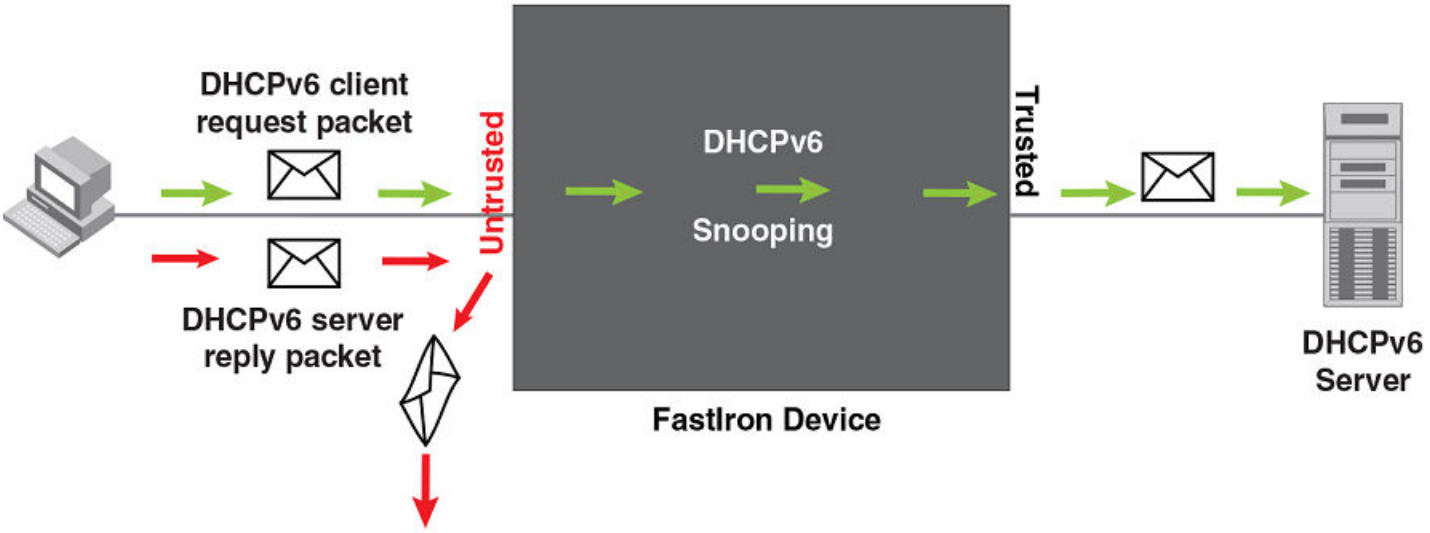
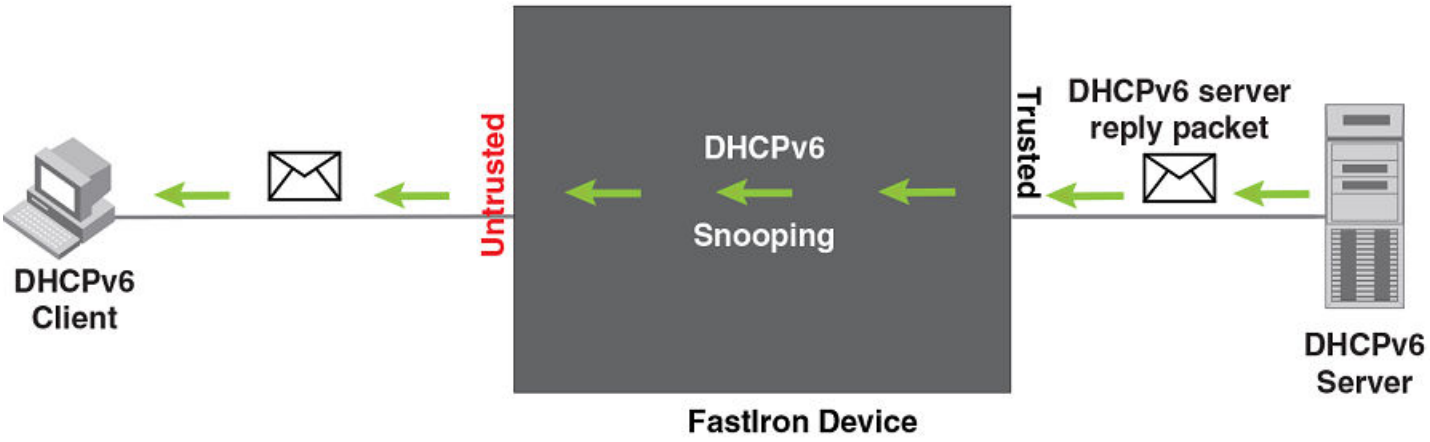


FIGURE 20 DHCPv6 snooping at work on a trusted port



DHCPv6 binding database

On trusted ports, DHCPv6 server reply packets are forwarded to DHCPv6 clients. The lease time will be refreshed when the client renews its IPv6 address with the DHCPv6 server; otherwise the Ruckus device removes the entry when the lease time expires.

Configuration notes and feature limitations for DHCPv6 snooping

The following configuration considerations apply to DHCPv6 snooping:

- DHCPv6 snooping must be enabled on both client and server VLANs.
- For default VLAN-ID changes, DHCPv6 snooping should be re-applied on the new default VLAN.
- The maximum number of DHCPv6 entries supported is 3072.

Configuring DHCPv6 snooping

DHCPv6 snooping must be enabled on VLANs, after which the trust setting of ports connected to a DHCP server must be changed to trusted. DHCP packets for a VLAN with DHCP snooping enabled are inspected.

To run DHCPv6 snooping, you must first enable support for ACL filtering based on VLAN membership or VE port membership. Enter the following commands at the global configuration level.

```
device(config)# enable ACL-per-port-per-vlan
device(config)# write memory
device(config)# exit
device# reload
```

NOTE
You must save the configuration and reload the software for the changes to take effect.

NOTE
DHCP snooping is disabled by default and the trust setting of ports is untrusted by default. DHCPv6 snooping must be enabled on the client and the DHCP server VLANs.

1. Enter global configuration mode by issuing the **configure terminal** command.

   ```
   device# configure terminal
   ```

2. Enable DHCPv6 snooping on a VLAN.

   ```
   device(config)# ipv6 dhcp6 snooping vlan 2
   ```

3. Change the trust setting of the ports that are connected to the DHCP server to trusted at the interface configuration level.

   ```
   device(config)# interface ethernet 1/1/1
   device(config-if-e10000-1/1/1)# dhcp6 snooping trust
   ```

   Port 1/1/1 is connected to a DHCPv6 server. The commands change the CLI to the interface configuration level of port 1/1/1 and set the trust setting of port 1/1/1 to trusted.

4. If required, disable the learning of DHCP clients on ports at the interface configuration level. Disabling the learning of DHCP clients can be configured on a range of ports as well.

   ```
   device(config-if-e10000-1/1/1)# dhcp6 snooping client-learning disable
   ```

5. Clear the DHCP binding database. You can remove all entries in the database or for a specific IP address only.

   ```
   device# clear ipv6 dhcp6 snooping

   device# clear ipv6 dhcp6 snooping 2001::2
   ```

   The first command removes all entries from the DHCP binding database and the second removes entries for a specific IP address.

The following example configures VLAN 10, and changes the CLI to the global configuration level to enable DHCPv6 snooping on the configured VLANs.

```
device(config)# vlan 10
device(config-vlan-10)# untagged ethernet 1/1/1 to 1/1/3
device(config-vlan-10)# exit
device(config)# ipv6 dhcp6 snooping vlan 10
```

On VLAN 10, client ports 1/1/2 and 1/1/3 are untrusted. By default, all client ports are untrusted. Only DHCPv6 client's SOLICIT and REQUEST packets received on ports 1/1/2 and 1/1/3 are forwarded.

The following example sets the DHCPv6 server port as trusted.

```
device(config)# interface ethernet 1/1/1
device(config-if-e10000-1/1/1)# dhcp6 snooping trust
device(config-if-e10000-1/1/1)# exit
```

Port 1/1/1 is connected to a DHCPv6 server. The DHCPv6 server ADVERTISE and REPLY packets received on port 1/1/1 are forwarded.

Configuring DHCPv6 snooping for Multi-VRF

DHCPv6 snooping supports Multi-VRF (Virtual Routing and Forwarding) instances. You can deploy multiple VRFs on a Ruckus Ethernet switch. Each VLAN with a Virtual Ethernet (VE) interface is assigned to a VRF.

You can enable DHCPv6 snooping on individual VLANs and assign any interface as the DHCPv6 trust interface. If an interface is a tagged port in this VLAN, you can turn on the trust port per VRF, so that traffic intended for other VRF VLANs is not trusted.

1. Enter global configuration mode by issuing the **configure terminal** command.

   ```
   device# configure terminal
   ```

2. To configure DHCP snooping to support a Multi-VRF instance, enable the ACL-per-port-per-VLAN setting.

   ```
   device(config)# enable acl-per-port-per-vlan
   Reload required. Please write memory and then reload or power cycle.
   ```

3. Configure DHCP snooping on a specific VLAN.

   ```
   device(config)# ipv6 dhcp6 snooping vlan 2
   ```

4. Set the port as a trusted port.

   ```
   device(config)# interface ethernet 1/1/4
   device(config-if-e10000-1/1/4)# dhcp6 snooping trust vrf red
   ```

   The trust port setting for DHCP snooping can be specified per VRF.

5. Configure the DHCPv6 relay agent on the VE interface if the client and server are not in the same VLAN.

   ```
   device(config-vif-23)# ipv6 dhcp-relay destination 2001:100::2
   ```

6. To clear a DHCPv6 binding database of a specific Multi-VRF enter the following command.

   ```
   device(config)# clear ipv6 dhcp6 snooping vrf vrf2
   ```

7. To clear a specific DHCPv6 binding belonging to a specific IPv6 address and VRF, enter the following command.

   ```
   device# clear ipv6 dhcp6 snooping 2001::2 vrf vrf2
   ```

8. To clear default VRF DHCPv6 snooping entries, enter the following command.

   ```
   device# clear ipv6 dhcp6 snooping vrf default
   ```

Displaying DHCPv6 snooping information

You can use various show commands to view information about DHCPv6 snooping.

Use one of the following commands to view DHCPv6 snooping information. The commands do not need to be entered in the specified order.

1. Enter the **show ipv6 dhcp6 snooping** command.

```
device# show ipv6 dhcp6 snooping
IP dhcpv6 snooping enabled on 1 VLANS(s):
VLAN:10
device# show ipv6 dhcp6 snooping vlan 10
IP dhcpv6 snooping VLAN 10: Enabled
Trusted Ports: ethe 1/1/1
Untrusted Ports: ethe 1/1/2 ethe 1/1/3
```

   The output of this command displays information about the DHCPv6 snooping status and ports

2. Enter the **show ipv6 dhcp6 snooping info** command.

```
device# show ipv6 dhcp6 snooping info
IPv6 Address LinkLayer-Addr  Age    Port        Virtual Port  vlan    VRF
 15::4        0000.0006.0003  259199  e 22/1/48    v15          15    default-vrf
 14::5        0000.0005.0004  259199  e 21/1/48    v14          14    default-vrf
 13::6        0000.0004.0005  259199  e 19/1/24    v13          13    default-vrf
 10::2        0000.0001.0001  259199  e 2/1/48     v10          10    default-vrf
 13::2        0000.0004.0001  259199  e 19/1/24    v13          13    default-vrf
 12::3        0000.0003.0002  259199  e 18/1/48    v12          12    default-vrf
 11::4        0000.0002.0003  259199  e 3/1/48     v11          11    default-vrf
 10::5        0000.0001.0004  259199  e 2/1/48     v10          10    default-vrf
 15::3        0000.0006.0002  259199  e 22/1/48    v15          15    default-vrf
 14::4        0000.0005.0003  259199  e 21/1/48    v14          14    default-vrf
 13::5        0000.0004.0004  259199  e 19/1/24    v13          13    default-vrf
 12::6        0000.0003.0005  259199  e 18/1/48    v12          12    default-vrf
 15::6        0000.0006.0005  259199  e 22/1/48    v15          15    default-vrf
 12::2        0000.0003.0001  259199  e 18/1/48    v12          12    default-vrf
 11::3        0000.0002.0002  259199  e 3/1/48     v11          11    default-vrf
 10::4        0000.0001.0003  259199  e 2/1/48     v10          10    default-vrf
 15::2        0000.0006.0001  259199  e 22/1/48    v15          15    default-vrf
 14::3        0000.0005.0002  259199  e 21/1/48    v14          14    default-vrf
 13::4        0000.0004.0003  259199  e 19/1/24    v13          13    default-vrf
 12::5        0000.0003.0004  259199  e 18/1/48    v12          12    default-vrf
 11::6        0000.0002.0005  259199  e 3/1/48     v11          11    default-vrf
 15::5        0000.0006.0004  259199  e 22/1/48    v15          15    default-vrf
 14::6        0000.0005.0005  259199  e 21/1/48    v14          14    default-vrf
 11::2        0000.0002.0001  259199  e 3/1/48     v11          11    default-vrf
 10::3        0000.0001.0002  259199  e 2/1/48     v10          10    default-vrf
 14::2        0000.0005.0001  259199  e 21/1/48    v14          14    default-vrf
 13::3        0000.0004.0002  259199  e 19/1/24    v13          13    default-vrf
 12::4        0000.0003.0003  259199  e 18/1/48    v12          12    default-vrf
 11::5        0000.0002.0004  259199  e 3/1/48     v11          11    default-vrf
 10::6        0000.0001.0005  259199  e 2/1/48     v10          10    default-
vrf

Total number of entries: 30
```

   The output of this command displays the DHCPv6 snooping binding database.



© 2019 ARRIS Enterprises LLC. All rights reserved.
Ruckus Wireless, Inc., a wholly owned subsidiary of ARRIS International plc.
350 West Java Dr., Sunnyvale, CA 94089 USA
www.ruckuswireless.com