CONFIGURATION GUIDE

RUCKUS FastIron DHCP Configuration Guide, 10.0.10

Supporting FastIron Software Release 10.0.10

Part Number: 53-1005770-01
Publication Date: 22 May 2023

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, COMMSCOPE 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. CommScope 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. CommScope 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 CommScope 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 COMMSCOPE, COMMSCOPE 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 COMMSCOPE 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

CommScope and the CommScope logo are registered trademarks of CommScope and/or its affiliates in the U.S. and other countries. For additional trademark information see https://www.commscope.com/trademarks. All product names, trademarks, and registered trademarks are the property of their respective owners.

Patent Marking Notice

For applicable patents, see www.cs-pat.com.

Contents

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

About This Document **11**
New in This Document 11
Supported Hardware 11

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

DHCP Clients **15**
DHCP Client 15
DHCP Client Behavior on a Layer 3 Device 16
DHCP Over Default Virtual Ethernet Port (Layer 3 Devices) 16
Default Virtual Ethernet Port Creation (Layer 3 Devices) 16
Possible Reasons for Failure of Virtual Ethernet Port Creation 16
Enabling the DHCP Client for a Specific VE Port 17
Enabling the DHCP Client on a VE Port Associated with the Default VLAN 17
DHCP Client in Continuous Discovery Mode (Layer 2 and Layer 3 Devices) 18
DHCP Client as a New Device 18
DHCP Client Behavior after Reboot 20
BootP and DHCP Relay Parameters 20
Configuring an IP helper address 20
Configuring the BOOTP and DHCP reply source address 21
Changing the IP address used for stamping BootP and DHCP requests 21
Changing the maximum number of hops to a BootP relay server 22
DHCP Auto-Provisioning 22
Auto-Provisioning Using the bootfile.bin Option 23
DHCP Auto-Provisioning Using the Manifest File Option 24
DHCP Auto-Provisioning Enhancements 25
Configuring DHCP Auto-Provisioning Enhancements 27
DHCP auto-provisioning options 28
BOOTP Support 28
Configuring BOOTP Support 28
Disabling or re-enabling the DHCP client 29
DHCP Auto-provisioning on Layer 3 devices 30
Scenario 1: DHCP Auto-provisioning on a Layer 3 Device 31
Scenario 2: DHCP Auto-provisioning with a TFTP Server in a Different Network 32
Scenario 3: DHCP Client Connected through a DHCP Snooping Device 32

Scenario 4: DHCP Client Option 12 33
Scenario 5: DHCP Auto-provisioning on a Layer 2 Device 33
Configuration Notes and Feature Limitations for DHCP Auto-Provisioning 34
High Availability Considerations 35
Upgrade Considerations 35
How DHCP Client-Based Auto-Provisioning and Flash Image Update Works 35
Validating the IP Address and Lease Negotiation 35
Flash Image Download and Update 36
Auto-Provisioning Download and Update 36
Disabling or re-enabling auto-provisioning 36
Dynamic DHCP options configuration processing 37
Discovery of SmartZone Based on DHCP Option 43 37
Configuration Notes and Feature Limitations 38
Verifying Dynamic DHCP Options for a Router 39

DHCP Servers 41
DHCP Servers 41
Configuration Considerations for DHCP Servers 42
Configuring the DHCP server and creating an address pool 43
Default DHCP Server Settings 46
DHCP Server Options 46
Recommendations and Limitations 51
Upgrade Considerations 52
Disabling or re-enabling the DHCP server on the management port 53
Setting the wait time for ARP ping response 53
DHCP relay agent information support (option 82) 54
Configuring the IP address of the DHCP server 54
Configuring the Boot Image 54
Deploying an Address Pool Configuration to the Server 55
Specifying the Default Router Available to the Client 55
Specifying DNS Servers Available to the Client 55
Configuring the Domain Name for the Client 56
Configuring the lease duration for the address pool 56
Configuring the Number of Leases for the Address Pool 56
Specifying addresses to exclude from the address pool 57
Configuring the NetBIOS server for DHCP clients 57
Configuring the Subnet and Mask of a DHCP Address Pool 58
Configuring the TFTP Server 58
Configuring X Window System Display Manager IP Addresses (Option 49) 58
Vendor-specific Information (Option 43 and Option 60) Configurations 59
Configuring Vendor Details and Vendor Specific Information (Option 43 and Option 60) 59
Enabling static IP to MAC address mapping 60
Enabling IP to Physical Port Mapping 61
Configuring Avaya IP telephony (options 176 and 242) 62
Configuring WPAD (option 252) 64
Displaying DHCP server information 65

DHCPv4 67
DHCPv4 overview 67
Dynamic ARP Inspection Overview 67
ARP Poisoning 67

How Dynamic ARP Inspection Works ... 68
Configuration Notes and Feature Limitations for DAI ... 69
Configuring Dynamic ARP Inspection ... 69
Configuring Dynamic ARP Inspection on Multiple VLANs ... 70
Disabling Syslog Messages for DAI ... 71
Displaying ARP Information ... 72
Configuring DAI to Support Multi-VRF ... 72
Enabling Trust on a Port for a Specific VRF ... 73
DHCP Snooping ... 73
How DHCP Snooping Works ... 73
System Reboot and the Binding Database ... 75
Configuration Notes and Feature Limitations for DHCP Snooping ... 75
Configuring DHCP Snooping ... 76
Configuring DHCP Snooping on Multiple VLANs ... 77
Displaying DHCPv4 Snooping Information ... 78
Configuring DHCPv4 Snooping for Multi-VRF ... 79
Enabling DHCP Snooping MAC Address Verification ... 79
DHCP Relay Agent Information and Option 82 Insertion ... 80
Configuration Notes for DHCP Option 82 ... 81
DHCP Option 82 Sub-options ... 82
DHCP Option 82 Configuration ... 83
IP Source Guard ... 88
Configuration Notes and Feature Limitations for IP Source Guard ... 89
Enabling IP Source Guard on a Port or Range of Ports ... 90
Defining Static IP Source Bindings ... 90
Enabling IP Source Guard for a VLAN ... 91
Enabling IP Source Guard for a LAG Port for a VLAN ... 91
Enabling IP Source Guard on Multiple VLANs ... 92
Binding IP Source Guard ACLs to Ports ... 93
Displaying Learned IP Addresses ... 94

DHCPv6 ... 95
DHCPv6 overview ... 95
DHCP relay agent for IPv6 ... 95
Configuring a DHCPv6 relay agent ... 95
DHCPv6 relay agent include options ... 96
Specifying the IPv6 DHCP relay include options ... 97
DHCPv6 Relay Agent Prefix Delegation Notification ... 97
DHCPv6 Relay Agent Prefix Delegation Notification limitations ... 98
Upgrade and downgrade considerations ... 98
Configuring DHCPv6 Relay Agent Prefix Delegation Notification ... 98
Enabling DHCPv6 Relay Agent Prefix Delegation Notification on an interface ... 99
Assigning the administrative distance to DHCPv6 static routes ... 99
Displaying DHCPv6 relay agent and prefix delegation information ... 100
Clearing the DHCPv6 delegated prefixes and packet counters ... 101
DHCPv6 Snooping ... 101
How DHCPv6 Snooping Works ... 101
Configuration Notes and Feature Limitations for DHCPv6 Snooping ... 102
Configuring DHCPv6 Snooping ... 104
Configuring DHCPv6 Snooping on Multiple VLANs ... 105
Configuring DHCPv6 Snooping for Multi-VRF ... 106

Displaying DHCPv6 Snooping Information 107
DHCPv6 Server 107
Configuration Considerations for DHCPv6 Servers 107
Configuring the Stateless DHCPv6 Server 108
Configuring the Stateful DHCPv6 Server 110
Displaying DHCPv6 Server Information 112
Verification in Linux Mode 113
Prefix Delegation 113
Prefix Delegation for ICX DHCPv6 Servers 113
IPv6 Source Guard 114
Configuration Notes and Feature Limitations for IPv6 Source Guard 115
Enabling IPv6 Source Guard on a Port or Range of Ports 116
Defining Static IPv6 Source Bindings 116
Enabling IPv6 Source Guard for a VLAN 117
Enabling IPv6 Source Guard for a LAG Port for a VLAN 118
Displaying Learned IPv6 Addresses 118

Contact Information, Resources, and Conventions

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

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.ruckusnetworks.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://community.ruckuswireless.com
- 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.

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@commscope.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.ruckusnetworks.com.

Online Training Resources

To access a variety of online RUCKUS training modules, including free introductory courses to wireless networking essentials, site surveys, and products, visit the RUCKUS Training Portal at https://commscopeuniversity.myabsorb.com/. The registration is a two-step process described in this video. You create a CommScope account and then register for, and request access for, CommScope University.

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 Safety 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.

About This Document

- New in This Document..... 11
- Supported Hardware..... 11

New in This Document

The following table describes information added or modified in this guide for FastIron 10.0.10.

TABLE 2 Key Features and Enhancements in *FastIron 10.0.10*

Feature	Description	Reference
BOOTP Support	**New**: Processes the BOOTP request and uses a combination of DHCP and UDP to allocate an IP address or a range of IP addresses to BOOTP clients.	BOOTP Support on page 28 Configuring BOOTP Support on page 28
IP to Physical Port Mapping	**New**: IP addresses can be reserved within a DHCP address pool against selected Ethernet ports. This allows any device connecting to the selected port on the switch to obtain the same IP address irrespective of the client identifier sent by the device. Newly connected devices on a port are prevented from obtaining a new IP address.	Enabling IP to Physical Port Mapping on page 61
Updates to address defects	**Updated**: Minor updates on content throughout to address defects.	All chapters
Minor editorial updates	**Updated**: Minor editorial updates were made throughout the Configuration Guide.	All chapters

Supported Hardware

This guide supports the following RUCKUS products:

- RUCKUS ICX 8200 Switches
- RUCKUS ICX 7850 Switches
- RUCKUS ICX 7650 Switches
- RUCKUS ICX 7550 Switches

For information about what models and modules these devices support, refer to the hardware installation guide for the specific product family.

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 20
- Configuring an IP helper address 20
- Configuring the BOOTP and DHCP reply source address 21
- Changing the IP address used for stamping BootP and DHCP requests 21
- Changing the maximum number of hops to a BootP relay server 22
- DHCP Auto-Provisioning 22
- Auto-Provisioning Using the bootfile.bin Option 23
- DHCP Auto-Provisioning Using the Manifest File Option 24
- DHCP Auto-Provisioning Enhancements 25
- Configuring DHCP Auto-Provisioning Enhancements 27
- DHCP auto-provisioning options 28
- BOOTP Support 28
- Configuring BOOTP Support 28
- Disabling or re-enabling the DHCP client 29
- DHCP Auto-provisioning on Layer 3 devices 30
- Configuration Notes and Feature Limitations for DHCP Auto-Provisioning 34
- Disabling or re-enabling auto-provisioning 36
- Dynamic DHCP options configuration processing 37
- Discovery of SmartZone Based on DHCP Option 43 37
- Verifying Dynamic DHCP Options for a Router 39

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 device or other IP devices. 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 20. 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, and Virtual Ethernet ports. The DHCP client is not supported on tunnel ports or stacking ports when stacking is enabled.

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

DHCP Client Behavior on a Layer 3 Device

On a layer 3 device, all physical ports act as DHCP clients by default. When a DHCP offer is received, an IP address gets assigned to the port (for example, ethernet interface 1/1/1) on which the DHCP offer is received. No more DHCP offers are accepted on other ports at this point. If a virtual ethernet (VE) port is configured on the default VLAN, that VE can act as the DHCP client if the **ip dhcp-client ve default** command is configured. VEs configured on non-default VLANs (user created VLANs) do not act as the DHCP client by default. You can change this behavior by designating one of the non-default VEs as the DHCP client instead of the default VE.

Therefore, the DHCP client is functional on the following ports based on the configuration:

- Physical ports when the user does not configure a default VE, or
- The default VE configured by the user, or
- A non-default VE if the user overrides the default behavior by designating a non-default VE as the DHCP client.

DHCP Over Default Virtual Ethernet Port (Layer 3 Devices)

The following enhancements apply:

- 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 an IP address or upgrading the configuration uses zero-touch provisioning.
- By default, the ICX device allows traffic to pass across all ports (reachability).
- A single MAC address 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)

The DHCP server is reachable through a physical port, and, if option 43 VSI is configured on the DHCP server, DHCP server exchange option 43 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.

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 configurations. If any of the items are found, default Virtual Ethernet creation fails without other conditions being checked. The following configured items result in failure:

- IP routing
- VRF
- IP policy
- Route only
- RPF mode

- IP mac

Enabling the DHCP Client for a Specific VE Port

The DHCP client can be enabled for a specific Virtual Ethernet (VE) port, either default or non-default. By default, the DHCP client is enabled for the default VE port.

NOTE
When option 43 is received as “Create Default VE” while running the DHCP client on the VE, a trap and syslog is generated to ignore Option 43.

NOTE
The DHCP client can be configured for only one specific VE port at a time.

NOTE
When this feature is enabled, DHCP-based zero touch provisioning will not be functional.

The following task enables the DHCP client for a specified VE port.

1. Enter global configuration mode.

```
device# configure terminal
```

2. Enable the DHCP client for a specified VE interface.

```
device(config)# ip dhcp-client ve 22
```

The following example enables the DHCP client for a specified VE port.

```
device# configure terminal
device(config)# ip dhcp-client ve 22
```

Enabling the DHCP Client on a VE Port Associated with the Default VLAN

For the default startup configuration, a default VE is created and and the DHCP client assosciated with this default VE interface isadded to the running configuration. The following task enables the DHCP Client on a VE associated with the default VLAN.

1. Enter global configuration mode.

```
device# configure terminal
```

2. Enable the DHCP Client on a VE associated with the default VLAN.

```
device(config)# ip dhcp-client ve default
```

The following example enables the DHCP client on a VE associated with the default VLAN.

```
device# configure terminal
device(config)# ip dhcp-client ve default
```

DHCP Client in Continuous Discovery Mode (Layer 2 and Layer 3 Devices)

The DHCP Client process starts automatically when the system boots up and runs in a continuous manner.

Each time a DHCP Discovery message is sent, the interval between messages is incremented by twice the current interval multiplied by a random number between zero and one. If it is greater than the backoff-cutoff amount, it is set to that amount. The client uses an exponential backoff algorithm with some randomness, so that if many clients try to configure themselves at the same time, they will not make their requests in lockstep. The maximum amount of time that the client is allowed to back off, will be evaluated randomly between 1/2 to 1 1/2 times the maximum backoff-cutoff of 64 seconds.

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

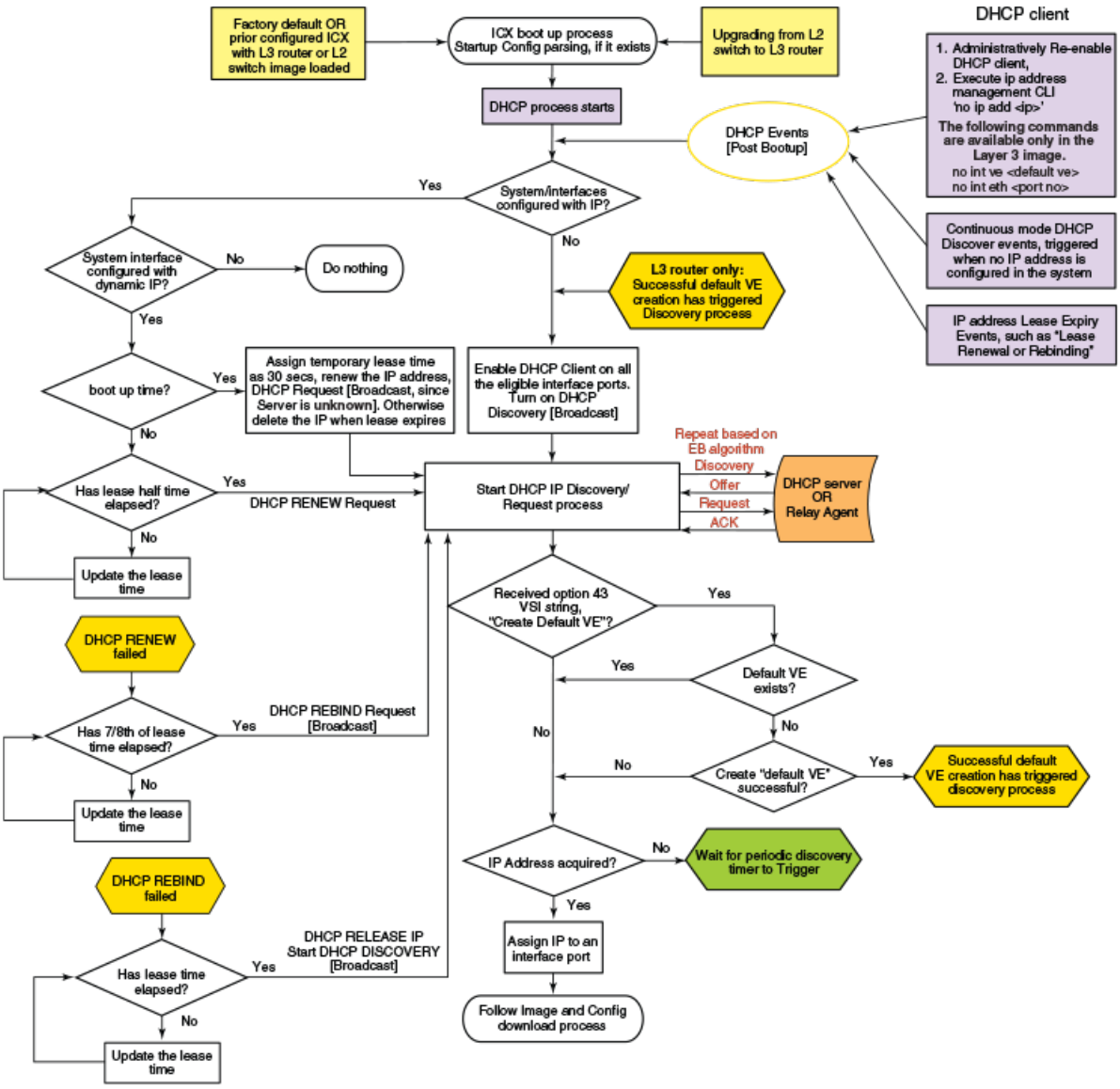
If the client does not receive a DHCP Server response, the client continues to send DHCP discover packets untill it gets a response from DHCP Server, or a static IP address is configured. The DHCP Client service or the DORA process runs by default on ICX devices if there is no static IP address configured on any of the interfaces of 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.

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.

DHCP Client Behavior after Reboot

All dynamic options, including the IP address, are relearned from the DHCP server once the ICX device reboots. All options are removed when the ICX device reboots, and are relearned when the ICX device comes back up.

BootP and DHCP Relay Parameters

The following parameters control the Layer 3 device 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 device 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 device 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 device 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 device 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
   ```

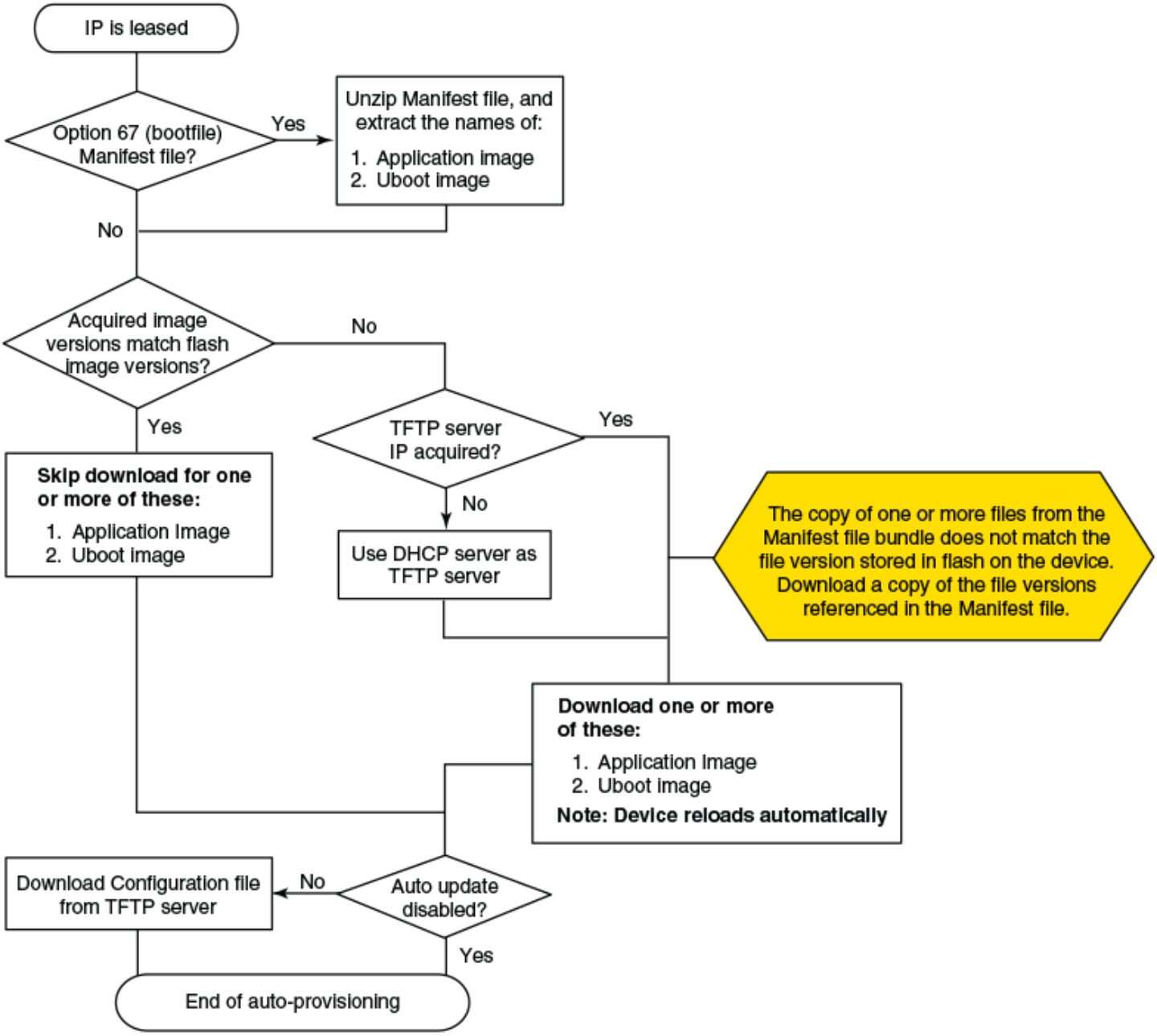
   The example allows the Layer 3 switch to forward BootP or DHCP requests that have passed through ten previous hops before reaching the Layer 3 switch. Requests that have traversed 11 hops before reaching the switch are dropped. Since the hop count value initializes at zero, the hop count value of an 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 DHCP server for details on DHCP server configuration and options.

NOTE
DHCP auto-provisioning is platform independent and does not differ 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 uses the following process.

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 memory. 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 memory. 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 or based on the location specified in option 67. Refer to DHCP Auto-Provisioning Enhancements on page 25 for more details.
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 DHCP auto-provisioning using the manifest file option was introduced in FastIron 08.0.40.

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 uses the following process.

NOTE
From FastIron 08.0.90 release onward, if the booted application image is not a Unified FastIron Image (UFI), the DHCP manifest upgrade will continue even if the image versions in flash image and Boot filename option image name are same.

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 (for example, SPR08040q054.bin) and boot image (for example, spz10106b002.bin) with the images stored in flash memory. 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 memory. 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 or based on the location specified in option 67. Refer to DHCP Auto-Provisioning Enhancements on page 25 for more details.
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, the DHCP client then proceeds to download the configuration files after the reload.

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 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.
```

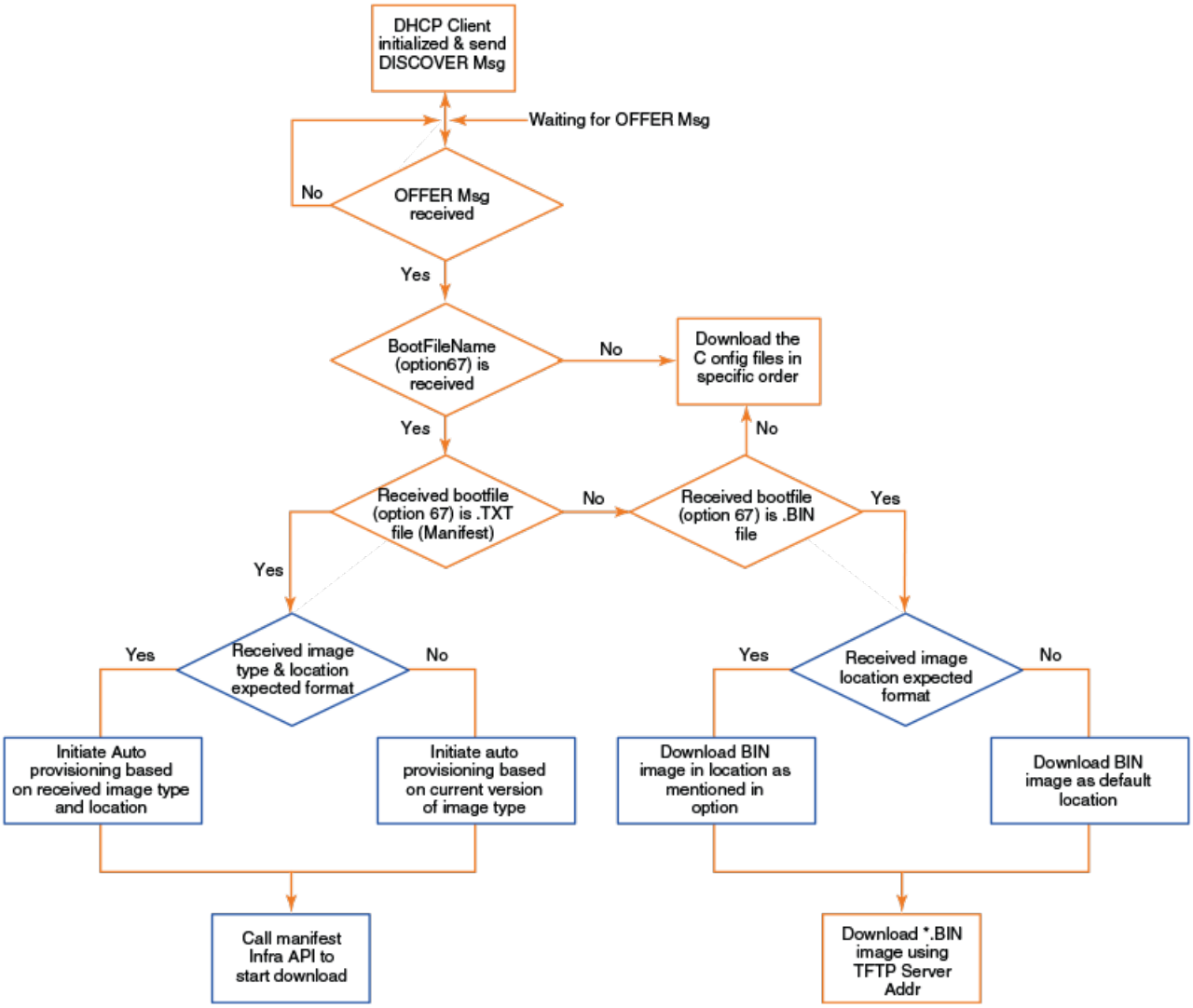
DHCP Auto-Provisioning Enhancements

Auto-provisioning allows DHCP clients to boot up with the latest flash image and configuration without manual intervention. DHCP auto-provisioning enhancements have been introduced in FastIron 08.0.80 so that you can override the default behavior. The current behavior is that the ICX device (DHCP client) is forced to download the application image type based on the current version of the device.

When DHCP auto-provisioning enhancements are configured for option 67, the application image type (router or switch) and the flash image location (primary or secondary) can be configured as part of option 67 along with the file name. This means that you can decide the image type and the flash memory location to which the DHCP client should be upgraded. The DHCP client then upgrades to a specific image type and flash location as received by option 67 from the server.

When option 67 is received from the server, the DHCP client triggers DHCP auto-provisioning based on the image type and flash location specified in option 67. If a specified image type and flash location is not received from the server, the DHCP client behaves according to the default settings.

FIGURE 3 DHCP Auto-Provisioning Enhancements



DHCP auto-provisioning enhancements allow option 67 to be configured with up to three ASCII strings, separated by a space, where each ASCII string configures a specific operation. The example below configures the “fi8080_manifest.txt” boot image, router as the image type, and the flash image as primary.

```
device(config-dhcp-GenericOption)# option bootfile-name "fi8080_manifest.txt router primary"
```

The example below configures the “fi8080_manifest.txt” boot image, router as the image type, and the flash image as secondary.

```
device(config-dhcp-GenericOption)# option bootfile-name "fi8080_manifest.txt router secondary"
```

The example below configures the “fi8080_manifest.txt” boot image, switch as the image type, and the flash image as secondary.

```
device(config-dhcp-GenericOption)# option bootfile-name "fi8080_manifest.txt switch secondary"
```

The example below configures the “fi8080_manifest.txt” boot image, switch as the image type, and the flash image as primary.

```
device(config-dhcp-GenericOption)# option 67 "fi8080_manifest.txt switch primary"
```

For information on configuration notes and feature limitations for DHCP auto-provisioning, refer to Configuration Notes and Feature Limitations for DHCP Auto-Provisioning on page 34.

Configuring DHCP Auto-Provisioning Enhancements

The application image type (router or switch), the flash image (primary or secondary), and the file name to be used by the DHCP client can all be configured as part of option 67 using one command. The following task configures the “fi8080_manifest.txt” boot image, router as the image type, and the flash image as primary as part of option 67.

1. Use the **configure terminal** command to enter global configuration mode.

```
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 GenericOption
```

4. Configure the DHCP server address pool.

```
device(config-dhcp-GenericOption)# dhcp-default-router 10.10.70.1
device(config-dhcp-GenericOption)# network 10.10.70.0 255.255.254.0
device(config-dhcp-GenericOption)# lease 1 0 0
device(config-dhcp-GenericOption)# dns-server 10.10.64.1 8.8.8.8
device(config-dhcp-GenericOption)# domain-name office.s-cloud.net
```

5. Use the **option** command with the **bootfile-name** keyword, specifying a file name, the flash image location, and the image type, to configure option 67 with both the image type and flash image location.

```
device(config-dhcp-GenericOption)# option bootfile-name ascii “fi8080_manifest.txt router primary”
```

   In this example, boot image fi8080_manifest.txt, router as the image type, and flash image as primary is configured to be used by the DHCP client.

   NOTE
   The configuration of the image type and flash location for option 67 is case insensitive.

The following example configures the “fi8080_manifest.txt” boot image, router as the image type, and flash image as primary as part of option 67 using one command.

```
device# configure terminal
device(config)# ip dhcp-server enable
device(config)# ip dhcp-server pool GenericOption
device(config-dhcp-GenericOption)# dhcp-default-router 10.10.70.1
device(config-dhcp-GenericOption)# network 10.10.70.0 255.255.254.0
device(config-dhcp-GenericOption)# lease 1 0 0
device(config-dhcp-GenericOption)# dns-server 10.10.64.1 8.8.8.8
device(config-dhcp-GenericOption)# domain-name office.s-cloud.net
device(config-dhcp-GenericOption)# option bootfile-name ascii “fi8080_manifest.txt router primary”
```

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

BOOTP Support

The Bootstrap Protocol (BOOTP) uses a combination of Dynamic Host Configuration Protocol (DHCP) and User Datagram Protocol (UDP) to assign an IP address or a range of IP addresses to the BOOTP clients. By default, the DHCP server is enabled to process BOOTP requests from the BOOTP client at the global level, and dynamic BOOTP is disabled at the DHCP server address pool. Dynamic BOOTP enables the DHCP server to assign the IP address or a range of IP addresses to the BOOTP clients within its address pool.

Configuring BOOTP Support

Dynamic Bootstrap Protocol (BOOTP) is enabled at the DHCP server address pool. The Dynamic BOOTP allows the DHCP server to assign an IP address or a range of IP addresses to the BOOTP clients within its address pool.

1. Enter global configuration mode.

```
device# configure terminal
```

2. Enable the DHCP server.

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

3. Enable the BOOTP request.

```
device(config)# no ip dhcp-server bootp ignore
```

4. Create a DHCP server pool.

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

5. Configure the DHCP server address pool.

```
device(config-dhcp-GenericOption)# dhcp-default-router 10.10.70.1
device(config-dhcp-GenericOption)# network 10.10.70.0 255.255.254.0
device(config-dhcp-GenericOption)# lease 1 0 0
device(config-dhcp-GenericOption)# dns-server 10.10.64.1 8.8.8.8
device(config-dhcp-GenericOption)# domain-name office.s-cloud.net
```

6. Enable dynamic BOOTP.

```
device(config-dhcp-GenericOption)# dynamic-bootp
```

The following example enables dynamic BOOTP at the DHCP server address pool. The DHCP server assigns an IP address or a range of IP addresses to the BOOTP client within its address pool.

```
device# configure terminal
device(config)# ip dhcp-server enable
device(config)# no ip dhcp-server bootp ignore
device(config)# ip dhcp-server pool GenericOption
device(config-dhcp-GenericOption)# dhcp-default-router 10.10.70.1
device(config-dhcp-GenericOption)# network 10.10.70.0 255.255.254.0
device(config-dhcp-GenericOption)# lease 1 0 0
device(config-dhcp-GenericOption)# dns-server 10.10.64.1 8.8.8.8
device(config-dhcp-GenericOption)# domain-name office.s-cloud.net
device(config-dhcp-GenericOption)# dynamic-bootp
```

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 global configuration mode.

```
switch# configure terminal
```

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

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

3. Enter the **ip dhcp-client enable** command to re-enable the DHCP client.

```
switch(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.

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

5. Enter the **no ip dhcp-client disable** command to re-enable the DHCP client service on all physical interface and virtual interface level.

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

6. Enter interface configuration mode.

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

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

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

8. Enter the **ip dhcp-client enable** command at the interface configuration level to re-enable the DHCP client.

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

9. Enter the **ip dhcp-client enable** command at the virtual interface level to re-enable the DHCP client.

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

The DHCP client is enabled by default. The following example disables the DHCP client for a switch.

```
switch# configure terminal
switch(config)# no ip dhcp-client enable
switch(config)# ip dhcp-client enable
```

The following example re-enables the DHCP client for a switch if it has been disabled.switch# configure terminal

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

The following example disables the DHCP client service on all physical interface and virtual interface levels for a router.

```
router# configure termnial
router(config)# ip dhcp-client disable
```

The following example re-enables the DHCP client service on all physical interface and virtual interface level for a router.

```
router# configure terminal
router(config)# no ip dhcp-client disable
```

Refer to the *RUCKUS FastIron Command Reference* for more information on the commands used in this task.

DHCP Auto-provisioning on Layer 3 devices

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

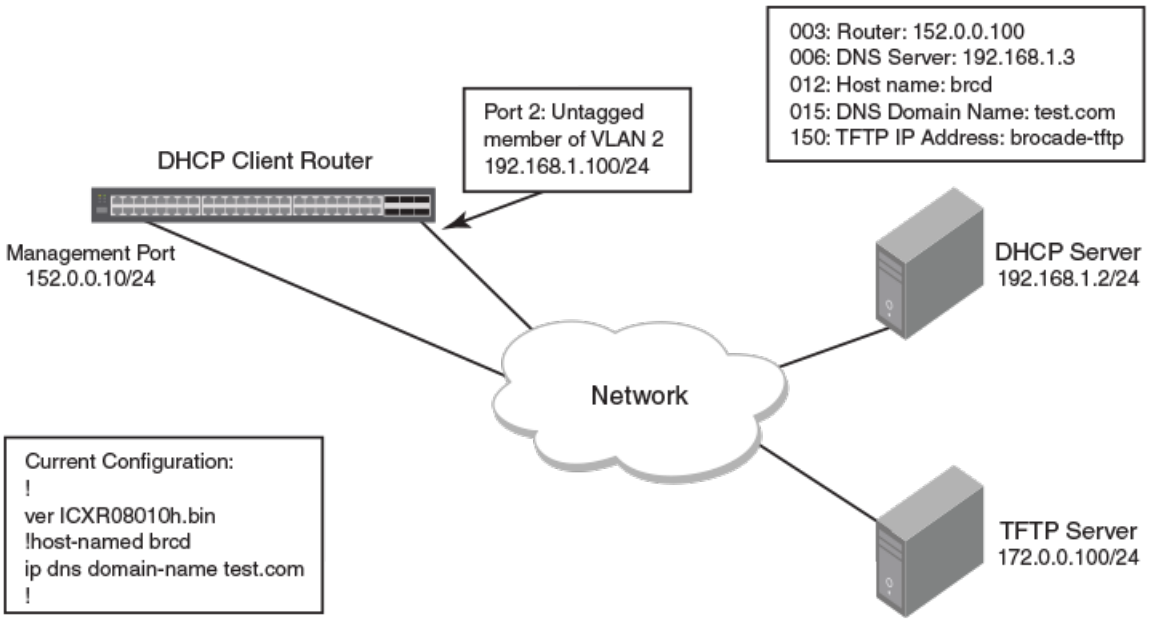
- If the non-default VLAN has multiple untagged ports connected to different DHCP servers, the first port that received the IP address offer will be considered and the other port will not receive an IP address. This behavior applies for default VLANs, too.
- After an image update and device reload, the 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.

Consider the following behavior for a Layer 3 DHCP Client:

- The IP address is configured on the specific client port .
- The default route is configured as “IP route” with the distance metric 254.

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

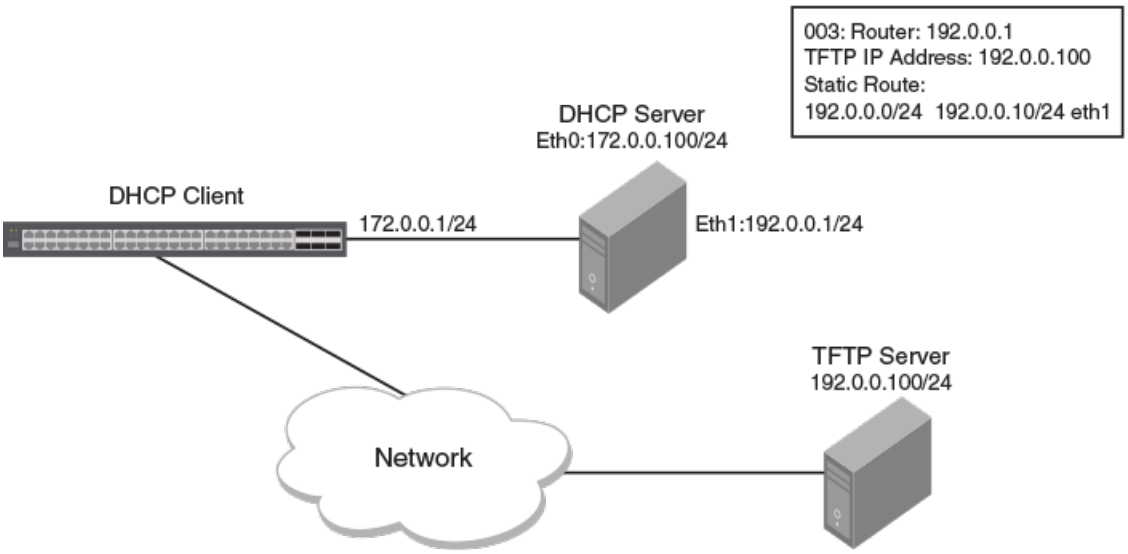
Scenario 1: DHCP Auto-provisioning on a Layer 3 Device



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.

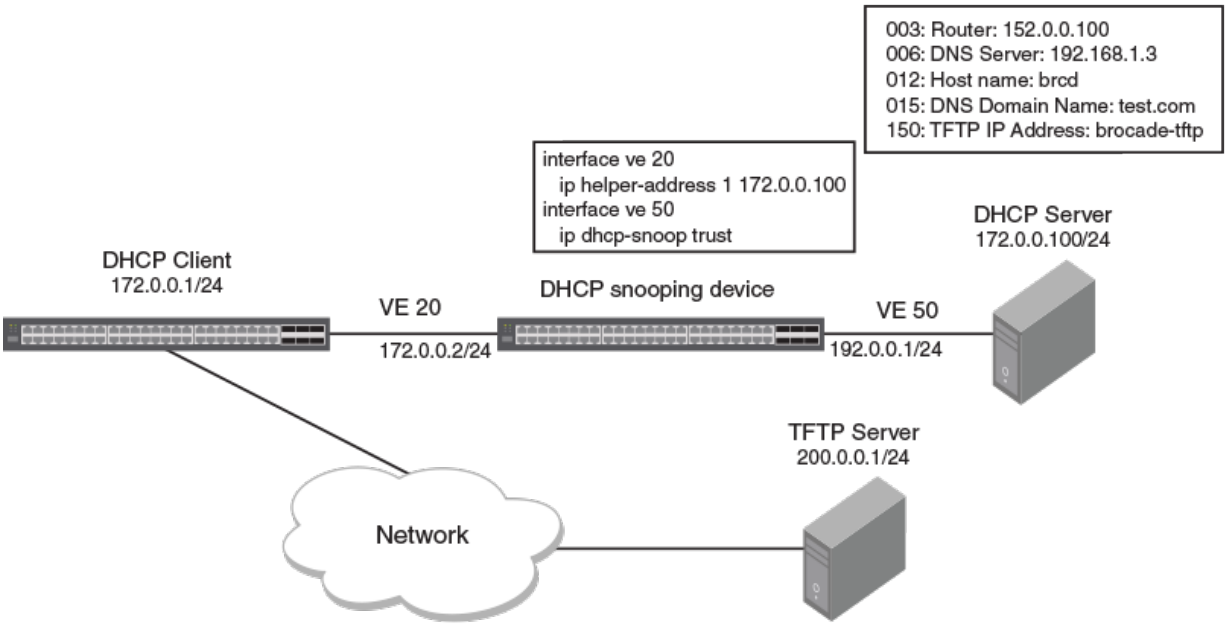
1. The FastIron router (DHCP client) connected to the DHCP server is booted.
2. The client obtains a dynamic IP address lease from the DHCP server through the untagged member port 2 of the VLAN 2 (which is a non-default VLAN) along with other DHCP server options.
3. Once DHCP server options are enabled, 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



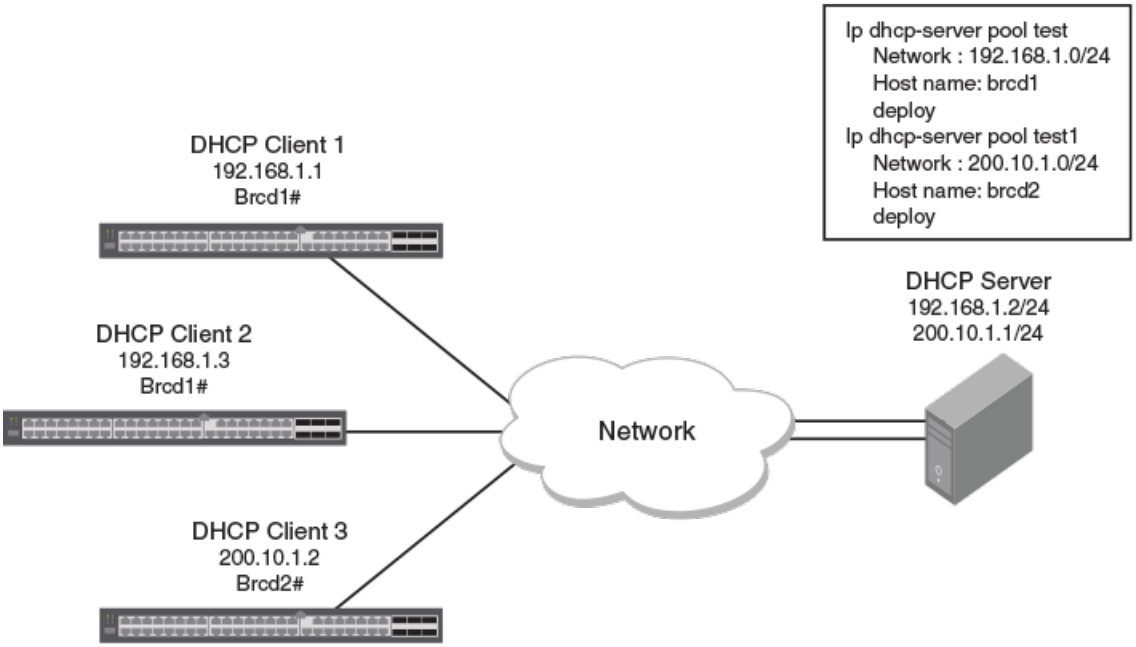
In this scenario, the DHCP client and server are connected in the same network, but the TFTP server is connected in a different network through the DHCP server. Here the DHCP client device needs a default route to reach the TFTP server. The steps are the same as in scenario 1, except that the TFTP server 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



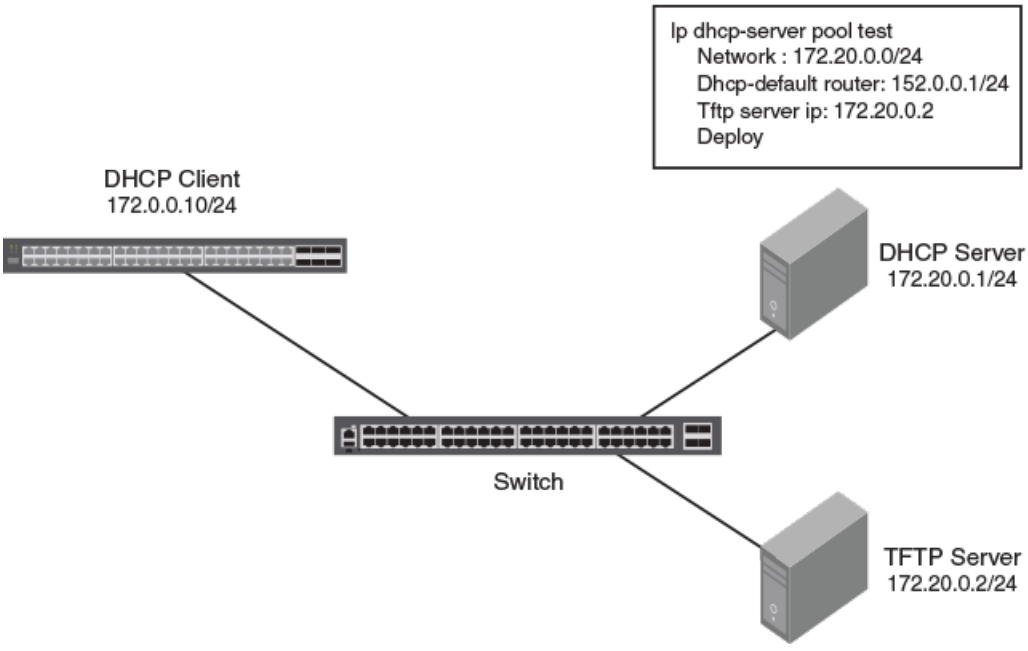
In this scenario, the DHCP client and server are connected through ports on which DHCP snooping or relay agent are enabled and are part of non-default VLANs. The working scenario is the same as Scenario 1.

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 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 DHCP auto-provisioning.

- Although the DHCP server may provide multiple addresses, only one IP address is installed at a time.
- DHCP auto-provisioning is not supported together with DHCP snooping.
- POE firmware is bundled with the ICX image file. If the ICX software is upgraded, the POE firmware is automatically updated after the upgrade completes.
- 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.
- 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, the boot image download is skipped if the flash images are the same.
- From FI 09.0.10a, the DHCP server accepts more than one default router in the address pool for a Layer 3 image. However, the DHCP client configures the first router-ip as the default route when the options are received.
- The DHCP client contacts the TFTP server to obtain the hostnameMAC-config.cfg file only five times if the TFTP server is busy or 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. After five minutes, 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.

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.
- The option 67 (boot file name) is available for DHCP Offer and ACK packets only under Option 67 and not under the “Boot file name” header.

The following configuration rules apply to DHCP auto-provisioning enhancements:

- Only “router” can be used for specifying an image type. If any other value is entered, the DHCP client accepts and stores the values specified in the string. However, these values cannot be used and the DHCP client behavior will not change based on the option 67 configurations.
- Only “primary” or “secondary” can be used for specifying the flash image. If any other value is entered, the DHCP client accepts and stores the values specified in the string. However, these values cannot be used and the DHCP client behavior will not change based on the option 67 configurations.
- The received option 67 value for the boot image name is not saved in the DHCP client configuration.
- DHCP auto-provisioning enhancements are only supported beginning with FastIron 08.0.80. If the DHCP client image is downgraded to that of a prior release, and option 67 is received by the DHCP client with the image type and flash location specified, DHCP auto-provisioning does not work because the DHCP client expects only a specified file type. Option 67 must be reconfigured on the DHCP server for the format supported for the particular release.

High Availability Considerations

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

Upgrade Considerations

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

How DHCP Client-Based Auto-Provisioning and Flash Image Update Works

Auto-provisioning is enabled by default. To disable auto-provisioning, refer to Disabling or re-enabling the DHCP client on page 29 and Disabling or re-enabling auto-provisioning on page 36 respectively.

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.
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 memory. 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 memory. 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: ICX7650-router.cfg	**New format:** ICX7650.cfg

< ICX7650>.cfg overwrites the existing configuration.

6. default.cfg (applies to all devices), (for example: default.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
From FI 09.0.10a, all dynamic options including the IP address route are relearned (not persistent) from the DHCP server 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.

Discovery of SmartZone Based on DHCP Option 43

Beginning with SmartZone release 5.0, the administrator can monitor and manage switches and routers in the RUCKUS ICX 7000 switches running FastIron 08.0.80 and later. ICX (the DHCP client) can parse the value of DHCP option 43 containing SmartZone IP addresses received from the DHCP server and connect to SmartZone.

Discovery of SmartZone based on DHCP option 43 works in the following manner:

- The DHCP client sends the vendor class identifier (VCI) option as "Ruckus CPE" to the DHCP server in every request packet.
- The DHCP client processes the vendor-specific information (VSI) option data during the RENEW & REBIND process.
- The SmartZone IP Address data received through VSI is not displayed in the running configuration.
- The **show ip dhcp-client options** command displays the received VSI data in TLV or ASCII format. The data can be displayed in two formats based on data received. Refer to the **show ip dhcp-client options** command in the *RUCKUS FastIron Command Reference* for more information.
- If the DHCP client fails to parse the received VSI data, or is not able to extract the SmartZone IP addresses from the VSI data received, the SmartZone IP addresses are not passed to the FSM API.

The following example shows how a DHCP server can be configured to send SmartZone IP addresses to ICX devices using DHCP Option 43.

Configure DHCP Option 43 on the DHCP server, using RKUS.scg-address to identify the SmartZone IP addresses. A single SmartZone IP address or a comma-separated list can be configured. SmartZone IP addresses are sent with a sub-option value of 6. The ICX device ignores all other data in DHCP Option 43 if SmartZone IP addresses are present. The IP addresses listed in the following configuration are examples only.

```
subnet 192.168.12.0 netmask 255.255.255.0 {
range 192.168.12.100 192.168.12.199;
option routers 192.168.12.1;
option subnet-mask 255.255.255.0;
option broadcast-address 192.168.12.255;
option ntp-servers 192.168.11.22;
class "Ruckus AP" {
match if option vendor-class-identifier = "Ruckus CPE";
```

```
option vendor-class-identifier "Ruckus CPE";
default-lease-time 86400;
vendor-option-space RKUS;
option RKUS.scg-address "192.168.11.200, 192.168.11.201, 192.168.11.202";
}
}
```

Configuration Notes and Feature Limitations

The following configuration notes and feature limitations apply for discovery of SmartZone based on DHCP option 43:

- The vendor-specific information (VSI) data received from the DHCP server must be in simple ASCII text format.
- The VCI option must be configured as “Ruckus CPE” and sent to the DHCP server during DHCP discovery and renewed. The DHCP server then fills the VSI option data in the offer packet that is sent to the client in response.
- A maximum of 128 characters (bytes) of VSI data can be received and processed by the DHCP client. If the received VSI data size is more than 128 characters, the DHCP client does not save or process the received data.
- With the exception of the “create default ve” value and SmartZone IP addresses in ASCII format with sub-option 7, the DHCP client treats any received option 43 information in TLV format.
- The DHCP client passes the IP address list to the FSM API only when the received VSI data is in TLV format with sub-option Code 6, and the corresponding data is in IP address format with a comma (,) separating the IP addresses.

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
...
!
!
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
 ...
!
!
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 41
- DHCP Server Options 46
- Disabling or re-enabling the DHCP server on the management port 53
- Setting the wait time for ARP ping response 53
- DHCP relay agent information support (option 82) 54
- Configuring the IP address of the DHCP server 54
- Configuring the Boot Image 54
- Deploying an Address Pool Configuration to the Server 55
- Specifying the Default Router Available to the Client 55
- Specifying DNS Servers Available to the Client 55
- Configuring the Domain Name for the Client 56
- Configuring the lease duration for the address pool 56
- Configuring the Number of Leases for the Address Pool 56
- Specifying addresses to exclude from the address pool 57
- Configuring the NetBIOS server for DHCP clients 57
- Configuring the Subnet and Mask of a DHCP Address Pool 58
- Configuring the TFTP Server 58
- Configuring X Window System Display Manager IP Addresses (Option 49) 58
- Vendor-specific Information (Option 43 and Option 60) Configurations 59
- Enabling static IP to MAC address mapping 60
- Enabling IP to Physical Port Mapping 61
- Configuring Avaya IP telephony (options 176 and 242) 62
- Configuring WPAD (option 252) 64
- Displaying DHCP server information 65

DHCP Servers

All FastIron devices can be configured to function as DHCP servers. Internet Systems Consortium (ISC) DHCP is supported.

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.

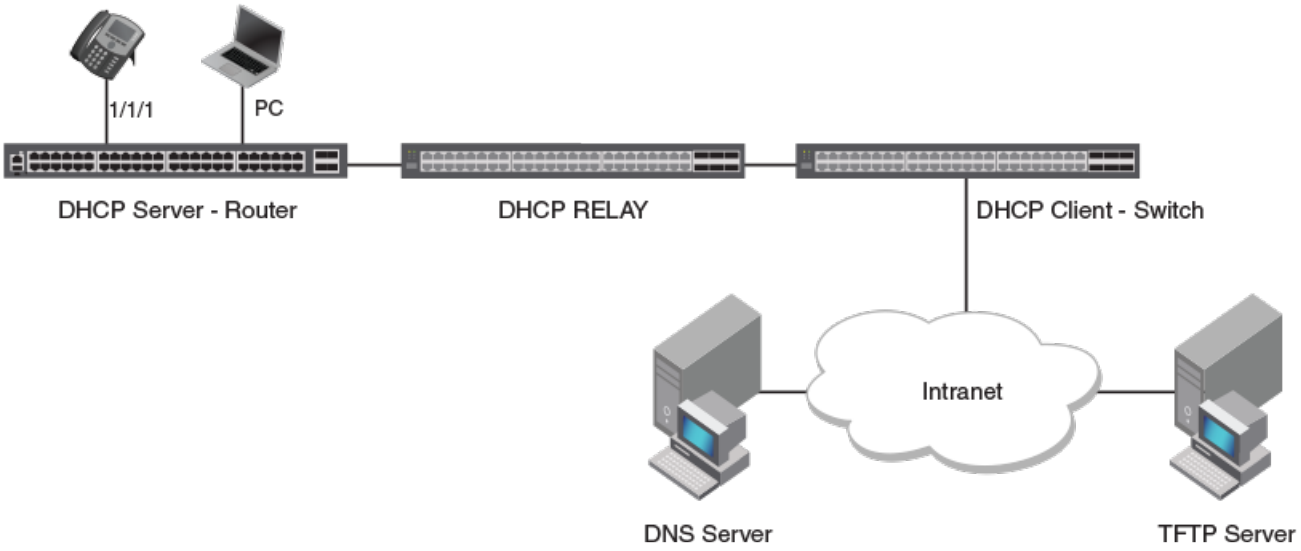
DHCP allocates temporary or permanent network IP addresses to clients. When a client requests the use of an address for a time interval, the DHCP server guarantees not to reallocate that address within the requested time and tries to return the same network address each time the client makes a request. 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 not supported on non-default VRF.
- Physical ports, LAG ports, Virtual Ethernet (VE) ports, and management ports are supported.
- Stacking ports, PE ports, and loopback ports are not supported.
- 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 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.
- A network cannot be configured for a DHCP server pool if that network is already part of a network in a different DHCP server pool.
- A network cannot be configured for a DHCP server pool if that network is already a superset of a network in a different DHCP server pool. For example, if network 10.10.10.0/24 is configured in DHCP server pool 1, then then network 10.10.0.0/16 and 10.10.10.0/26 cannot be configured for other DHCP server pools.

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.
- The following table shows IP DHCP binding scalability for RUCKUS ICX devices for a stand-alone switch or a stack:

TABLE 4 IP DHCP Binding Scalability

Device	IP DHCP Binding Scalability
RUCKUS ICX 7550	3000
RUCKUS ICX 7650	3000
RUCKUS ICX 7850	3000
RUCKUS ICX 8200	3000

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.
- The options in the DHCP server pool cannot be configured without first configuring the network option.
- 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.

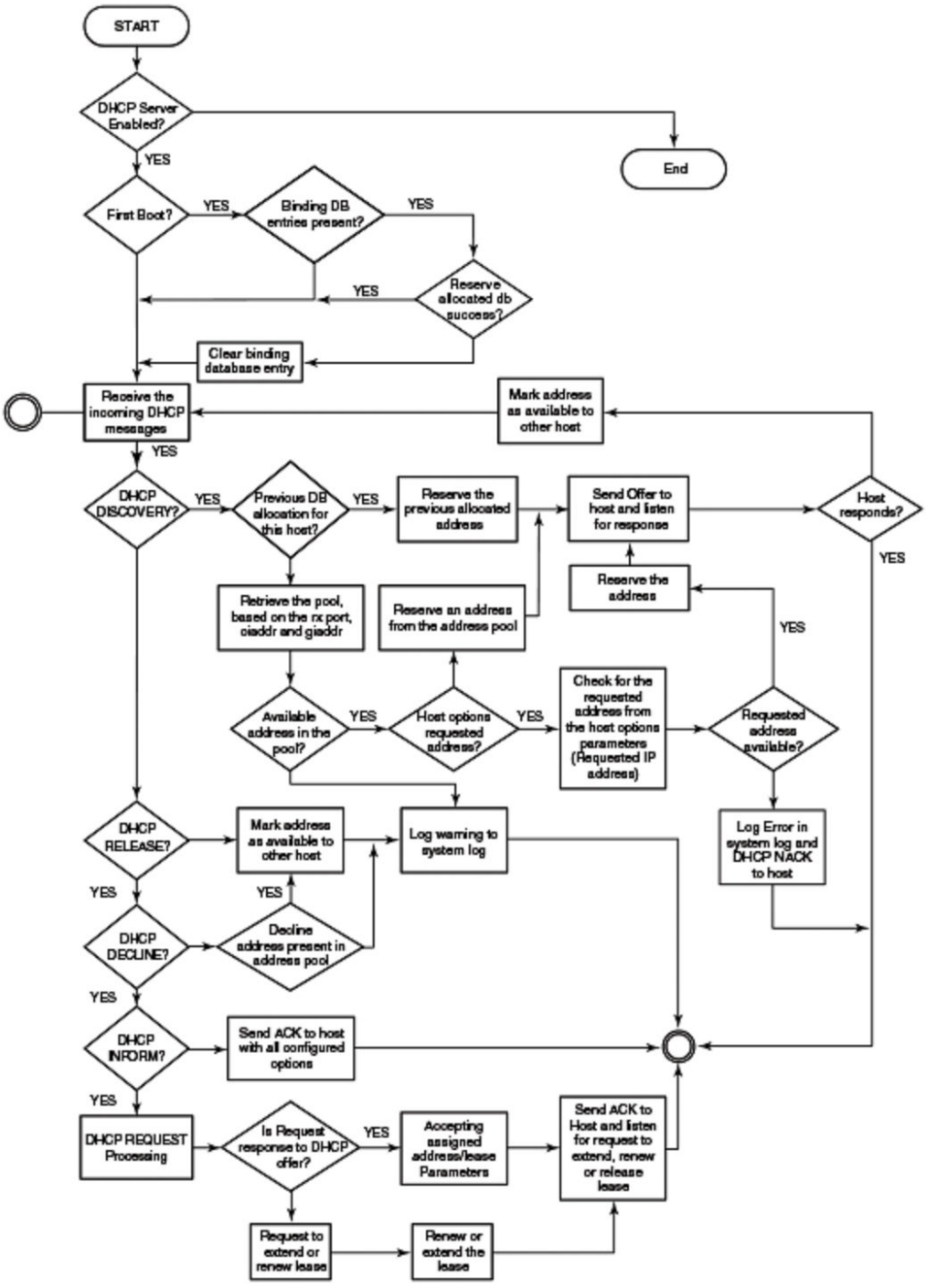
```
device(config)# clear ip dhcp-server binding *
```

   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	Enabled
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 3000 DHCP clients.

Where a FastIron device is configured as a DHCP server, you can configure DHCP options. These options are passed to the connected DHCP clients and allow configuration of parameters such as default router, host name, and domain name server.

The list of supported DHCP options that are configured using option number is shown in the following table:

The following option numbers must be configured using the option number: 80 through 84, 90, 95, 96, 99 through 111, 115 through 117, 126 through 149, 151 through 255. The options 1 through 254 are allowed to be configured using the option number. Options that have option names support are automatically configured as **option option-name** *option-value*.

TABLE 6 DHCP Server Options

Option	Option Number	Option Name	Description / Notes
subnet-mask	1	Subnet Mask	Specifies the client subnet mask (per RFC 950). This is not configurable using the option command. This option is configured using the network (dhcp) command. Network <router IP> <subnet mask>
time-offset	2	Time offset	Specifies the offset of the subnet of the client in seconds from UTC.
routers	3	Router Option	Specifies an IP addresses of the default router on the client subnet. Only one router can be specified. **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: DHCP: Failed to configure default gateway.
time-servers	4	Time Server	Specifies a list of Time Servers available to the client. Time Servers are listed in order of preference.
ien116-name-servers	5	Name Server	Specifies a list of Name Servers available to the client. Name Servers are listed in order of preference.

TABLE 6 DHCP Server Options (continued)

Option	Option Number	Option Name	Description / Notes
domain-name-servers	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.
log-servers	7	Log Server	Specifies a list of UDP log servers available to the client. Servers are listed in order of preference.
cookie-servers	8	Cookie Server	Specifies the list of RFC 865 cookie servers available to the client. Servers are listed in order of preference. .
lpr-servers	9	LPR Server	Specifies a list of Line Printer Servers available to the client. Servers are listed in order of preference.
impress-servers	10	Impress Server	Specifies a list of Imagen Impress Servers available to the client. Servers are listed in order of preference.
resource-location-servers	11	RLP Server	Specifies a list of Resource Location Servers available to the client. Servers are listed in order of preference.
host-name	12	Hostname	Configures the host name that can be assigned to the DHCP clients.
boot-size	13	Boot size	Specifies the length of the default boot image for the client in 512-octet blocks.
merit-dump	14	Merit dump	Specifies the path name of the core file of the client when the client crashes.
domain-name	15	Domain name	Specifies the domain name the client should use when resolving host names using the Domain Name System.
swap-server	16	Swap Server	Specifies the IP address of the client Swap Server.
root-path	17	Root Path	Specifies the path name (entered as an ASCII character string) that contains the client root disk.
extensions-path	18	Extension Path	Specifies a file, retrievable through TFTP, that contains information that can be interpreted in the same way as the vendor-extension field within the BOOTP.
ip-forwarding	19	IP forwarding	Specifies if the client should configure its IP layer for packet forwarding.
non-local-source-routing	20	Non-local source routing	Specifies a flag to enable or disable non-local source route forwarding in the client.
policy-filter *ip-address network mask*	21	Policy Filter	Specifies Policy Filters for non-local source routing. The filters consist of a list of IP addresses and masks that specify destination/mask pairs with which to filter incoming source routes. Any source-routed datagram whose next-hop address does not match one of the filters should be discarded by the client.
max-dgram-reassembly	22	Maximmum datagram reassembly	Specifies the maximum size datagram that the client can reassemble.
default-ip-ttl	23	Default IP TTL	Specifies the default time-to-live that the client should use on outgoing datagrams.
path-mtu-aging-timeout	24	Path MTU aging timeout	Specifies the timeout (in seconds) to use when aging Path MTU values discovered.
path-mtu-plateau-table	25	Path MTU plateau table	Specifies a table of MTU sizes to use when performing Path MTU Discovery.
interface-mtu	26	Interface MTU	Specifies the MTU to use for the interface.
all-subnets-local	27	All subnets local	Specifies that all connected subnets use the same MTU.
broadcast-address	28	Broadcast Address	Specifies the Broadcast Address in use on the client subnet.
perform-mask-discovery	29	Perform mask discovery	Specifies a table of MTU sizes to use when performing Path MTU Discovery.
mask-supplier	30	Mask Supplier	Specifies if the client responds to subnet mask requests using ICMP.

TABLE 6 DHCP Server Options (continued)

Option	Option Number	Option Name	Description / Notes
router-discovery	31	Router Discovery	Specifies if the client should perform Router Discovery.
router-solicitation-address	32	Router Request	Specifies the address to which the client should transmit router solicitation requests.
static-routes *destination ip-address static-route*	33	Static Route	Specifies a list of Static Routes that the client should install in its routing cache. If multiple routes to the same destination are specified, they are listed in descending order of priority. The routes consist of a list of IP address pairs. The first address is the destination address, and the second address is the router for the destination. Note that the default route (0.0.0.0) is an illegal destination for a static route.
trailer-encapsulation	34	Trailer encapsulation	Specifies if the client uses trailers when using the ARP protocol.
arp-cache-timeout	35	ARP cache timeout	Specifies the timeout in seconds for ARP cache entries.
ieee802-3-encapsulation	36	IEEE 802-3 encapsulation	Specifies if the client should use Ethernet Version 2 (RFC 894) or IEEE 802.
default-tcp-ttl	37	Default TCP TTL	Specifies the default TTL that the client should use when sending TCP segments.
tcp-keepalive-interval	38	TCP keepalive interval	Specifies the TCP keepalive interval timeout value used by the client.
tcp-keepalive-garbage	39	TCP keepalive garbage	Specifies a flag to enable or disable TCP keepalive garbage in the client.
nis-domain	40	NIS Domain	Specifies the NIS domain (entered as an ASCII character string) for the client.
nis-servers	41	NIS Servers	Specifies a list of IP addresses for NIS servers available to the client. Servers are listed in order of preference.
ntp-servers	42	NTP Servers	Specifies a list of IP addresses for NTP servers available to the client. Servers are listed in order of preference.
vendor-encapsulated-options { **ascii** *string* | **hex** *string* | **ip** { *address* | *address-list*} }	43	Vendor Specific	Specifies vendor-specific information. This allows clients and servers to exchange vendor-specific information. The vendor is specified in the Vendor Class Identifier option (option 60).
netbios-name-servers	44	NetBIOS Name Srv	Specifies a list of NetBIOS Name Servers (NBNS) (RFC 1001 and RFC 1002). NBNS servers are listed in order of preference.
netbios-dd-server	45	NetBIOS Dist Srv	Specifies a list of NetBIOS Datagram Distribution Servers (NBDD) servers (RFC 1001 and RFC 1002). NBDD servers are listed in order of preference.
netbios-node-type	46	NitBios Node Type	Specifies the NetBIOS node type option.
netbios-scope	47	NetBIOS Scope	Specifies the NetBIOS over TCP/IP scope parameter (RFC 1001 and RFC 1002) for the client.
font-servers	48	X Window Font	Specifies a list of IP addresses of X Window System Font servers available to the client. X Window System Font servers are listed in order of preference.
x-display-manager	49	X Window Manager	Specifies a list of IP addresses of X Window System Display Managers available to the client. X Window System Display Managers are listed in order of preference.
dhcp-requested-address	50	Address Request	Specifies an IP address used in a client request (DHCPDISCOVER) to allow the client to request a particular IP address be assigned.
dhcp-lease-time	51	DHCP Lease Time	Specifies the DHCP lease time.
dhcp-option-overload	52	DHCP Option Overload	Indicates the DHCP 'sname' or 'file' fields are overloaded by using them to carry DHCP options
dhcp-message-type	53	DHCP Message Type	Specifies the type of DHCP message contained in the DHCP packet.

TABLE 6 DHCP Server Options (continued)

Option	Option Number	Option Name	Description / Notes
dhcp-server-identifier	54	DHCP Server Identifier	Specifies the IP address of the server.
dhcp-parameter-request-list *list-of-intergers*	55	DHCP Parameter Request List	Specifies the options to be sent to the client.
dhcp-message	56	DHCP Message	This option is used by a DHCP server to provide an error message to a DHCP client in a DHCPNAK message in the event of a failure.
dhcp-max-message-size	57	DHCP Maxiumum Message Size	DHCP maximum message size. Used as default, if not provided by the client.
dhcp-renewal-time	58	DHCP Renewal Time	Specifies the renewal time in the DHCP client.
dhcp-rebinding-time	59	DHCP Rebinding Time	Specifies the rebinding time in the DHCP client.
vendor-class-identifier *string*	60	Vendor Class Identifier	Specifies the Vendor Class Identifier. This is used in conjunction with option 43 (Vendor Specific information), allowing clients and servers to exchange vendor-specific information.
dhcp-client-identifier	61	DHCP Client Identifier	Specifies the DHCP client identifier.
nwip-domain	62	NetWare/IP Domain	Specifies the NetWare/IP Domain Name used by the NetWare/IP product.
nwip-suboptions	63	NetWare sub-options	Specifies a sequence of suboptions for NetWare/IP clients (RFC2242).
nisplus-domain	64	NIS-Domain-Name	Specifies the NIS+ domain (entered as an ASCII character string) for the client.
nisplus-servers	65	NIS-Server-Addr	Specifies a list of IP addresses for NIS+ servers available to the client. Servers are listed in order of preference.
tftp-server-name	66	TFTP server hostname or IP address	Specifies the address or name of the TFTP server available to the client.
bootfile-name	67	Boot File name	Specifies a boot image to be used by the client.
mobile-ip-home-agent	68	Home-Agent-Addrs	Specifies a list of IP addresses for Mobile IP Home Agents available to the client. Agents are listed in order of priority.
smtp-server	69	SMTP-Server	Specifies a list of Simple Mail Transport Protocol (SMTP) Servers available to the client. Servers are listed in order of priority.
pop-server	70	POP3-Server	Specifies a list of Post Office Protocol (POP3) Servers available to the client. Servers are listed in order of priority.
nntp-server	71	NNTP-Server	Specifies a list of Network News Transport Protocol (NNTP) Servers available to the client. Servers are listed in order of priority.
www-server	72	WWW-Server	Specifies a list of World Wide Web (WWW) Servers available to the client. Servers are listed in order of priority.
finger-server	73	Finger-Server	Specifies a list of Finger Servers available to the client. Servers are listed in order of preference.
irc-server	74	IRC-Server	Specifies a list of Internet Relay Chat (IRC) Servers available to the client. Servers are listed in order of priority.
streettalk-server *ip-address*	75	StreetTalk-Server	Specifies a list of StreetTalk Servers available to the client. Servers are listed in order of priority.
streettalk-directory-assistance-server *ip-address*	76	STDA-Server	Specifies a list of StreetTalk Directory Assistance (STDA)Servers available to the client. Servers are listed in order of priority.
user-class	77	User Class	Specifies identifying information to the DHCP client.
slp-directory-agent	78	SLP Directory Agent	Specifies the IP addresses of SLP Directory Agents, and flags to set the use of these addresses.

TABLE 6 DHCP Server Options (continued)

Option	Option Number	Option Name	Description / Notes
slp-service-scope	79	SLP Service Scope	Specifies a list of service scopes for SLP, and whether the use of this list is mandatory.
nds-servers	85	NDS Servers	Specifies the IP addresses for Novell Directory Services (NDS) servers available to the client. Servers are listed in order of priority.
nds-tree-name *string*	86	NDS Tree Name	Specifies the name of the Novell Directory Services (NDS) Tree to which the client will connect.
nds-context	87	NDS Context	Specifies the name of the initial Netware Directory Service for an NDS client.
bcms-controller-names	88	BCMCS Domain List	Specifies a list of Broadcast and Multicast Service (BCMCS) Controller domain names.
bcms-controller-address	89	BCMCS IPv4 addr	Specifies a list of IP addresses for Broadcast and Multicast Service (BCMCS) controllers. Controllers are listed in order of preference56.
client-last-transaction-time	91	Client last transaction time	Specifies the last client transactin time in units.
associated-ip	92	Associated IP	Specifies that all IP addresses associated with a given DHCP client are listed.
pxe-system-type	93	PXE System Type	A list of one ore more 16-bit integers that allows a client to specify its pre-boot architecture type(s).
pxe-interface-id	94	Client NDI	Specifies the Network Interface Identifier (NDI) for the client.
option 95	95	LDAP	This option is supported if the option value type is IP, ASCII, or HEX
pxe-client-id	97	PXE client ID	Allows a client to specify its PXE client identity.
uap-servers	98	User-Auth	Specifies a list of URLs, each pointing to a user authentication service that is capable of processing authentication requests encapsulated in the User Authentication Protocol (UAP). If a URL does not contain a port component, the normal default port is assumed (port 80 for http and port 443 for https) If a URL does not include a path component, the path /uap is assumed.
option 100	100	Pcode	Specifies the TZ-POSIX string used to provide timezone details.
option 101	101	Tcode	Specifies the TZ-Database string used to provide timezone details.
option *value*	102 - 111	Removed/ Unassigned	These options are supported if the value type is defined as IP, ASCII, or HEX
netinfo-server-address *ip-address*	112	Netinfo Address	This option is supported if the option value type is IP, ASCII, or HEX
netinfo-server-tag *string*	113	Netinfo Tag	This option is supported if the option value type is IP, ASCII, or HEX
default-url	114	URL	This option is supported if the option value type is IP, ASCII, or HEX
subnet-selection	118	Subnet Selection	Specifies the client preferred subnet for address assignment.
domain-search	119	Domain Search	Specifies a Domain Names search list used by the client to locate not-fully-qualified domain names.
vivso *string*	125	V-I VendorSpeciInfo	Specifies Vendor-Identified vendor specific information. Only the string value is accepted.
option *value*	126 - 127	Removed/ Unassigned	These options are supported if the option value type is IP, ASCII, or HEX
option *value*	128 - 135	PXE-VendorSpecific	These options are supported if the option value type is IP, ASCII, or HEX
option *value*	137	V4_LOST	Specifies the fully qualified domain name (FQDN) to be used by the client to locate a Location-to-Service Translation (LoST) server.
option *value*	141	SIP UA Domains	Specifies a list of domain names to search for Session Initiation Protocol (SIP) User Agent Configuration.

TABLE 6 DHCP Server Options (continued)

Option	Option Number	Option Name	Description / Notes
option *value*	142	IPv4-ANDSF	Specifies the IP addresses for Access Network Discover and Selection Function (ANDSF) Servers available to the client. The servers are listed in order of priority.
option *value*	146	RDNSS Selection	This option is supported if the option value type is IP, ASCII, or HEX
option *value*	147 - 148	Unassigned	These options are supported if theoption value type is IP, ASCII, or HEX
tftp-server-address	150	TFTP Server Addr	Specifies the address of the TFTP Server available to the client.
option *value*	156	dhcp-state	This option is supported if the option value type is IP, ASCII, or HEX
option *value*	160	Captive-Portal	This option is supported if the option value type is IP, ASCII, or HEX
option *value*	161 - 174	Unassigned	These options are supported if the option value type is IP, ASCII, or HEX
option *value*	175	Etherboot	This option is supported if the option value type is IP, ASCII, or HEX
option *value*	176	IP Tele-VoiceSrvr	Configures the IP telephone voice parameters for Avaya IP phones running as DHCP clients.
option *value*	177	PktCable-CableHome	This option is supported if the option value type is IP, ASCII, or HEX
option *value*	178 - 206	Unassigned	These options are supported if theoption value type is IP, ASCII, or HEX
option *value*	209	Config File	Specifies the configuration file to be used in a PXELINUX environment.
option *value*	210	Path Prefix	Specifies a path prefix for the configuration file used in a a PXELINUX environment.
option *value*	213	V4_ACCESS_DOMAIN	Specifies the access network domain name available to the client for the purposes of discovering a Local Information Server (LIS).
option *value*	214 - 218	Unassigned	These options are supported if the option value type is IP, ASCII, or HEX
option *value*	221	VSS	This option is supported if the option value type is IP, ASCII, or HEX
option *value*	222 - 223	Unassigned	These options are supported if the option value type is IP, ASCII, or HEX
option *value*	224 - 241	Reserved	These options are supported if the option value type is IP, ASCII, or HEX
option *value*	242	IP Tele-DataSrvr	Configures the IP telephone data parameters for Avaya IP phones running as DHCP clients.
option *value*	243 - 251	Reserved	These options are supported if the option value type is P, ASCII, or HEX
option *value*	252	WPAD	Configures the Proxy-Auto Config (PAC) file location string for the Web Proxy Auto-Discovery (WPAD) supported DHCP clients.
option *value*	253 - 254	Reserved	These options are supported if the option value type is IP, ASCII, or HEX

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.

Recommendations and Limitations

The list of supported DHCP options is extensive. However, the number of options that can be passed to the client is limited by the size of the ACK packet. It is recommended that you configure essential options only for the specific DHCP server address pool.

The following options (if configured) are prioritized, with additional options added as needed:

- 3 - Router Option
- 6 - Domain Name Server
- 12 - Hostname
- 15 - Domain name

- 66 - TFTP server hostname or IP address
- 67 - Boot file name
- 60 - Vendor-Specific Information

DHCP options are not validated by the DHCP server. You must ensure the values are configured correctly.

Upgrade Considerations

In FastIron 08.0.61 or earlier releases, it was possible to configure a subset of these DHCP options using specific commands. For example, **dhcp-default-router** allows configuration of the DHCP default router (which is now also configurable using DHCP option 3). When upgrading to FastIron 08.0.70, any configured DHCP options are retained. However, the configuration is stored and shown in the new options format. The following table shows the options available in earlier releases and a mapping between the new option format and the corresponding commands available in earlier releases.

Option Number and Name	Command in Release 08.0.70	Command in Release 08.0.61 and Earlier
1 - Subnet Mask	**network***router-IPsubnet mask* Note that this essential option is configured using the **network** command. It is not configurable using the option command.	**network***router-IPsubnet mask*
3 - Router Option	**option 3 ip***router -IP*	**dhcp-default-router***router -IP*
6 - Domain Name Server	**option 6 ip***server-IP-address*	**dns-server***server-IP-address*
12 - Hostname	**option 12 ascii***hostname*	**host-name***hostname*
15 - Domain name	**option 15 ascii***domain-name*	**domain-name***ascii-string-domain-name*
47 - NetBIOS over TCP/IP Name Server	**option 47 ip***Server-IP*	**netbios-name-server***Server-IP*
49 - X Window System Display Manager	**option 49 ip***XWindow-manager-IP*	**xwindow-manager***XWindow-manager-IP*
66 - TFTP server hostname	**option 66 ascii***TFTP-server-hostname*	**tftp-server***TFTP-server-hostname*
67 - Bootfile name	**option 67 ascii***bootfile-name*	**bootfile***bootfile-name*
150 - TFTP server IP address	**option 150 ip***TFTP-server-IP*	**tftp-server***TFTP-server-IP*
176 - ip-telephony voice server	**option 176 mcipadd***mcport,...*	**ip-telephony voice mcipadd***mcport,...*
242 - ip-telephony data server	**option 242 mcipadd***mcport,...*	**ip-telephony data mcipadd***mcport,...*
252 - Proxy-Auto Config (PAC)	**option 252 ascii***URL-to-config-file*	**wpad***URL-to-config-file*
60 - Vendor-Specific Information	**option 60 ascii***VCI*	**vendor-class***ascii-string-VCI*

Note that the existing commands are still supported. However, it is recommended that you configure these using the option command where appropriate. The configuration is stored and shown in the options format, irrespective of whether the option is configured using the option command or the commands available in previous releases.

When upgrading from any previous version to FastIron 09.0.00, the **deploy** and **ip dhcp-server relay-agent-echo enable** commands are not available and will not be seen in the running configuration after upgrade.

Follow the below process for the ISC options:

- If the option is of type ASCII string, convert the option value to ASCII string and change the option type to "ascii".
- If the option is of type Hex string, convert the option value to HEX string and change the option type to"hex".
- If the option is of type integer, convert the option value as ASCII to integer, if it is a valid integer value, and save the configuration as "option <option-num> integer <option-value>", or convert the option value as hex to integer, if it is a valid integer value, and save the config as "option <option-num> integer <option-value>", or ignore the option value if it is of type IP address.

- If the option is of type bool in 9000, convert the option value from ascii to integer, if it is a valid integer value and greater than zero, save the bool as true, if it is zero, and save the bool as false. Or, comvert the option value from hex to integer, if it is valid integer value and greater than zero, save the bool as true, if it is zero, then save the bool as false. Or, ignore the option value if it is of type IP address.
- If the option is of type IP address,check that the option supports the list of IPs or single IPs. If the list of IPs are supported, no change is required. If single IP is supported,save the first IP address and remove the other IP addresses. If the option is slp-service-scope, configure the bool flag as true always and save the option value as ASCII string. If the option is slp-directory-agent, configure the bool flag as true always, and save the IP addresses configured.
- For the policy-filter(21) options, delete the option type IP. If there are three IP addresses, remove the last IP address. In FastIron 09.0.00, option 21 accepts destination IP and subnet mask as a pair. This means that option 21 configured in previous releases are not applied when upgrading to FI 09.0.00.
- For the static-route(33) option, delete the option type IP from the command. If there are three IP addresses, remove the last IP address.

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 relay agent information support (option 82)

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 assignments, 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. When DHCP option 82 is enabled, a subscriber is identified by the physical port through which it connects to the network DHCP option 82 is enabled by default.

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)# option bootfile-name RDR10000_b277ufi.bin
```

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
```

Specifying the Default Router Available to the Client

Complete the following steps to specify the IP address of the default router 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 address of the default router for the client.

```
device(config-dhcp-cabo)# option routers 10.2.1.141
```

NOTE
Specify one default router IP address only. Do not enter multiple router addresses.

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. Specify the IP addresses of the DNS servers that are available to the DHCP clients.

```
device(config-dhcp-cabo)# option domain-name-servers 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 DHCP server pool configuration mode.

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

3. Specify the domain name for the client.

   ```
   device(config-dhcp-cabo)# option 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 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.

Configuring the Number of Leases for the Address Pool

The number of lease IP addresses used for the DHCP address pool can be configured.

Memory is allocated based on the number of leases configured on the switch. The switch allocates the memory for the first 3000 leases. Any configured leases on the remaining address pools are then removed from the configuration.

NOTE
A maximum of 3000 leases can be configured. When 3000 leases are allocated, the configuration under any remaining pools is removed from the configuration.

NOTE
If more than 3000 leases are configured, the following error is displayed while rebooting: *Error: exceeds maximum 3000 leases*.

NOTE
After upgrading to FastIron 09.0.10a, it is recommended to re-configure the DHCP server address pool, and to configure the lease count with the number of leases specific to the address pool.

Complete the following steps to configure the number of lease IP addresses used for 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. Configure the number of lease IP addresses.

```
device(config-dhcp-cabo)# lease-count 2500
```

The following example sets the number of lease IP addresses used for the DHCP address pool to 2500.

```
device# configure terminal
device(config)# ip dhcp-server-pool cabo
device(config-dhcp-cabo)# lease-count 2500
```

Specifying addresses to exclude from the address pool

Complete the following steps to specify the 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)# option netbios-scope 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)# option network 10.1.1.0/24
```

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.

```
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)# option tftp-server-address 10.7.5.48
device(config-dhcp-cabo)# option tftp-server-name 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 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)# option x-display-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)# option x-display-manager 10.38.12.1 10.38.12.3 10.38.12.5
```

Vendor-specific Information (Option 43 and Option 60) Configurations

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

Configuring 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).

Option 60 defines the vendor type and configuration, while option 43 defines the vendor-specific information (VSI). If option 60 is configured, the VSI (defined in option 43) is returned to clients that provide the appropriate vendor type and configuration value. If option 60 is not configured, the VSI is sent to all clients.

Configuring Vendor Details and Vendor Specific Information (Option 43 and Option 60)

RUCKUS ICX switches running as DHCP servers can be configured with option 43 and option 60.

Complete the following steps to configure option 60 and option 43 for a device running as a DHCP server.

1. Enter global configuration mode.

```
device# configure terminal
```

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. Use the **option 60** command to specify the vendor type and configuration value for the DHCP client.

```
device(ip dhcp-server pool ruckus)# option vendor-class-identifier ascii "Ruckus CPE"
```

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

4. Use the **option 43** command to specify the vendor-specific information.

NOTE
Choose the appropriate syntax from the following options:

- **option vendor-encapsulated-options ascii** *ascii-string*
- **option vendor-encapsulated-options hex** *hex-string*
- **option vendor-encapsulated-options ip** *ip-address*

A single IP address or a series of comma-separated IP addresses may be entered after the **ip** keyword.

```
device(ip dhcp-server pool ruckus)# option vendor-encapsulated-options hex 0108c0a80a01c0a81401
```

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)# option vendor-class-identifier ascii "Ruckus CPE"
device(ip dhcp-server pool ruckus)# option vendor-encapsulated-options ascii ruckusconfig
```

The following example configures option 43, using the **ip** option and specifying the SmartZone IP addresses.

```
device# configure terminal
device(config)# ip dhcp-server pool ruckus
device(ip dhcp-server pool ruckus)# option vendor-encapsulated-options ip 0710.10.10.1,11.11.11.10
```

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
```

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
```

Enabling IP to Physical Port Mapping

You can reserve IP addresses within a DHCP address pool against selected Ethernet ports. This allows any device connecting to the selected port on the switch to obtain the same IP address irrespective of the client identifier sent by the device. This configuration is useful in preventing a newly connected device on a port from getting a new IP address.

This option works by replacing the DHCP client identifier (option 61) sent by the DHCP client with an auto-generated port name. The port name is derived from the configured port number in the DHCP address pool.

The following limitations must be considered when using this option:

- This option should be used only when the ICX switch is being used as an Edge device.
- Only one IP address is allowed to be reserved for a selected port.
- This option should be used only when a single device is expected to be connected on the selected port. Any additional devices connected to the same port using a hub or a downstream switch will result in all the devices getting assigned the same IP address.
- Static port to IP mapping is not available on tagged ports, nor on virtual interfaces including VEs, LAGs and loopback interfaces. Only untagged ports are supported.
- This option works only when the client Identifier used is Ethernet type; it does not work if a string type is used as the client identifier.

  NOTE
  To achieve better scaling performance, disable the feature explicitly for an interface if a burst of DHCP client traffic is expected on a single interface. If the feature is not explicitly disabled for the interface, some of the DHCP clients may not be assigned an IP address and may need to send the request again. Similar behavior may be seen during the release of IP addresses also.

Use the following procedure to configure static port to IP mapping in a DHCP address pool.

1. Enter global configuration mode.

   ```
   device# configure terminal
   ```

2. Enter interface configuration mode.

   ```
   device# interface ethernet 1/1/8
   ```

3. Enable the replacement of the DHCP client identifier (option 61) with the port name for the Interface.

   ```
   device(config-if-e1000-1/1/8)# ip dhcp-server use-port-name enable
   ```

4. Return to global configuration mode.

   ```
   device(config-if-e1000-1/1/8)# exit
   ```

5. Create a DHCP server pool.

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

6. Configure the DHCP server address pool.

   ```
   device(config-dhcp-list)# network 10.10.10.0 255.255.255.0
   device(config-dhcp-list)# lease-count 254
   device(config-dhcp-list)# lease 1 0 0
   ```

7. Map an Ethernet interface to the IP address.

   ```
   device(config-dhcp-list)# static-port-ip-mapping 10.10.10.2 e1/1/3
   ```

The following example shows a configured static port to IP mapping.

```
device# configure terminal
device(config)# interface ethernet 1/1/8
device(config-if-e1000-1/1/8)# ip dhcp-server use-port-name enable
device(config-if-e1000-1/1/8)# exit
device(config)# ip dhcp-server pool list
device(config-dhcp-list)# network 10.10.10.0 255.255.255.0
device(config-dhcp-list)# lease-count 254
device(config-dhcp-list)# lease 1 0 0
device(config-dhcp-list)# static-port-ip-mapping 10.10.10.2 e1/1/3
```

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.

The following table lists the parameters for each option:

Option	Paramaters
Option 176: Voice server options	**mcipadd** *ip-address* Specifies the IP telephony server port number. The default is 1719. **mcport** *portnum* Specifies the IP telephony server port number. The default is 1719. **tftpsrvr/httpsrvr/tlssrvr** *server-ip-address* Specifies the IP addresses of the TFTP, HTTP, and TLS servers. **l2qaud or l2qsig** *prio* Specifies the IP telephony L2QAUD or L2QSIG priority value. The range is from 1 to 6. The default value is 6. **l2qvlan** *vlan-id* Specifies the IP telephony L2QVLAN number. The default is 0. **vlantest** *secs* The number of seconds a phone attempts to return to the previously known voice VLAN. This is not applicable for the default VLAN.

Option	Paramaters
Option 242: Data server options	**mcipadd** *ip-address* IP address of the gatekeeper. Atleast one IP address is required. **mcport** *portnum* Specifies IP telephony server port number. The default is 1719. **tftpsrvr/httpsrvr/tlssrvr** *server ip-address* Specifies the IP addresses of the TFP, HTTP, and TLS servers. **l2qaud or l2qsig** *prio* L2QAUD is the IP telephony L2 audio priority value. L2QSIG is the IP telephony L2 signaling priority value. This range is from 1 through 6. The default value is 6. **l2qvlan** *vlan-id* Specifies the IP telephony L2QVLAN number. The default is 0. **vlantest** *secs* The number of seconds a phone attempts to return to the previously known voice VLAN. This is not applicable for the default VLAN.

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 **option** 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)# option 242 mcipadd 1.1.1.2 mcport 1719
```

4. Enter the **option** 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)# option 176 mcipadd 1.1.1.2 mcport 1719
```

5. Enter the **show ip dhcp-server address-pools** command to view and verify the IP telephony options.

```
device(config)# 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  60 (Vendor Class Id   ):  hex FF
option 176 (IP Tele-VoiceSrvr ):  MCIPADD=10.10.10.1,MCPORT=1719
option 242 (IP Tele-DataSrvr  ):  MCIPADD=10.10.10.1,MCPORT=1719
```

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 **option** command followed by the full network location of the PAC file.

```
device(config-dhcp-cabo)# option 252 ascii 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
                      network:  50.50.50.0 255.255.255.0
        option 252 (WPAD    ):  http://172.26.67.243:8080/wpad.dat
```

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 address-pools: 1
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 icx7650-20-qxg-port-management-module
module 2 icx7650-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 67
- Dynamic ARP Inspection Overview 67
- DHCP Snooping 73
- DHCP Relay Agent Information and Option 82 Insertion 80
- IP Source Guard 88

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.

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 (MITM) 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 completes the following tasks:

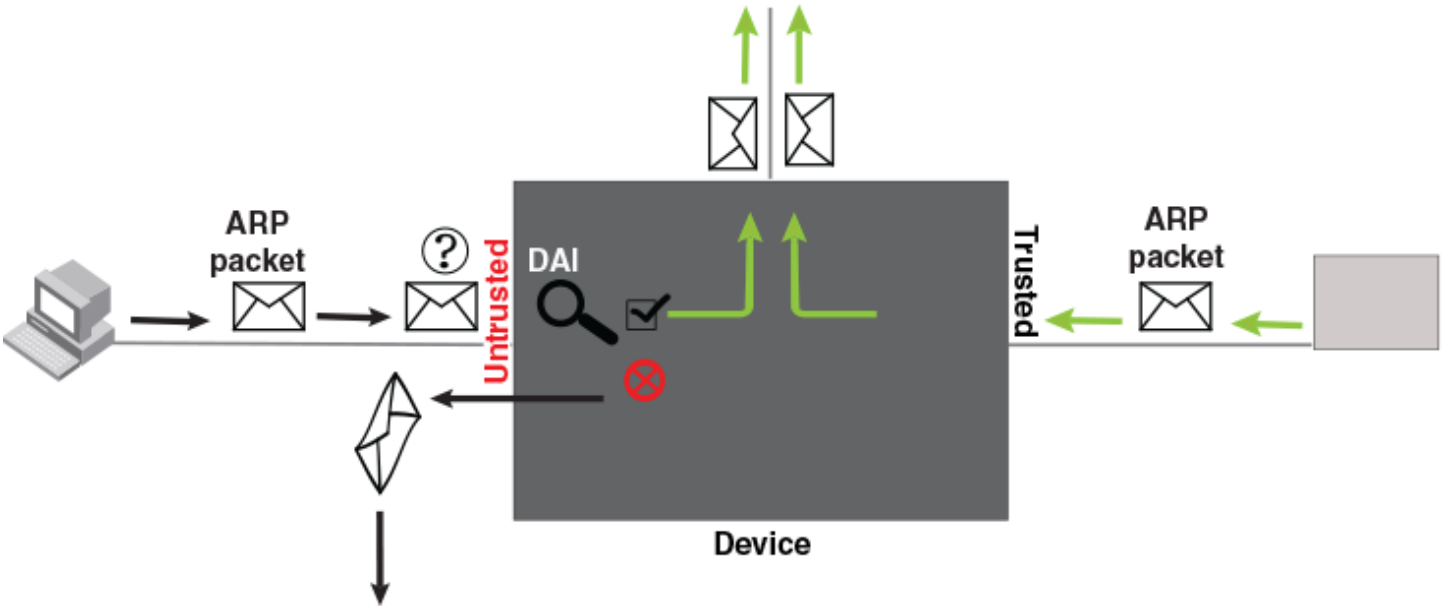
- Intercepts ARP packets received by the system CPU
- Inspects all ARP requests and responses received on untrusted ports
- Verifies that each of the intercepted packets has a valid IP-to-MAC address binding before updating the local ARP table, or before forwarding the packet to the appropriate destination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

- 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 75.

Configuration Notes and Feature Limitations for DAI

The following configuration notes and limitations apply when configuring Dynamic ARP Inspection (DAI):

- The maximum number of static DAI entries that can be configured is 6000. This value cannot be changed.
- DAI can be configured on a maximum of 511 VLANs.
- 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.
- For default VLAN ID changes, DAI must be re-applied on the new default VLAN.
- ACLs are supported on member ports of a VLAN on which DHCP snooping and Dynamic ARP Inspection (DAI) are enabled.
- When a device receives the ARP packet with source 0.0.0.0, "allow source ip 0.0.0.0" is used to allow the packet when DAI is enabled.

Configuring Dynamic ARP Inspection

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

You must first configure static ARP or ARP inspection entry for hosts configured with a static IP address. 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.

Complete the following steps to configure DAI.

1. Enter global configuration mode.

   ```
   device# configure terminal
   ```

2. (Optional) Configure an ARP inspection entry only if there are hosts configured with a static IP address.

   ```
   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.

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

3. 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 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.

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

```
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
```

Configuring Dynamic ARP Inspection on Multiple VLANs

Dynamic ARP Inspection (DAI) can be enabled on multiple VLANs using one command. The following task configures multiple VLANs and enables DAI on most of the configured VLANs using a single command.

Complete the following steps to configure DAI for multiple VLANs.

NOTE
DAI can be configured on a maximum of 511 VLANs.

1. Enter global configuration mode.

```
device# configure terminal
```

2. Configure the port-based VLANs.

```
device(config)# vlan 100 to 150
```

3. Add port Ethernet 1/1/12 as a tagged port.

```
device(config-mvlan-100-150)# tagged ethernet 1/1/12
```

4. Use the **exit** command to return to global configuration mode.

```
device(config-mvlan-100-150)# exit
```

5. Configure more port-based VLANs.

```
device(config)# vlan 151 to 200
```

6. Add port Ethernet 1/1/12 as a tagged port.

```
device(config-mvlan-151-200)# tagged ethernet 1/1/12
```

7. Use the **exit** command to return to global configuration mode.

```
device(config-mvlan-151-200)# exit
```

8. Use the **ip arp inspection** command with the **to** keyword, specifying a VLAN range, to enable DAI on multiple VLANs.

```
device(config)# ip arp inspection vlan 100 to 150 160 170 to 200
```

   The command enables DAI on VLANs 100 through 150, VLAN 160, and VLANs 170 through 200. ARP packets from untrusted ports in this VLAN range will undergo DAI.

   NOTE
   The maximum number of VLANS that can be configured using the **to** keyword is 1024.

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

```
device(config)# interface ethernet 1/1/12
```

   b) Enable trust on the port.

```
device(config-if-e10000-1/1/12)# arp inspection trust
```

10. Enable DHCP snooping to populate the DHCP snooping IP-to-MAC address binding database. Refer to the *RUCKUS FastIron DHCP Configuration Guide* for more information.

The following example configures a DAI table entry, configures multiple VLANs, and enables DAI on most of the configured VLANS. Port 1/1/12 is designated as trusted.

```
device# configure terminal
device(config)# arp 10.20.20.12 0000.0002.0003 inspection
device(config)# vlan 100 to 150
device(config-mvlan-100-150)# tagged ethernet 1/1/12
device(config-mvlan-100-150)# exit
device(config)# vlan 151 to 200
device(config-mvlan-151-200)# tagged ethernet 1/1/12
device(config-mvlan-100-150)# exit
device(config)# ip arp inspection vlan 100 to 150 160 170 to 200
device(config)# interface ethernet 1/1/12
device(config-if-e10000-1/1/12)# arp inspection trust
```

Disabling Syslog Messages for DAI

You can disable syslog messages for Dynamic ARP Inspection (DAI). Syslog messages are enabled by default on RUCKUS ICX devices.

Complete the following steps to disable DAI messages.

1. Enter global configuration mode.

```
device# configure terminal
```

2. Enter the following command to disable syslog messages.

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

   If you want to re-enable DAI syslog messages, use the **no** form of the command.

The following example disables DAI syslog messages.

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

The following example re-enables the DAI syslog messages.

```
device# configure terminal
device(config)# no 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
```

2. Display the ARP inspection entries.

```
device> show ip arp inspection entries

Total entries               : 2
DHCP Snooping Learnt entries: 1
ARP Learnt entries          : 1
Static entries              : 0
     IP Address      Mac Address    VRF                          Entry Type
     10.177.144.1    02e0.52da.d665 default-vrf                  arp table entry
     1.1.8.197       00c1.0400.0001 default-vrf                  dhcp snoop entry
```

Configuring DAI to Support Multi-VRF

DAI supports Multi-VRF. You can deploy multiple Virtual Routing and Forwarding instances (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 using the **configure terminal** command.

```
device# configure terminal
```

2. Configure DAI on a VLAN.

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

   This example configures DAI on VLAN 2.

3. Add a static ARP inspection entry for a specific VRF.

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

4. 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 using the **configure terminal** command.

```
device# configure terminal
```

2. Enter interface configuration mode.

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

3. Enable **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 man-in-the-middle (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 (DAI) and IP Source Guard (IPSG).

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 7 DHCP Snooping at Work on an Untrusted Port

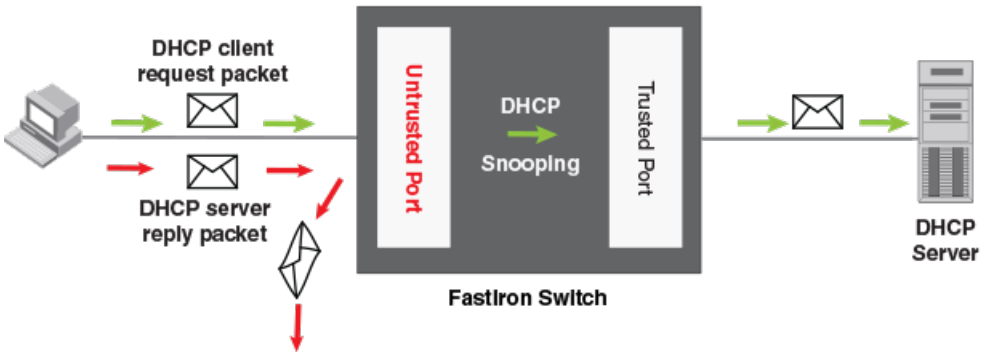
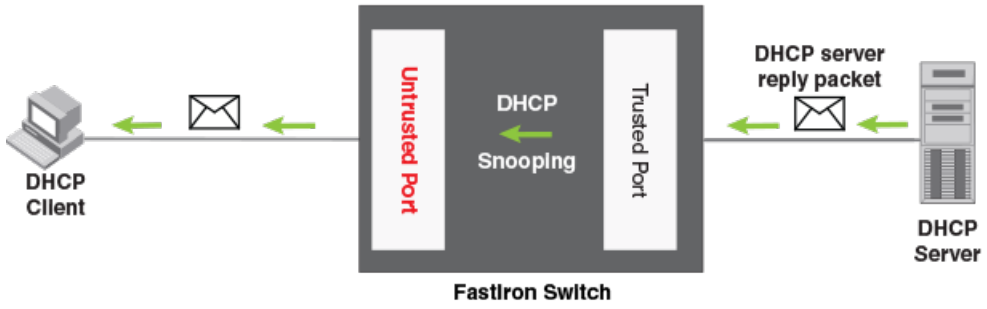


FIGURE 8 DHCP Snooping at Work on a Trusted Port

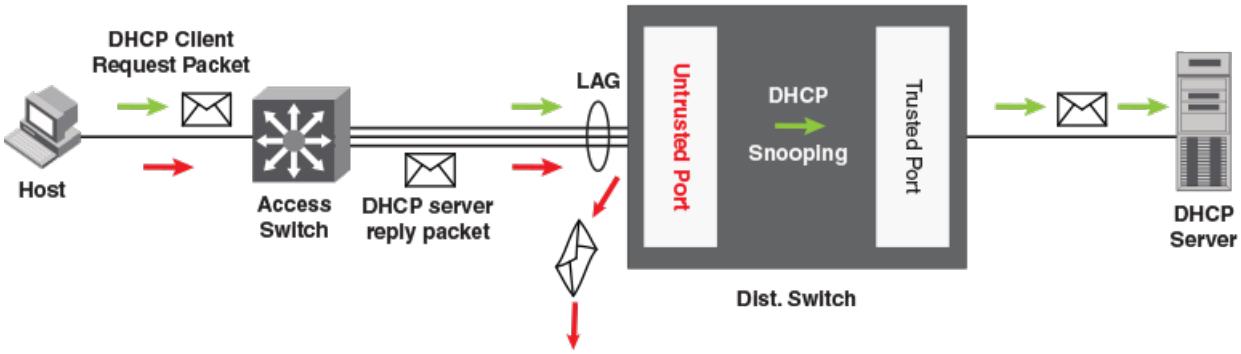


NOTE
Trusted client ports can lead to DHCP starvation and spoofing attacks. When DHCP snooping is enabled, DHCP request packets received on trusted ports are dropped.

DHCP Snooping Deployment over a LAG

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

FIGURE 9 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 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 68.

The lease time is refreshed when the client renews or rebinds 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.

System Reboot and the Binding Database

To allow DHCP snooping, and all dependent features such as IP Source Guard (IPSG) and Dynamic ARP Inspection (DAI), to work smoothly across a system reboot, the binding database is saved to a file system inline without any delay.

Configuration Notes and Feature Limitations for DHCP Snooping

The following notes, limitations, and restrictions apply to DHCP snooping:

- DHCP snooping is supported on LAG ports. If a LAG port is removed or undeployed, DHCP snooping entries for that LAG are deleted.
- DHCP snooping is supported on Multi-Chassis. Trunking (MCT) clients. DHCP snooping is not supported on the MCT peer for the MCT VLAN.
- If IP Source Guard (IPSG) is configured, the recommended maximum number of DHCP snooping entries for a stack is 8192. Although the maximum number of DHCP snooping entries for a stack can exceed 8192, system performance may go down once this number is exceeded. Refer to Configuration Notes and Feature Limitations for IP Source Guard on page 89 for more information on the recommended number of entries for RUCKUS ICX devices.
- DHCP snooping is not supported along with DHCP auto-configuration.
- When a client moves from one port to another port in the same VLAN, the old snoop entry for the client MAC address is automatically updated. This occurs even when the client acquires a new IP address. In previous releases, two snoop entries were maintained with both the old IP address and the new IP address.
- Duplicate IP entries across VLANs are allowed in the DHCP snooping table. When a client moves from one VLAN to another and acquires the same address, two snooping entries are maintained for the same MAC address and IP address.
- Layer 2 MAC movement is supported.
- 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 74 for more information. In previous releases, these were mutually exclusive.
- DHCP snooping supports DHCP relay agent information (DHCP option 82). Refer to DHCP Relay Agent Information and Option 82 Insertion on page 80 for more information.
- For default VLAN ID changes, DHCP snooping must be re-applied on the new default VLAN. DHCP snooping is not automatically configured on the new default VLAN. Therefore, when DHCP Snooping is configured for the default VLAN (for example, VLAN 1), if the default VLAN is changed from VLAN 1 to VLAN 4000, the DHCP Snooping configurations remain configured on the old default VLAN 1. The DHCP Snooping configurations are not automatically configured on the new default VLAN 4000. In previous releases, DHCP Snooping configurations were automatically removed from the old default VLAN and automatically moved to the new default VLAN.
- DHCP snooping cannot be enabled for a VLAN that is a member of a VLAN group.
- DHCP snooping doesn't depend on MAC learning and MAC collisions. However, the total number of client(s) or host(s) in a system is limited by the system MAX limits for Layer 2 MAC Addresses.
- DHCP snooping entries learnt on a member port of a VLAN are deleted except for flexible authentication enabled ports, if the port is removed from the membership of that VLAN.
- DHCP Snooping can be configured for a VLAN or VLANS even before the VLAN or VLANS are created. VLANs and DHCP Snooping configurations on the VLANS are not automatically deleted when the VLAN is deleted.
- When DHCP Snooping is enabled, client and server packets are not allowed on same port.
- DHCP snooping can be configured on a maximum of 511 VLANs.
- When configuring DHCP snooping on a range of VLANs or multi-VLAN, there cannot not be any VLAN in the range that is a member of a VLAN group or any reserved VLAN. Otherwise, onfiguration will be rejected for the entire range.
- The following limitation applies to ICX 8200 devices. To support DHCP snooping for Flexible authentication clients in multiple untagged mode, DHCP snooping should also be enabled on the Flexible authentication auth-default VLAN.

Example Flexible authentication configuration:

```
ICX8200-48P Router# configure terminal
ICX8200-48P Router(config)# authentication
ICX8200-48P Router(config-authen)# auth-default-vlan 12
ICX8200-48P Router(config-authen)# auth-mode multiple-untagged
ICX8200-48P Router(config-authen)# exit
```

Example DHCP configuration:

```
ICX8200-48P Router(config)# ip dhcp snooping vlan 12
```

Configuring DHCP Snooping

DHCP snooping can 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.

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

NOTE
DHCP Snooping can be configured for a VLAN or VLANS even before the VLAN or VLANS are created. VLANs and DHCP Snooping configurations on the VLANS are not automatically deleted when the VLAN is deleted.

1. Enter global configuration mode by using 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 enables DHCP snooping on the two VLANs.

```
device(config)# vlan 2
device(config-vlan-2)# untagged ethernet 1/1/3 to 1/1/4
device(config-vlan-2)# interface ve 2
device(config-vlan-2)# exit
device(config)# ip dhcp snooping vlan 2
device(config)# vlan 20
device(config-vlan-20)# untagged ethernet 1/1/1 to 1/1/2
device(config-vlan-20)# 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. Therefore, 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 address and MAC address 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
```

Configuring DHCP Snooping on Multiple VLANs

DHCP snooping can be enabled on multiple VLANs using one command. The following task configures multiple VLANs and enables DHCP snooping on most of the configured VLANs using a single command.

NOTE
DHCP snooping can be configured on a maximum number of 511 VLANs at one time.

NOTE
DHCP Snooping can be configured for a VLAN or VLANS even before the VLAN or VLANS are created. VLANs and DHCP Snooping configurations on the VLANS are not automatically deleted when the VLAN is deleted.

NOTE
When configuring DHCP snooping on a range of VLANs or multi-VLAN, there cannot not be any VLAN in the range that is a member of a VLAN group or any reserved VLAN. Otherwise, configurations fail on the entire range.

1. Enter global configuration mode.

   ```
   device# configure terminal
   ```

2. Configure the port-based VLANs.

   ```
   device(config)# vlan 100 to 150
   ```

3. Add port Ethernet 1/1/12 as a tagged port.

   ```
   device(config-mvlan-100-150)# tagged ethernet 1/1/12
   ```

4. Use the **exit** command to return to global configuration mode.

```
device(config-mvlan-100-150)# exit
```

5. Configure more port-based VLANs.

```
device(config)# vlan 151 to 200
```

6. Add port Ethernet 1/1/12 as a tagged port.

```
device(config-mvlan-151-200)# tagged ethernet 1/1/12
```

7. Use the **exit** command to return to global configuration mode.

```
device(config-mvlan-151-200)# exit
```

8. Use the **ip dhcp snooping** command with the **to** keyword, specifying a VLAN range, to enable DHCP snooping on multiple VLANs.

```
device(config)# ip dhcp snooping vlan 100 to 150 160 170 to 200
```

9. Change the trust setting of the ports that are connected to the DHCP server to trusted at the interface configuration level.
   a) To enable trust on a port, enter interface configuration mode.

```
device(config)# interface ethernet 1/1/12
```

   b) Enable trust on the port.

```
device(config-if-e10000-1/1/12)# dhcp snooping trust
```

The following example configures VLANs 100 through 200, and enables DHCP snooping on VLANs 100 through 150, VLAN 160, and VLANs 170 through 200.

```
device# configure terminal
device(config)# vlan 100 to 150
device(config-mvlan-100-150)# tagged ethernet 1/1/12
device(config-mvlan-100-150)# exit
device(config)# vlan 151 to 200
device(config-mvlan-151-200)# tagged ethernet 1/1/12
device(config-mvlan-100-150)# exit
device(config)# ip dhcp snooping vlan 100 to 150 160 170 to 200
device(config)# interface ethernet 1/1/12
device(config-if-e10000-1/1/12)# dhcp snooping trust
```

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 learned entries.

```
device> show ip dhcp snooping info

Dhcp snooping Info
Total Learnt Entries 1
Learnt DHCP Snoop Entries
     IP Address      Mac Address    Port/Lag     Vlan     lease      VRF
     1.1.0.4         00c7.0400.0001 1/2/4        1        3597       default-vrf
     …
```

2. 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
```

3. Display the DHCP snooping binding database.

```
device> show ip dhcp snooping

IP DHCP snooping enabled on 24 VLAN(s):
        VLAN(s): 1001 to 1024
```

Configuring DHCPv4 Snooping for Multi-VRF

DHCP supports Multi-VRF. You can deploy multiple Virtual Routing and Forwarding instances (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 using the **configure terminal** command.

```
device# configure terminal
```

2. Configure DHCP snooping on a specific VLAN.

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

3. 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)# 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.

4. 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.

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

```
device(config)# clear dhcp 10.3.3.5 vrf one
```

Enabling DHCP Snooping MAC Address Verification

The DHCP malformed packet coming from the client is blocked when DHCP snooping is enabled along with "ip dhcp snooping verify mac-address" MAC address verification command.

The MAC address verification command works only when DHCP snooping is enabled on the device.

Limitation: DHCP client and DHCP snooping device are connected on either sides of a relay. Source MAC address in the DHCP DISCOVER or DHCP REQUESTpacket will be the MAC address of the relay and the client hardware MAC address will be the MACaddress of the client. You must disable MAC address verification for the IP acquisition by the client to work properly.

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

```
device# configure terminal
```

2. Enable MAC address verification.

```
device(config)# ip dhcp snooping verify mac-address
```

NOTE
DHCP snooping MAC address verification is disabled by default.

3. (Optional) Disable DHCP snooping MAC address verification.

```
device(config)# no ip dhcp snooping verify mac-address
```

```
device# configure terminal
device(config)# ip dhcp snooping verify mac-address
```

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.

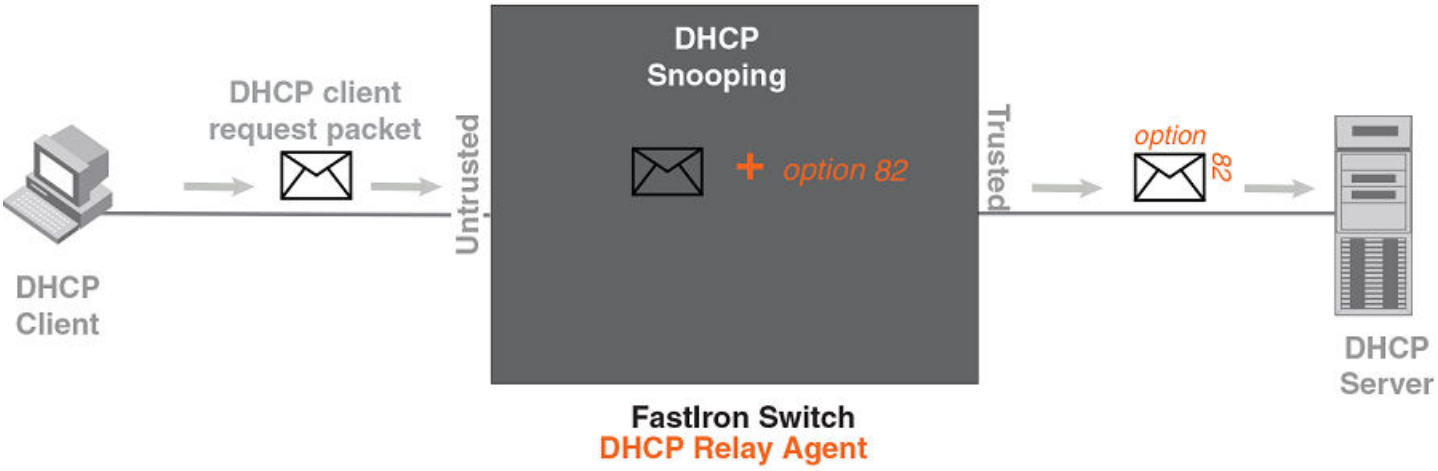
The RUCKUS device inserts DHCP option 82 when relaying DHCP request packets to DHCP servers. When DHCP server reply packets are forwarded back to DHCP clients, and sub-option 2 as as Remote ID (RID) matches the local port MAC address, then DHCP option 82 is deleted. The VLAN and port information is used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

DHCP packets use the following process:

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

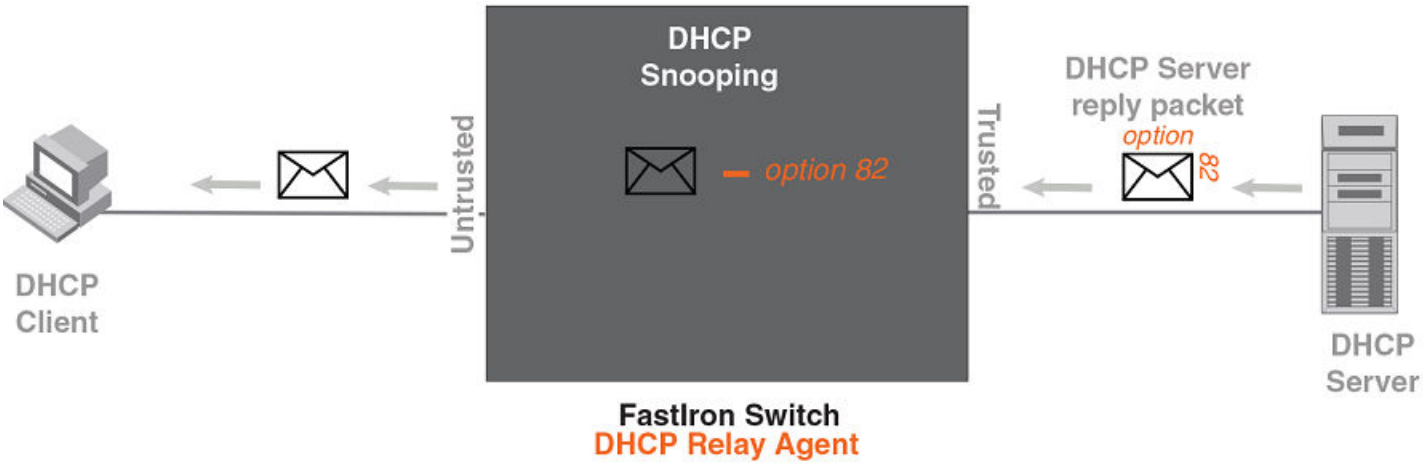
The DHCP relay agent (the FastIron switch) inserts DHCP option 82 attributes when relaying a DHCP request packet to a DHCP server.

FIGURE 10 DHCP Option 82 Attributes Added to the DHCP Packet



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

FIGURE 11 DHCP Option 82 Attributes Removed from the DHCP Packet



DHCP option 82 insertion or deletion 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 75.
- Option-82 can be disabled or re-enabled on multiple VLANs or a range of VLANS using a single command, ip dhcp snooping relay information disable.

DHCP Option 82 Sub-options

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

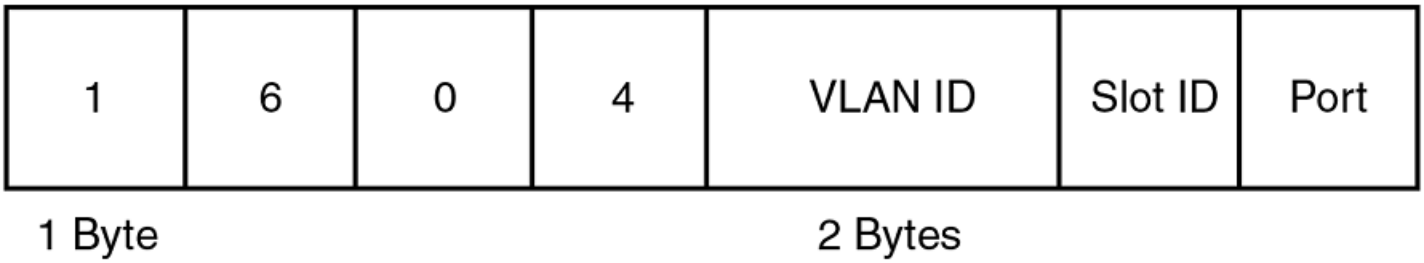
- Sub-option 1: Circuit ID
- Sub-option 2: Remote ID
- Sub-option 6: Subscriber ID

Sub-option 1: Circuit ID

The Circuit ID (CID) identifies the circuit or port from which a DHCP client request was sent. The ICX 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 ICX 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.

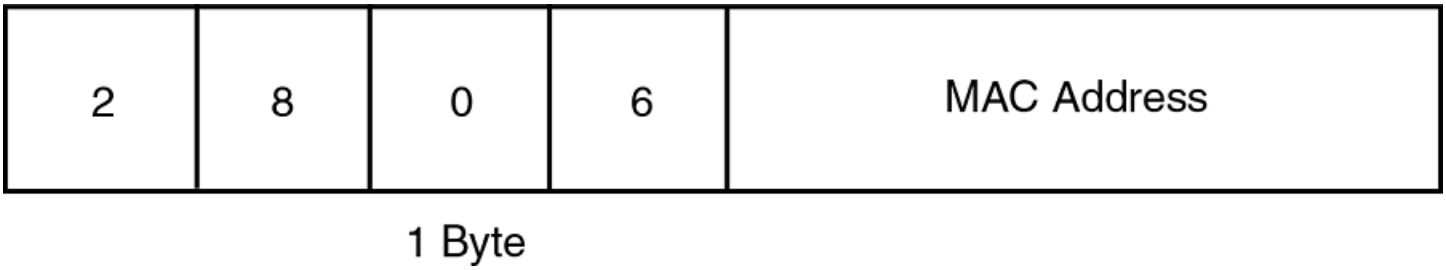
FIGURE 12 General CID Packet Format



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 13 RID Packet Format



Sub-option 6: Subscriber ID

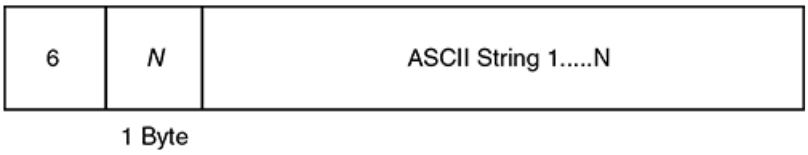
The Subscriber ID (SID) is a unique identification number that enables an Internet Service Provider (ISP) to perform the following actions:

- Identify a subscriber
- Assign specific attributes to that subscriber (for example, host IP address, subnet mask, and domain name server.

- Trigger accounting

The following figure illustrates the SID packet format.

FIGURE 14 SID Packet Format



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

DHCP Option 82 Configuration

DHCP option 82 is automatically 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 76 to enable DHCP snooping.

When processing DHCP packets, the ICX device 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, on all ports of the VLAN, or globally on all VLANs.
- Configure the device to drop the DHCP packet with existing relay agent Information, 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.

The following table details the supported configuration and expected functionality for DHCP option 82.

TABLE 7 DHCP Option 82 Supported Configuration

Configuration	Port-Config	VLAN-Config	Global-Config	Functionality
Default.	Enable	Enable	Enable	Option 82 enabled
Disabled globally.	Disable	Disable	Disable	Option 82 disabled
Disabled globally, enabled on port.	Enable	Enable	Disable	Option 82 enabled
Disabled globally, enabled on port, disabled on VLAN.	Enable	Disable	Disable	Option 82 enabled
Enabled globally, enabled on port, disabled on VLAN.	Enable	Disable	Enable	Option 82 disabled
Enabled globally, disabled on port, disabled on VLAN.	Disable	Disable	Enable	Option 82 disabled
Enabled globally, disabled on port, enabled on VLAN.	Disable	Enable	Enable	Option 82 disabled

TABLE 7 DHCP Option 82 Supported Configuration (continued)

Configuration	Port-Config	VLAN-Config	Global-Config	Functionality
Disabled globally, disabled on port, disabled on VLAN.	Disable	Disable	Disable	Option 82 disabled

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.

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

1. To disable DHCP option 82, enter global configuration mode by using 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
```

Disabling DHCP Option 82 Globally and Re-enabling It for 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 globally for all VLANs. The following task disables DHCP option 82 globally for all VLANs so that it is not enabled when DHCP snooping is configured for VLAN 100. It then re-enables DHCP option 82 for a specified Ethernet interface.

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

1. Enter global configuration mode.

```
device# configure terminal
```

2. Use the **ip dhcp snooping relay information disable** command to disable DHCP option 82 globally for all ports and VLANs.

```
device(config)# ip dhcp snooping relay information disable
```

3. Use the **ip dhcp snooping** command and specify a VLAN to configure DHCP snooping for the VLAN.

```
device(config)# ip dhcp snooping vlan 100
```

   DHCP option 82 is not enabled when DHCP snooping is configured for VLAN 100.

4. Enter interface configuration mode.

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

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

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

The following example disables DHCP option 82 globally for all ports and VLANs so that it is not enabled when DHCP snooping is configured for VLAN 100.

```
device# configure terminal
device(config)# ip dhcp snooping relay information disable
device(config)# ip dhcp snooping vlan 100
```

The following example disables DHCP option 82 globally for all ports and VLANS, and re-enables it for interface Ethernet 1/1/1.

```
device# configure terminal
device(config)# ip dhcp snooping relay information disable
device(config)# ip dhcp snooping vlan 100
device(config)# interface ethernet 1/1/1
device(config-if-e1000-1/1/1)# dhcp snooping relay information
```

The following example disables DHCP option 82 for VLAN 100 after it was automatically enabled when DHCP snooping was configured for VLANs 100, 200, and 300.

```
device# configure terminal
device(config)# ip dhcp snooping vlan 100 to vlan 300
device(config)# ip dhcp snooping relay information disable vlan 100
```

Disabling or Re-enabling DHCP Option 82 Processing on all VLAN Member Ports

You can disable or re-enable DHCP option 82 processing globally, and disable and re-enable as necessary on specified VLANs. The following task disables DHCP option 82 globally. IP DHCP snooping is then enabled for VLANs 100, 200, and 300, but DHCP option 82 is not automatically enabled because it has been disabled globally. DHCP option 82 is then re-enabled on all ports for VLAN 100.

1. Enter global configuration mode.

```
device# configure terminal
```

2. Use the **ip dhcp snooping relay information disable** command to disable DHCP option 82 globally for all VLANs.

```
device(config)# ip dhcp snooping relay information disable
```

3. Use the **ip dhcp snooping** command, specifying VLANs as required, to configure DHCP snooping for the specified VLANs.

```
device(config)# ip dhcp snooping vlan 100 to 300
```

4. Enable DHCP option 82 on all ports for VLAN 100.

```
device(config)# no ip dhcp snooping relay information disable vlan 100
```

The following example disables DHCP option 82 globally and enables IP DHCP snooping for VLANs 100 through 300. DHCP option 82 is then disabled on all ports for VLAN 100.

```
device# configure terminal
device(config)# ip dhcp snooping relay information disable
device(config)# ip dhcp snooping vlan 100 to 300
device(config)# no ip dhcp snooping relay information disable vlan 100
```

The following example automatically enables DHCP option 82 for VLANs 100, 200, and 300. It then disables DHCP option 82 globally for all ports on VLAN 100.

```
device# configure terminal
device(config)# ip dhcp snooping vlan 100 to 300
device(config)# ip dhcp snooping relay information disable vlan 100
```

The following example disables DHCP option 82 globally for all VLANs and ports.

```
device# configure terminal
device(config)# ip dhcp snooping vlan 100 to 300
device(config)# ip dhcp snooping relay information disable
Warning - DHCP snooping relay information will be disabled on all port(s) & VLAN(s). You can enable it on
individual ports/VLAN(s)
device(config)#
```

The following example disables DHCP option 82 globally for all ports and VLANs and re-enables it for VLAN 100.

```
device# configure terminal
device(config)# ip dhcp snooping vlan 100 to 500
device(config)# ip dhcp snooping relay information disable
Warning - DHCP snooping relay information will be disabled on all port(s) & VLAN(s). You can enable it on
individual ports/VLAN(s)
device(config)# no ip dhcp snooping relay information disable vlan 100
```

The following example enables DHCP option 82 for a specified range of VLANs.

```
device# configure terminal
device(config)# ip dhcp snooping relay information disable vlan 11 to 15
```

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 using 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 DHCP packet with existing relay agent Information.

```
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 Subscriber ID (SID), Circuit ID (CID) or Remote ID (RID) 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, 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(config)# show ip dhcp relay information

Relay Agent Information: format: Circuit-ID: vlan-port
                                 Remote-ID : stack mac
                                 Policy    : replace
```

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 that DHCP option 82 is enabled on the device and the configured Subscriber ID is 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

You can enable 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 (IPSG) together with Dynamic ARP Inspection (DAI) on untrusted ports.

The RUCKUS implementation of the IPSG technology supports configuration on a port and specific VLAN memberships on a port.

When IPSG 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, an access-list with a permit filter for the IP address is added or deleted. By default, if IPSG 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):

- Configuring IPSG static entries at the VLAN or port level is allowed only after IPSG is configured at the VLAN level, at the port level, or both.
- IPSG configuration can be removed at the VLAN or port level only after all IPSG static entries are unconfigured at the VLAN or port level.
- IPSG is supported on LAGs.
- If you change the default VLAN ID when IPSG is enabled on a LAG, then IPSG is not inherited. All IPSG configuration is lost for the VLAN if the default VLAN ID is changed.
- IPSG functions across reload.
- RUCKUS ICX devices do not support IPSG and user ACLs on the same port.
- RUCKUS devices do not support IPSG with ingress IPv4 ACLs for the same port, neither at VLAN-level, port-level, or across different levels. For ports with IPSG enabled, a special ingress IPv4 ACL viz SGACL has been introduced. Therefore, IPSG and SG ACL can be configured for the same port.
- When IPSG is enabled for a LAG at the VLAN-level or VLAG-interface-level, IPSG entries learned on the LAG ports remain intact if the non-last member port of lag is removed. However, when the last member port is removed, it causes the LAG to undeploy. In that case, the IPSG entry is also flushed out.
- IPSG is not supported for VLAN groups. If upgrading from FastIron 08.0.92 to FastIron 08.0.95, IPSG is not configured for a VLAN group, even if this was previously configured.
- IPSG is not supported for VE interfaces.
- When configuring IPSG on a range of ports, the configuration succeeds on all valid ports.
- IPSG and IPv6 ACLs are supported for the same port.
- IPSG can be enabled on tagged ports or untagged ports in a VLAN.
- IPSG snooping can be configured on a maximum of 511 VLANs.
- IPSG and ACLs are supported together on the same device, as long as they are not configured on the same port or VLAN. If IPSG is enabled for a port, VLAN, or interface level, ACLs cannot be applied to inbound traffic on the port for the VLAN or interface using the **ip access-group** command. When IPSG is configured for a port at the VLAN or interface level, an error will occur if you attempt to apply an ACL to inbound traffic. To bind an IPSG ACL to an interface for incoming traffic, use the **ip sg-access-group** command. Refer to the **ip sg-access-group** command in the *RUCKUS FastIron Command Reference* command for more information.
- If IPSG is configured for a specified port for a VLAN, it cannot be configured globally for the VLAN. Beginning with FastIron 08.0.40a, IPSG 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.
- The scaling number of 512 entries per port is not guaranteed and depends on the rules regarding free TCAM. The amount of free TCAM determines the number of allowed IPSG entries because IPSG is programmed in the TCAM and there are fewer TCAM rules.
- The recommended number of entries for RUCKUS ICX devices is outlined in the following table:.

TABLE 8 Recommended Number of Entries for Ruckus ICX Devices

Devices	Recommended Maximum Number of IPSG Entries Per Device
RUCKUS ICX 7650	4096
RUCKUS ICX 7850	1526
RUCKUS ICX 8200	1024

The recommended maximum number of IPSG entries for the stacking system for RUCKUS ICX 7650, ICX 7850, and ICX 8200 devices is 8192.

- You can enable IPSG on a range of ports within a given slot only. Enabling IPSG across multiple slots is not supported.
- If you enable IPSG 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, is blocked.
- If you enable IPSG 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.
- IPSG protection enables concurrent support with MAC authentication.

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.

1. Enter global configuration mode.

```
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 message 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.

```
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 for a VLAN

You can enable IP Source Guard (IPSG) on a switch or a router for a range of ports in a VLAN or on the entire VLAN.

1. Enter global configuration mode.

```
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 1/1/8
```

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 IPSG on the tagged ports.

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

The following example configures IPSG 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 IPSG 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 IPSG 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
```

The following example configures IPSG on a LAG interface 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 lag 1
```

Enabling IP Source Guard for a LAG Port for a VLAN

You can enable IP Source Guard for a LAG port for a VLAN.

1. Enter global configuration mode.

```
device# configure terminal
```

2. Configure the port-based VLAN.

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

3. Add port LAG 9 as a tagged port.

```
device(config-vlan-12)# tagged lag 9
```

4. Enable Source Guard on the tagged port.

```
device(config-vlan-12)# source-guard enable lag 9
```

The following example configures IP Source Guard for a LAG port for a VLAN.

```
device# configure terminal
device(config)# vlan 12
device(config-vlan-12)# tagged lag 9
device(config-vlan-12)# source-guard enable lag 9
```

Enabling IP Source Guard on Multiple VLANs

You can enable IP Source Guard (IPSG) on a switch or a router for a range of ports in multiple VLANs or all ports on multiple VLANs. The following task configures IPSG on a single port on multiple VLANs.

NOTE
IPSG snooping can be configured on a maximum of 511 VLANs.

1. Enter global configuration mode.

```
device# configure terminal
```

2. Configure the port-based VLANs.

```
device(config)# vlan 100 to 150
```

3. Add port Ethernet 1/1/12 as a tagged port.

```
device(config-mvlan-100-150)# tagged ethernet 1/1/12
```

4. Enable IPSG on the tagged port for multiple VLANs.

```
device(config-mvlan-100-150)# source-guard enable ethernet 1/1/12
```

The following example configures IPSG on a range of ports on multiple VLANs.

```
device# configure terminal
device(config)# vlan 100 to 150
device(config-mvlan-100-150)# tagged ethernet 1/1/23 to 1/1/24
device(config-mvlan-100-150)# source-guard enable ethernet 1/1/23 to 1/1/24
```

The following example configures IPSG on a single port on multiple VLANs.

```
device# configure terminal
device(config)# vlan 151 to 200
device(config-mvlan-151-200)# tagged ethernet 1/1/23
device(config-mvlan-151-200)# source-guard enable ethernet 1/1/23
```

The following example configures IPSG on all ports on multiple VLANs.

```
device# configure terminal
device(config)# vlan 151 to 200
device(config-mvlan-151-200)# tagged ethernet 1/1/23 to 1/1/24
device(config-mvlan-151-200)# source-guard enable
```

Binding IP Source Guard ACLs to Ports

You can bind IPv4 ACLs meant for IP Source Guard (IPSG) ports (SG ACL) to a port or VLAN. IP Source Guard ACLs can then be configured to allow TCP traffic and all UDP traffic. The following task binds IPSG ACL sg-acl1 to port 1/1/2.

1. Enter global configuration mode.

   ```
   device# configure terminal
   ```

2. Configure an Ethernet Interface.

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

3. Enable IPSG on the port.

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

4. Bind the IPSG ACL to the port.

   ```
   device(config-if-e1000/1/1/2)# ip sg-access-group sg-acl1 in
   ```

The following example binds IPSG ACL sg-acl1 to port 1/1/2.

```
device# configure terminal
device(config)# interface ethernet 1/1/2
device(config-if-e1000/1/1/2)# source-guard enable
device(config-if-e1000/1/1/2)# ip sg-access-group sg-acl1 in
```

The following example unbinds the ACL.

```
device# configure terminal
device(config)# interface ethernet 1/1/2
device(config-if-e1000/1/1/2)# no ip sg-access-group sg-acl1 in
```

The following example binds an IPSG ACL for a VLAN interface.

```
device# configure terminal
device(config)# vlan 11
device(config-vlan-11)# source-guard enable
device(config-vlan-11)# ip sg-access-group sg-acl1 in
```

The following example defines IP Source Guard ACL sg123 to allow all TCP traffic and all UDP traffic.

```
device# configure terminal
device(config)# ip sg-access-list sg123
device(config-sg-sg123)# permit tcp any any
device(config-sg-sg123)# permit udp any any
device(config-sg-sg123)# exit
device(config)#
```

The following example defines IP Source Guard ACL sg456 to allow TCP traffic destined for any port number from 100 through 200.

```
device# configure terminal
device(config)# ip sg-access-list sg456
device(config-sg-sg123)# permit tcp any range 100 200
device(config-sg-sg123)# exit
device(config)#
```

The following example binds IP Source Guard ACL sg-acl1 to port 1/1/2.

```
device# configure terminal
device(config)# interface ethernet 1/1/2
device(config-if-e1000/1/1/2)# source-guard enable
device(config-if-e1000/1/1/2)# ip sg-access-group sg-acl1
```

The following example unbinds the ACL.

```
device# configure terminal
device(config)# interface ethernet 1/1/2
device(config-if-e1000/1/1/2)# no ip sg-access-group sg-acl1
```

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 ethernet 1/1/48

Total number of IP Source Guard entries: 33
No    Interface      Type  Flter-mode       IP-address     Vlan   Static
--    ---------      ----  ----------       ----------     ----   -------
1     1/1/48         ip     active        15.15.15.127      1    Yes
2     1/1/48         ip     active          15.15.15.9      1     No
3     1/1/48         ip     active         15.15.15.10      1     No
4     1/1/48         ip     active         15.15.15.11      1     No
5     1/1/48         ip     active         15.15.15.12      1     No
6     1/1/48         ip     active         15.15.15.13      1     No
7     1/1/48         ip     active         15.15.15.14      1     No
8     1/1/48         ip     active         15.15.15.15      1     No
9     1/1/48         ip     active         15.15.15.16      1     No
10    1/1/48         ip     active         15.15.15.17      1     No
```

NOTE

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

DHCPv6

- DHCPv6 overview 95
- DHCP relay agent for IPv6 95
- DHCPv6 Snooping 101
- DHCPv6 Server 107
- IPv6 Source Guard 114

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, the DHCPv6 Relay Agent Prefix Delegation Notification, and DHCPv6 Servers.

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**.

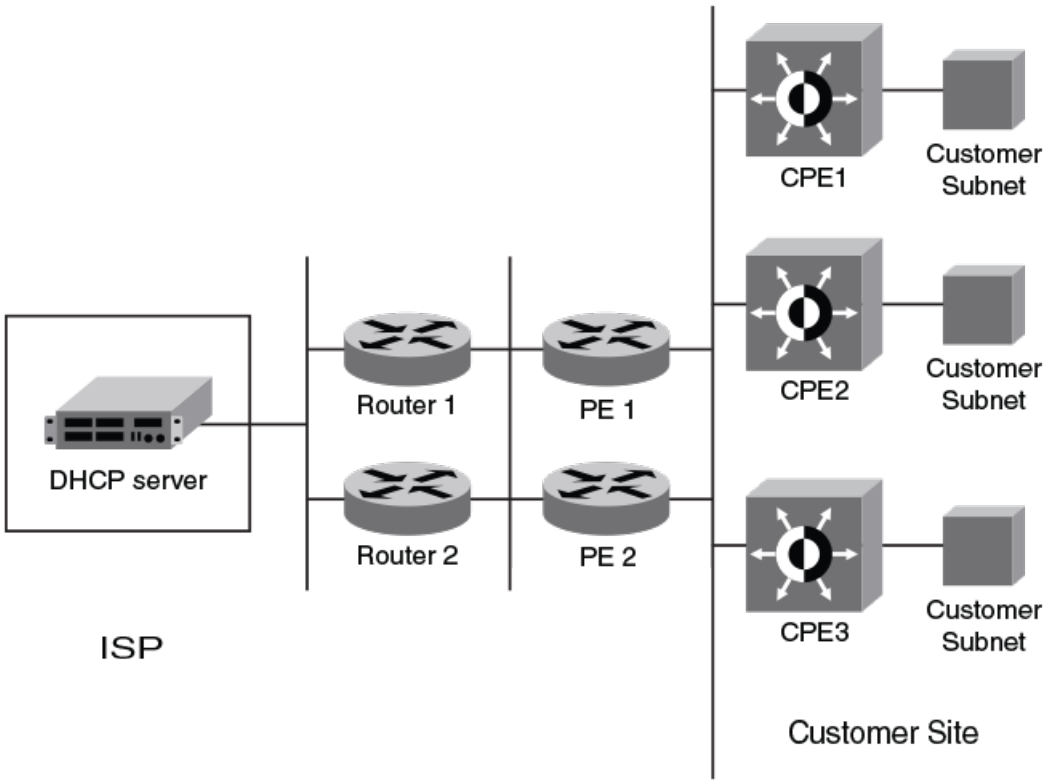
   The following example shows specifying the link layer option.

   ```
   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 15 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 ICX 7850 devices 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 (MITM) attack, the attacker can snoop or spoof the traffic acting 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. The VLAN forwards DHCPv6 server reply packets on trusted ports to DHCPv6 clients, as shown in the following figures.

FIGURE 16 DHCPv6 Snooping at Work on an Untrusted Port

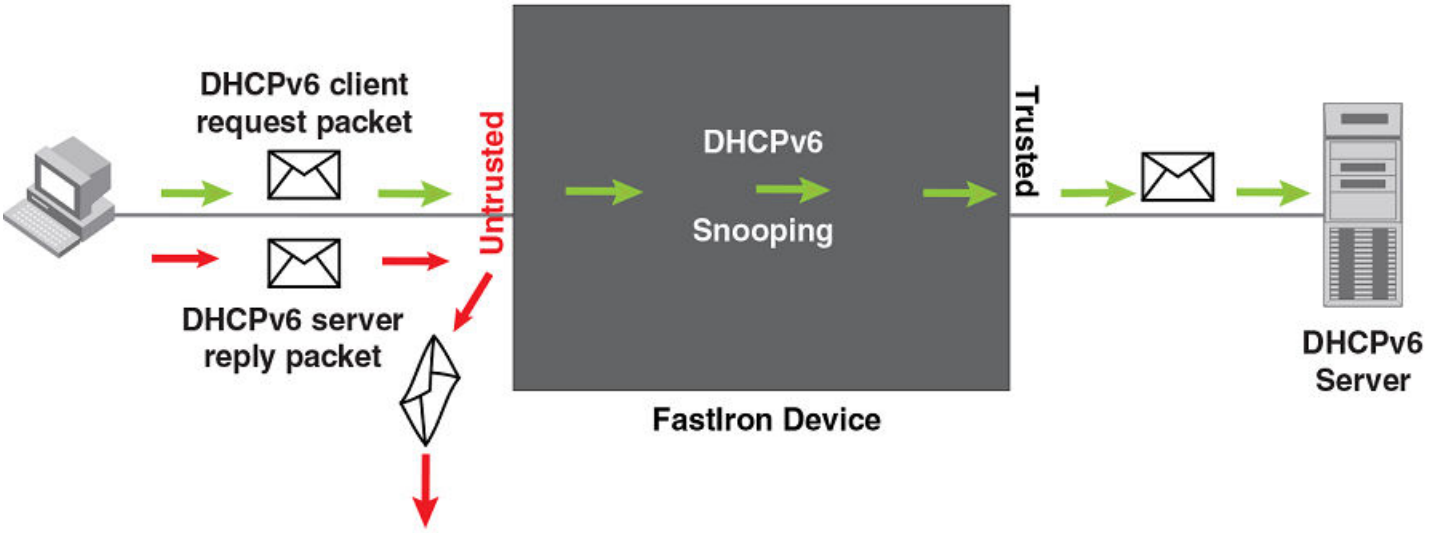
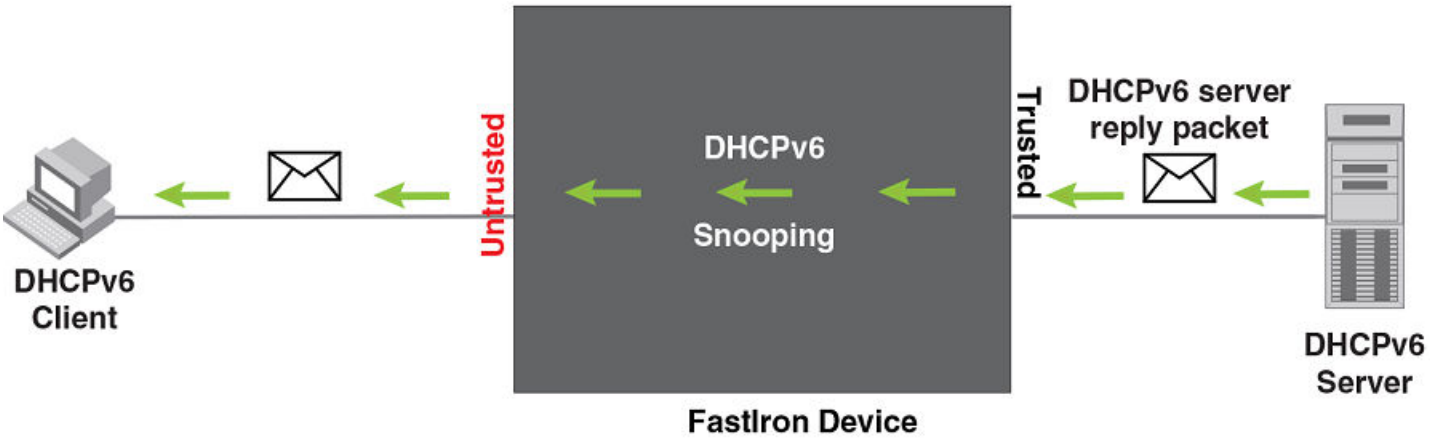


FIGURE 17 DHCPv6 Snooping at Work on a Trusted Port



NOTE
Trusted client ports can lead to DHCPv6 starvation and spoofing attacks. When DHCPv6 snooping is enabled, DHCPv6 request packets received on trusted ports are dropped.

DHCPv6 Binding Database

On trusted ports, DHCPv6 server reply packets are forwarded to DHCPv6 clients. The RUCKUS ICX device removes the entry when the valid lifetime, the time period during which an address is allowed to remain available and usable on a port, 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 must be re-applied on the new default VLAN. DHCPv6 snooping is not automatically configured on the new default VLAN. Therefore, when DHCPv6 Snooping is configured for the default VLAN (for example, VLAN 1), if the default VLAN is changed from VLAN 1 to VLAN 4000, the DHCPv6 Snooping configurations remain configured on the old default VLAN 1. The DHCPv6 Snooping configurations are not automatically configured on the new default VLAN 4000. In previous releases, DHCPv6 Snooping configurations were automatically removed from the old default VLAN and automatically moved to the new default VLAN.
- When a client moves from one port to another port in the same VLAN, the old snoop entry for the client MAC address is automatically updated. This occurs even when the client acquires a new IPv6 address. In previous releases, two snoop entries were maintained with both the old IPv6 address and the new IPv6 address.
- Duplicate IPv6 entries across VLANs are allowed in the DHCPv6 snooping table. When a client moves from one VLAN to another and acquires the same address, two snooping entries are maintained for the same MAC address and IP address.
- Layer 2 MAC movement is supported.
- DHCPv6 snooping cannot be enabled for a VLAN that is a member of a VLAN group.
- When DHCPv6 snooping is enabled, replies are prevented from going out on DHCPv6 snooping trusted ports.
- When configuring DHCPv6 snooping on a range of VLANs, no VLAN in the range can be a member of a VLAN group or any reserved VLAN. Otherwise, the configuration fails on the entire range.
- If required, disable the learning of DHCPv6 clients on ports at the interface configuration level.
- DHCPv6 snooping entries learnt on a member port of VLAN are deleted, with the exception of flexible authentication enabled ports, if the port is removed from the membership of that VLAN.
- DHCPv6 Snooping can be configured for a VLAN or VLANS even before the VLAN or VLANS are created. VLANs and DHCPv6 Snooping configurations on the VLANS are not automatically deleted when the VLAN is deleted.
- When DHCPv6 Snooping is enabled, client and server packets are not allowed on same port.
- DHCP snooping can be configured on a maximum of 511 VLANs.
- When configuring DHCPv6 snooping on a range of VLANs or multi-VLAN, there cannot not be any VLAN in the range that is a member of a VLAN group or any reserved VLAN. Otherwise, configurations fail on the entire range.
- ACLs are supported on member ports of a VLAN on which DHCPv6 snooping is enabled. Refer to Client IP-to-MAC address mappings on page 74 for more information. In previous releases, these were mutually exclusive.
- The following limitation applies to ICX 8200 devices. To support DHCPv6 snooping for Flexible authentication clients in multiple untagged mode, DHCPv6 snooping should also be enabled on the Flexible authentication auth-default VLAN.

  Example Flexible authentication configuration:

  ```
  ICX8200-48P Router# configure terminal
  ICX8200-48P Router(config)# authentication
  ICX8200-48P Router(config-authen)# auth-default-vlan 12
  ICX8200-48P Router(config-authen)# auth-mode multiple-untagged
  ICX8200-48P Router(config-authen)# exit
  ```

  Example DHCP configuration:

  ```
  ICX8200-48P Router(config)# ip dhcp snooping vlan 12
  ```

  Example DHCPv6 configuration:

  ```
  ICX8200-48P Router(config)# ipv6 dhcp6 snooping vlan 12
  ```

Configuring DHCPv6 Snooping

DHCPv6 snooping must be enabled on VLANs, after which the trust setting of ports connected to a DHCPv6 server must be changed to trusted. DHCPv6 packets for a VLAN with DHCPv6 snooping enabled are inspected.

NOTE
DHCPv6 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 DHCPv6 server VLANs.

NOTE
DHCPv6 Snooping can be configured for a VLAN or VLANS even before the VLAN or VLANS are created. VLANs and DHCPv6 Snooping configurations on the VLANS are not automatically deleted when the VLAN is deleted.

1. Enter global configuration mode by using 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 DHCPv6 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 access 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 DHCPv6 clients on ports at the interface configuration level. Disabling the learning of DHCPv6 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 DHCPv6 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 DHCPv6 binding database and the second removes entries for a specific IP address.

```
device# clear ipv6 dhcp6 snooping

device# clear ipv6 dhcp6 snooping 2001::2
```

The following example configures VLAN 10, and enables DHCPv6 snooping for 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 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 on Multiple VLANs

DHCPv6 snooping can be enabled on multiple VLANs using one command. The following task configures multiple VLANs and enables DHCPv6 snooping on most of the configured VLANs using a single command.

NOTE
DHCPv6 snooping can be configured on a maximum number of 511 VLANs at one time.

NOTE
DHCPv6 Snooping can be configured for a VLAN or VLANS even before the VLAN or VLANS are created. VLANs and DHCPv6 Snooping configurations on the VLANS are not automatically deleted when the VLAN is deleted.

NOTE
When configuring DHCPv6 snooping on a range of VLANs or multi-VLAN, there cannot not be any VLAN in the range that is a member of a VLAN group or any reserved VLAN. Otherwise, configurations fail on the entire range.

1. Enter global configuration mode.

```
device# configure terminal
```

2. Configure the port-based VLANs.

```
device(config)# vlan 100 to 150
```

3. Add port Ethernet 1/1/12 as a tagged port.

```
device(config-mvlan-100-150)# tagged ethernet 1/1/12
```

4. Use the **exit** command to return to global configuration mode.

```
device(config-mvlan-100-150)# exit
```

5. Configure more port-based VLANs.

```
device(config)# vlan 151 to 200
```

6. Add port Ethernet 1/1/12 as a tagged port.

```
device(config-mvlan-151-200)# tagged ethernet 1/1/12
```

7. Use the **exit** command to return to global configuration mode.

```
device(config-mvlan-151-200)# exit
```

8. Use the **ipv6 dhcp6 snooping** command with the **to** keyword, specifying a VLAN range, to enable DHCPv6 snooping on multiple VLANs.

```
device(config)# ipv6 dhcp6 snooping vlan 100 to 150 160 170 to 200
```

9. Change the trust setting of the ports that are connected to the DHCP server to trusted at the interface configuration level.
   a) To enable trust on a port, enter interface configuration mode.

```
device(config)# interface ethernet 1/1/12
```

   b) Enable trust on the port.

```
device(config-if-e10000-1/1/12)# dhcp6 snooping trust
```

The following example configures VLANs 100 through 200, and enables DHCPv6 snooping on VLANs 100 through 150, VLAN 160, and VLANs 170 through 200.

```
device# configure terminal
device(config)# vlan 100 to 150
device(config-mvlan-100-150)# tagged ethernet 1/1/12
device(config-mvlan-100-150)# exit
device(config)# vlan 151 to 200
device(config-mvlan-151-200)# tagged ethernet 1/1/12
device(config-mvlan-100-150)# exit
device(config)# ipv6 dhcp6 snooping vlan 100 to 150 160 170 to 200
device(config)# interface ethernet 1/1/12
device(config-if-e10000-1/1/12)# dhcp6 snooping trust
```

Configuring DHCPv6 Snooping for Multi-VRF

DHCPv6 snooping supports Multi-VRF. You can deploy multiple Virtual Routing and Forwarding instances (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. Configure DHCPv6 snooping on a specific VLAN.

   ```
   device(config)# ipv6 dhcp6 snooping vlan 2
   ```

3. 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 DHCPv6 snooping can be specified per VRF.

4. 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
   ```

5. To clear a DHCPv6 binding database of a specific Multi-VRF, enter the following command.

   ```
   device(config)# clear ipv6 dhcp6 snooping vrf vrf2
   ```

6. 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
   ```

7. 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 to display information about the DHCPv6 snooping status and ports.

```
device# show ipv6 dhcp6 snooping
IPv6 DHCPv6 snooping enabled on 2 VLAN(s):
        VLAN(s): 1 11
```

2. Enter the **show ipv6 dhcp6 snooping info** command to display information about the DHCPv6 snooping binding database..

```
device> show ipv6 dhcp6 snooping info

Dhcp snooping Info
Total Learnt Entries 1
Learnt DHCPv6 Snoop Entries
IPv6 Address  Mac Address     Valid-Time  Preferred-Time  Port/Lag Vlan VRF
2001::5       00c5.0600.0001  2753        2753            1/2/4    1    default-vrf
…
```

DHCPv6 Server

The Dynamic Host Configuration Protocol version 6 (DHCPv6) is a network protocol for configuring IPv6 hosts with IP addresses, IP prefixes, and other configuration data required to operate in an IPv6 network. All FastIron devices can be configured to function as DHCPv6 servers.

DHCPv6 Server is the IPv6 equivalent of the Dynamic Host Configuration Protocol (DHCP) for IPv4 that is documented in the DHCP Server chapter. In the same manner as DHCP for IPv4, a DHCPv6 server allocates temporary or permanent network IPv6 addresses to clients. When a client requests the use of an address for a time interval, the DHCPv6 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. When the client is done with the address, the address is released back to the server. Clients may also receive a permanent assignment. In short, the DHCPv6 server assigns IPv6 addresses to all clients and it keeps track of the bindings. DHCPv6 Server also allows for greater control of address distribution within a subnet.

> **NOTE**
> For the DHCPv6 server to be enabled, you must upgrade to FI 08.0.90 using the Unified FastIron Image (UFI). Refer to the *Software Upgrade and Downgrade* chapter in the *RUCKUS FastIron Software Upgrade Guide* for more information.

Configuration Considerations for DHCPv6 Servers

The following configuration considerations apply to DHCPv6 servers.

- For the DHCPv6 server to be enabled, you must upgrade to FI 08.0.90 using the Unified FastIron Image (UFI). Refer to the *Software Upgrade and Downgrade* chapter in the *RUCKUS FastIron Software Upgrade Guide* for more information.
- The DHCPv6 server is not supported for non-default VRFs.
- The ICX DHCPv6 server does not assign IPv6 addresses via DHCPv6 relay.
- IPv6 unicast routing must be enabled.
- For stateless DHCPv6 servers, IPv6 addresses are assigned to the clients through auto-configuration. The DHCPv6 server is used only to assign information such as domain-names, multiple DNS servers other supported DHCPv6 options. One ICX interface should be configured with an IPV6 address that falls in the subnet range configured for the DHCPv6 server.
- Neighbor discovery protocol (NDP) should be configured for stateless DHCPv6 servers.
- A FastIron device configured as a DHCPv6 server can support up to 500 DHCP clients.

- Up to 100 DHCPv6 subnets can be configured for the DHCPv6 server.
- When the rapid commit option is configured on the server, only Solicit and Reply packets are sent between the client and the server instead of Solicit, Advertise, Request and Reply. For the rapid commit mode to work, the client should also have the rapid commit option enabled.
- Whenever a configuration change is made with respect to the DHCPv6 server, the configuration change is written to the **dhcpd.conf** file in the Linux within 30 seconds. When this occurs, the dhcpd process restarts.
- For a full list of commands supported for DHCPv6 Servers, refer to the **What's New** section in the *RUCKUS FastIron Command Reference*

Configuring the Stateless DHCPv6 Server

Perform the following steps to configure a stateless DHCPv6 server.

Consider the following when configuring the stateless DHCPv6 server:

- For stateless DHCPv6 servers, up to 100 DHCPv6 subnets can be configured.
- In SLAAC (Stateless Address Auto-configuration), the client does not require the DHCPv6 server to get the IPv6 address. It receives the prefix, prefix-length, and the Default Gateway from the RA and the address is auto-configured.
- The DHCPv6 client can only get other information, such as DNS and domain-name, from the DHCPv6 server.
- The configuration of the nd other-config-flag, using the **ipv6 nd other-config-flag** command, is required for the stateless DHCPv6 server to receive DNS and domain name configuration. When the **ipv6 nd other-config-flag** command is used, the O flag is set to 1.
- When the client sends an Information-Request to the server, the server replies with information such as domain-name and DNS server.
- Since the IPv6 address is not assigned by the DHCPv6 server, the lease entry is not seen on the server.

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

   ```
   router# configure terminal
   ```

2. Enter the **ipv6 unicast-routing** command to enable the forwarding of IPv6 traffic.

   ```
   router(config)# ipv6 unicast-routing
   ```

3. Enter the **ipv6 dhcp6-server enable** command to enable the DHCPv6 server.

   ```
   router(config)# ipv6 dhcp6-server enable
   ```

4. (Optional) Enter the **domain-name** command, entering a domain name, to configure the domain name server (DNS) domain name.

   ```
   router(config-dhcp6)# domain-name example.com
   ```

5. (Optional) Enter the **dns-server** command, specifying an IPv6 address, to specify the IPv6 address of the DNS server.

   ```
   router(config-dhcp6)# dns-server 8fef:400:efdd:301::10  8fef:400:efdd:301::20
   ```

6. Enter the **renewal-time** command, specifying an interval, to set the time interval after which the client transitions to the renewing state upon receipt of an IPv6 address.

   ```
   router(config-dhcp6)# renewal-time 50
   ```

   If the renewal time is not configured, half of the valued of the configured preferred lifetime is considered as the renewal time.

7. Enter the **subnet** command, specifying an IPv6 prefix, to configure a subnet for the DHCPv6 server and enter DHCPv6 subnet configuration mode.

   ```
   router(config-dhcp6)# subnet6 8fef:400:efdd:301::/64
   ```

8. Enter the **range6** command, specifying IPv6 addresses, to assign IPv6 addresses in the specified range.

```
router(config-dhcpv6-subnet)# range6 8fef:400:efdd:301::100 8fef:400:efdd:301::200
```

9. Enter the **exit** command until you return to global configuration mode.

```
router(config-dhcpv6-subnet)# exit
router(config-dhcp6)# exit
router(config)#
```

10. Enter the **vlan** command and enter a VLAN ID to create a VLAN.

```
router(config)# vlan 100
```

11. Enter the **untagged** command and specify a port to add an untagged Ethernet port to the port-based VLAN and specify the port connected to the client into one VLAN.

```
router(config-vlan-100)# untagged ethernet 1/1/2
```

12. Create a virtual routing interface

```
router(config-vlan-100)# interface ve 100
```

13. Enter the **exit** command to return to global configuration mode.

```
router(config-vlan-100)# exit
```

14. Enter the **interface ve** command specifying the configured VLAN.

```
router(config)# interface ve 100
```

15. Enter the **ipv6 address** command, specifying an IPv6 address, to configure an IPv6 address on the server interface in the range of the configured subnet6.

```
router(config-vif-100)# ipv6 address 8fef:400:efdd:301::3/64
```

16. Enter the **ipv6 nd other-config-flag** command to enable the hosts to use autoconfiguration to get non-IPv6-address information.

```
router(config-vif-100)# ipv6 nd other-config-flag
```

The following example enables IPv6 unicast routing, configures a stateless DHCPv6 server and configures an IPv6 address on the server interface in the range of the configured subnet6. The **ipv6 nd other-config-flag** command is used to set the 0 flag to 1.

```
router# configure terminal
router(config)# ipv6 unicast-routing
router(config)# ipv6 dhcp6-server enable
router(config-dhcp6)# domain-name example.com
router(config-dhcp6)# dns-server 8fef:400:efdd:301::10  8fef:400:efdd:301::20
router(config-dhcp6)# renewal-time 50
router(config-dhcp6)# subnet6 8fef:400:efdd:301::/64
router(config-dhcpv6-subnet)# range6 8fef:400:efdd:301::100 8fef:400:efdd:301::200
router(config-dhcpv6-subnet)# exit
router(config-dhcp6)# exit
router(config)# vlan 100
router(config-vlan-100)# untagged ethernet 1/1/2
router(config-vlan-100)# interface ve 100
router(config-vlan-100)# exit
router(config)# interface ve 100
router(config-vif-100)# ipv6 address 8fef:400:efdd:301::3/64
router(config-vif-100)# ipv6 nd other-config-flag
```

Configuring the Stateful DHCPv6 Server

Perform the following steps to configure a stateful DHCPv6 server.

Consider the following when configuring the stateful DHCPv6 server:

- For stateful DHCPv6 servers, up to 100 DHCPv6 subnets can be configured.
- For stateful DHCPv6 Servers, the client requires the DHCPv6 server to get the IPv6 address and other information such as DNS and domain-name.
- The configuration of the nd managed address configuration flag, using the **ipv6 nd managed-config-flag** command is required for stateful DHCPv6 servers. When the **ipv6 nd managed-config-flag** command is used, the M flag is set to 1.
- The IPv6 address is assigned by the DHCPv6 server, and the lease entry can be viewed on the server in the output of the **show ipv6 dhcp6-server lease** command.

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

   ```
   router# configure terminal
   ```

2. Enter the **ipv6 unicast-routing** command to enable the forwarding of IPv6 traffic.

   ```
   router(config)# ipv6 unicast-routing
   ```

3. Enter the **ipv6 dhcp6-server enable** command to enable the DHCPv6 server.

   ```
   router(config)# ipv6 dhcp6-server enable
   ```

4. Enter the **domain-name** command, entering a domain name, to configure the domain name server (DNS) domain name.

   ```
   router(config-dhcp6)# domain-name example.com
   ```

5. Enter the **dns-server** command, specifying an IPv6 address, to specify the IPv6 address of the DNS server.

   ```
   router(config-dhcp6)# dns-server 8fef:400:efdd:301::10  8fef:400:efdd:301::20
   ```

6. Enter the **renewal-time** command, specifying an interval, to set the time interval after which the client transitions to the renewing state upon receipt of an IPv6 address.

   ```
   router(config-dhcp6)# renewal-time 50
   ```

   If the renewal time is not configured, half of the valued of the configured preferred lifetime is considered as the renewal time.

7. Enter the **subnet6** command, specifying an IPv6 prefix, to configure a subnet for the DHCPv6 server and enter DHCPv6 subnet configuration mode.

   ```
   router(config-dhcp6)# subnet6 8fef:400:efdd:301::/64
   ```

8. Enter the **range6** command, specifying IPv6 addresses, to assign IPv6 addresses in the specified range.

   ```
   router(config-dhcpv6-subnet)# range6 8fef:400:efdd:301::100 8fef:400:efdd:301::200
   ```

9. Enter the **exit** command until you return to global configuration mode.

   ```
   router(config-dhcpv6-subnet)# exit
   router(config-dhcp6)# exit
   router(config)#
   ```

10. Enter the **vlan** command and enter a VLAN ID to create a VLAN.

    ```
    router(config)# vlan 100
    ```

11. Enter the **untagged** command and specify a port to add an untagged Ethernet port to the port-based VLAN and specify the port connected to the client into one VLAN.

```
router(config-vlan-100)# untagged ethernet 1/1/2
```

12. Create a virtual routing interface.

```
router(config-vlan-100)# interface ve 100
```

13. Enter the **exit** command to return to global configuration mode.

```
router(config-vlan-100)# exit
```

14. Enter the **interface ve** command specifying the configured VLAN.

```
router(config)# interface ve 100
```

15. Enter the **ipv6 address** command, specifying an IPv6 address, to configure an IPv6 address on the server interface in the range of the configured subnet6.

```
router(config-vif-100)# ipv6 address 8fef:400:efdd:301::3/64
```

16. Enter the **ipv6 nd managed-config-flag** command to enable the hosts to use autoconfiguration to get non-IPv6-address information.

```
router(config-vif-100)# ipv6 nd managed-config-flag
```

The following example enables IPv6 unicast routing, configures a stateful DHCPv6 server and configures an IPv6 address on the server interface in the range of the configured subnet6. The **ipv6 nd managed-config-flag** command is used to set the M flag to 1.

```
router# configure terminal
router(config)# ipv6 unicast-routing
router(config)# ipv6 dhcp6-server enable
router(config-dhcp6)# domain-name example.com
router(config-dhcp6)# dns-server 8fef:400:efdd:301::10  8fef:400:efdd:301::20
router(config-dhcp6)# renewal-time 50
router(config-dhcp6)# subnet6 8fef:400:efdd:301::/64
router(config-dhcpv6-subnet)# range6 8fef:400:efdd:301::100 8fef:400:efdd:301::200
router(config-dhcpv6-subnet)# exit
router(config-dhcp6)# exit
router(config)# vlan 100
router(config-vlan-100)# untagged ethernet 1/1/2
router(config-vlan-100)# interface ve 100
router(config-vlan-100)# exit
router(config)# interface ve 100
router(config-vif-100)# ipv6 address 8fef:400:efdd:301::3/64
router(config-vif-100)# ipv6 nd managed-config-flag
```

Displaying DHCPv6 Server Information

Various show commands can display statistical information about DHCPv6 Servers.

Use one or more of the following commands to verify DHCPv6 Server information. Using these commands is optional, and the variations of the command can be entered in any order.

1. Enter the **show ipv6 dhcp6-server** command with the **global** keyword to display global information for the DHCPv6 server.

```
device> show ipv6 dhcp6-server global

IPV6 DHCP6 SERVER GLOBAL CONFIGURATION SUMMARY:

                            Configuration Status :  enable
                              Preferred lifetime :  1230
                                  Valid lifetime :  2000
                                Renewal time(t1%):  0
                                 Rebind time(t1%):  700
                               Refresh time(t1%) :  1000
                              Enable Rapid Commit:  No
                                     Domain Name :
                                     DNS Servers :  1234::1
```

2. Enter the **show ipv6 dhcp6-server** command with the **lease** keyword to display information about the DHCPv6 server lease entries.

```
device> show ipv6 dhcp6-server lease

IA-NA: Client IP addr: 3ffe:501:ffff:100:dc87:7c42:d4fb:ba7e
Preffered-lifetime: 121
Binding State: active
Valid lifetime : 200
Expires at : 2018/10/09 17:42:42
```

3. Enter the **show ipv6 dhcp6-server** command with the **subnet6** keyword to display information about all the subnets configured on a device. The first subnet, “3efd:320:ddee:202::/64”, has range6 configured as a range of ipv6 addresses. The second subnet, “3ffe:501:ffff:100::/64”, has range6 configured as a prefix.

```
device> show ipv6 dhcp6-server subnet6

******IPV6 DHCP6 SERVER SUBNETS CONFIGURATION SUMMARY *********

-------------------------------------------------

                                        Subnet6 :  3efd:320:ddee:202::/64
                                   Subnet Name :
                                Preferred lifetime :  0
                                    Valid lifetime :  0
                                       Domain Name :
                                     Range6 prefix :  ::/0
                                             Range6:  3efd:320:ddee:202::5
                                                    :  3efd:320:ddee:202::15
                                        DNS Servers:
-------------------------------------------------

                                        Subnet6 :  3ffe:501:ffff:100::/64
                                   Subnet Name :
                                Preferred lifetime :  0
                                    Valid lifetime :  0
                                       Domain Name :
                                     Range6 prefix :  3ffe:501:ffff:100::/64
                                        DNS Servers:
```

4. Enter the **show ipv6 dhcp6-server** command with the **subnet6** keyword, and specify an IPv6 prefix address to display information about a specific subnet configured on a device.

```
device> show ipv6 dhcp6-server subnet6 3ffe:501:ffff:100::/64

******IPV6 DHCP6 SERVER SUBNETS CONFIGURATION SUMMARY *********
-------------------------------------------------
Subnet6 : 3ffe:501:ffff:100::/64
Subnet Name : testname
Preferred lifetime : 40
Valid lifetime : 100
Domain Name : www.test.com
Range6 prefix : 3ffe:501:ffff:100::/64
Prefix6 : ::/0
DNS Servers:
```

Verification in Linux Mode

1. Telnet to the remote IP reach Linux mode. Use the **ps-aef** and **grep dhcpd** to check if the dhcpd process is running.
2. Verify the configuration in the **dhcpd.conf** file in the /etc path in Linux.
3. Verify the **dhcpd6.leases** file in the /etc path and in the /fast_iron path for the lease file in the flash.

Prefix Delegation

Prefix delegation allows a DHCPv6 server assign prefixes chosen from a global pool to DHCPv6 clients. The DHCPv6 client can then configure an IPv6 address on its LAN interface using the received prefix. It then sends router advertisements that include the prefix, allowing other devices to use auto-configuration to configure their own IPv6 addresses.

The PD device will be connected to the DHCPv6 server. The DHCPv6 server should have prefix6 configured. The PD device receives the prefix from the DHCPv6 server. The hosts connected to the PD device receives the IPv6 address in the prefix received by the PD device.

The following example assigns a range of IPv6 prefixes to a subnet.

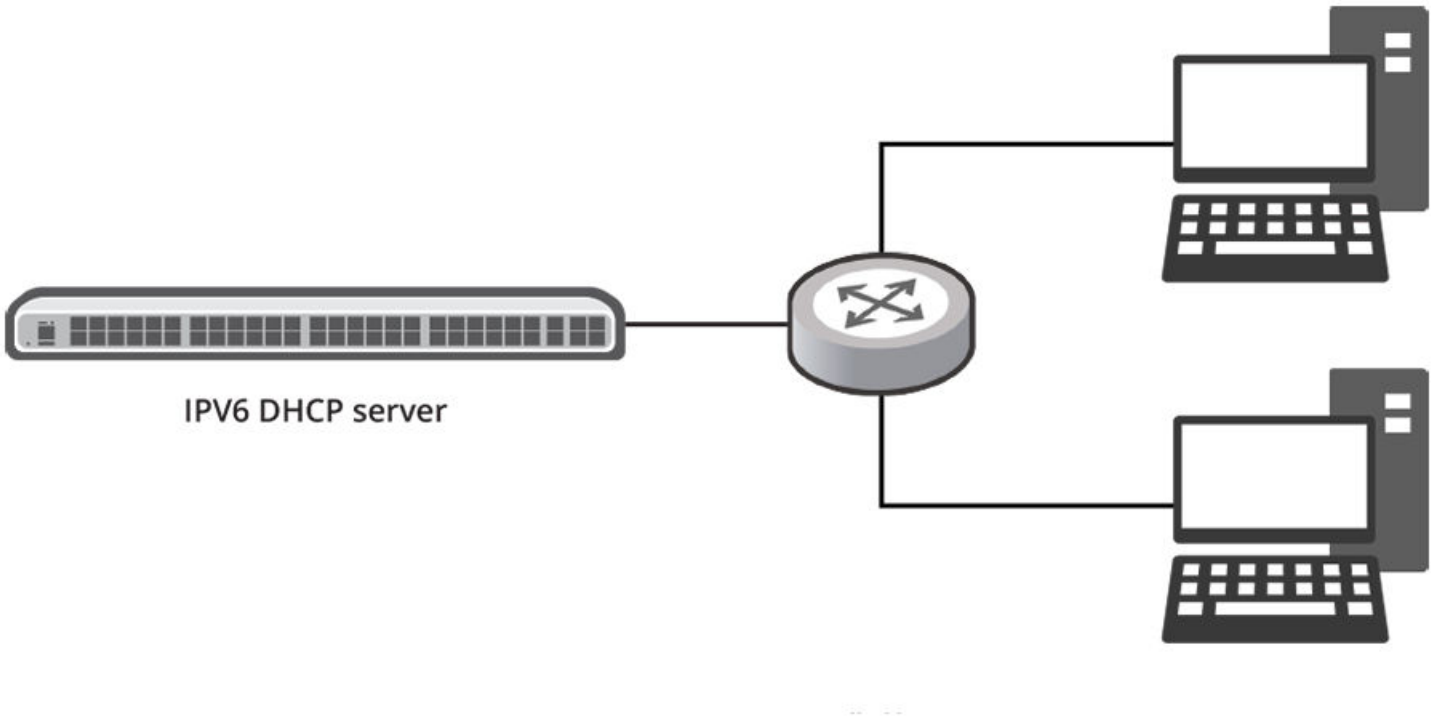
```
device# configure terminal
device(config)# ipv6 dhcp6-server enable
device(config-dhcp6)# subnet6 3ffe:501:ffff:100::/64
device(config-dhcpv6-subnet)# prefix6 3ffe:501:ffff:100::/64 3ffe:501:ffff:103::/64
```

Prefix Delegation for ICX DHCPv6 Servers

Prefix delegation allows a DHCPv6 server to assign prefixes selected from a global pool to DHCPv6 clients (requesting routers). The DHCPv6 client can then configure an IPv6 address on its LAN interface using the received prefix. The DHCPv6 client then sends router advertisements that include the prefix, allowing other devices to use auto-configuration to configure their own IPv6 addresses. The PD device (requesting routers) is connected to the DHCPv6 server (ICX box). The DHCPv6 server must have prefix6 configured. The PD device receives the prefix from the DHCPv6 server. The hosts connected to the PD device receive the IPv6 address in the prefix received by the PD device.

The following illustration shows delegated prefix addressing configured for an ICX device.

FIGURE 18 Delegated Prefix Addressing Using DHCPv6



The following example assigns a range of IPv6 prefixes to a subnet. The **prefix6** command is used to configure the prefix range for delegation to sub-routers.

```
device# configure terminal
device(config)# ipv6 dhcp6-server enable
device(config-dhcp6)# subnet6 2001:db8:0:1::/64
device (config-dhcp6-subnet)# range6 2001:db8:0:1::129 2001:db8:0:1::254
device(config-dhcpv6-subnet)# prefix6 2001:db8:0:100::/56 2001:db8:0:f00::/56
```

The following configuration example shows a sample configuration for an ICX device with the prefix delegation feature and DHCPv6 server enabled.

```
!
ipv6 dhcp6-server enable
 subnet6 2001:db8:0:1::/64
  prefix6 2001:db8:0:100::/56 2001:db8:0:f00::/56
  range6  2001:db8:0:1::129  2001:db8:0:1::254
exit
!
ipv6 unicast-routing
!
interface ve 4080
 ipv6 address 2001:db8:0:1::100/6
```

IPv6 Source Guard

You can use IPv6 Source Guard (IPSGv6) together with IPv6 Neighbor Discovery Inspection (NDI) on untrusted ports.

The RUCKUS implementation of the IPSGv6 technology supports configuration on a port and specific VLAN memberships on a port.

When IPSGv6 is first enabled, only DHCPv6 packets are allowed, while all other IPv6 traffic is blocked. IPSGv6 allows IPv6 traffic when the system learns IPv6 addresses via IPv6 DHCP snooping.

When a new IPv6 source entry binding on the port is created or deleted, an access-list with a permit filter for the IPv6 address is added or deleted. By default, if IPSGv6 is enabled without any IPv6 source binding on the port, an ACL that denies all IPv6 traffic is loaded on the port.

Configuration Notes and Feature Limitations for IPv6 Source Guard

The following configuration notes and feature limitations apply to IPv6 Source Guard (IPSGv6):

- Configuring IPSGv6 static entries at the VLAN or port level is allowed only after IPSGv6 is configured at the VLAN level, at the port level, or both.
- IPSGv6 configuration can be removed at the VLAN or port level only after all IPSGv6 static entries are unconfigured at the VLAN or port level.
- IPSGv6 is not supported for the default VLAN.
- If a LAG is undeployed, IPSGv6 configurations are auto-cleared.
- IPSGv6 configurations are auto-cleared for a VLAN if it is deleted.
- IPSGv6 cannot be configured for a range of VLANs.
- IPSGv6 functions across reload.
- IPSGv6 configurations are supported for all non-default VLANs.
- IPSGv6 is not supported for VLAN groups.
- IPSGv6 is not supported for VE interfaces.
- When configuring IPSGv6 on a range of ports, the configuration succeeds on all valid ports.
- IPSGv6 and IPv6 ACLs are not supported for the same port.
- IPSGv6 and Ingress IPv6 ACL are supported together on the same device, as long as they are not configured on the same port or VLAN.
- IPSGv6 can be enabled on tagged or untagged ports in a VLAN but cannot be configured globally for a VLAN.
- IPSGv6 can be configured on a maximum of 511 VLANs.
- The recommended number of entries for RUCKUS ICX devices is outlined in the following table:

TABLE 9 Recommended Number of Entries for Ruckus ICX Devices

Devices	Recommended Maximum Number of IPSGv6 Entries Per Device
RUCKUS ICX 7550	2048
RUCKUS ICX 7650	2048
RUCKUS ICX 7850	1536
RUCKUS ICX 8200	512

The recommended maximum number of IPSGv6 entries on a stack of RUCKUS ICX 7550, ICX 7650, ICX 7850, or ICX 8200 devices is 8192.

- You can enable IPSGv6 on a range of ports within a given slot only, for example, ports 1/1/1 thru 1/1/24. Enabling IPSGv6 across multiple slots is not supported.
- If you enable IPSGv6 in a network topology that has DHCPv6 clients, you must also enable DHCPv6 snooping. If you do not enable DHCPv6 snooping, all IPv6 traffic, including DHCPv6 packets, is blocked.
- Rate-limiting based on source IPv6 address cannot be combined with IPSGv6. Thus, a fixed rate-limit input cannot be configured when IPSGv6 is enabled on the port.

Enabling IPv6 Source Guard on a Port or Range of Ports

IPv6 Source Guard (IPSGv6) is disabled by default. You can enable IPSGv6 on DHCPv6 snooping untrusted ports.

1. Enter global configuration mode.

   ```
   device# configure terminal
   ```

2. Enter interface configuration mode.

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

3. Enable IPSGv6 on the port.

   ```
   device(config-if-e10000-1/1/1)# ipv6 source-guard enable
   ```

4. To enable IPSGv6 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 IPSGv6 on a range of ports, you can choose only a range of ports within a given slot.

5. Enable IPSGv6 on the range of ports specified in the previous step.

   ```
   device(config-mif-1/1/21-1/1/25)# ipv6 source-guard enable
   ```

The following example enables IPSGv6 for an Ethernet interface.

```
device# configure terminal
device(config)# interface ethernet 1/1/1
device(config-if-e10000-1/1/1)# ipv6 source-guard enable
```

The following example enable IPSGv6 for a range of Ethernet interfaces.

```
device# configure terminal
device(config)# interface ethernet 1/1/21 to 1/1/25
device((config-mif-1/1/21 to 1/1/25)# ipv6 source-guard enable
```

Defining Static IPv6 Source Bindings

You can manually enter valid IPv6 addresses in the binding database.

Note that because static IPv6 source bindings consume system resources, you should avoid unnecessary bindings.

1. Enter global configuration mode.

   ```
   device# configure terminal
   ```

2. Enter the **ipv6 source binding** command followed by a valid IPv6 address and the interface number. Entering the VLAN number is optional.

   ```
   device(config)# ipv6 source binding 10::10 ethernet 1/1/1 vlan 10
   ```

   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.

The following example configures IPSGv6 bindings on selective ports of a VLAN.

```
device# configure terminal
device(config)# ipv6 source binding 10::10 ethernet 1/1/1 vlan 10
```

The following example disables IPSGv6 bindings for an Ehternet interface..

```
device# configure terminal
device(config)# no ipv6 source binding 10::10 ethernet 1/1/1
```

Enabling IPv6 Source Guard for a VLAN

You can enable IPv6 Source Guard (IPSGv6) on a switch or a router for a range of ports in a VLAN or on the entire VLAN.

1. Enter global configuration mode.

   ```
   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 1/1/8
   ```

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 IPSGv6 on the tagged ports.

   ```
   device(config-vlan-12)# ipv6 source-guard enable ethernet 1/1/23 to 1/1/24
   ```

The following example configures IPSGv6 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)# ipv6 source-guard enable ethernet 1/1/23 to 1/1/24
```

The following example configures IPSGv6 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)# ipv6 source-guard enable ethernet 1/1/23
```

The following example configures IPSGv6 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)# ipv6 source-guard enable
```

The following example configures IPSGv6 on a LAG interface 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)# ipv6 source-guard enable lag 1
```

Enabling IPv6 Source Guard for a LAG Port for a VLAN

You can enable IPv6 Source Guard (IPSGv6) for a LAG port for a VLAN.

1. Enter global configuration mode.

```
device# configure terminal
```

2. Configure the port-based VLAN.

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

3. Add port LAG 9 as a tagged port.

```
device(config-vlan-12)# tagged lag 9
```

4. Enable IPSGv6 on the tagged port.

```
device(config-vlan-12)# ipv6 source-guard enable lag 9
```

The following example configures IPSGv6 for a LAG port for a VLAN.

```
device# configure terminal
device(config)# vlan 12
device(config-vlan-12)# tagged lag 9
device(config-vlan-12)# ipv6 source-guard enable lag 9
```

Displaying Learned IPv6 Addresses

To display the learned IPv6 addresses for IPv6 Source Guard ports, use the **show ipv6 source-guard** command.

```
device> show ipv6 source-guard

Total number of IP Source Guard entries: 8
No    Interface           Type  Flter-mode       IPv6-address      Vlan   Static
--    ---------           ----  ----------       ------------        ----   -------
1     1/1/25              ipv6     active               10::1      2    Yes
2     1/1/25              ipv6     active               10::2      2    Yes
3     1/1/25              ipv6     active               10::3      2    Yes
4     1/1/25              ipv6     active               10::4      2    Yes
5     1/1/25              ipv6     active               10::5      2    Yes
6     1/1/26              ipv6     active               10::5      ANY    No
7     1/1/26              ipv6     active               10::5      ANY    No
8     1/1/26              ipv6     active               10::5      ANY    No
```

NOTE

All static entries in the IPv6 source guard table will be populated as "Yes".

350 West Java Dr., Sunnyvale, CA 94089 USA
https://www.commscope.com