



ExtremeSwitching™

# **Configuring IP Routing and Multicast on Ethernet Routing Switch 3500 Series**

Release 5.3.6  
NN47203-502  
Issue 05.01  
December 2017

© 2017, Extreme Networks, Inc.  
All Rights Reserved.

#### Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Extreme Networks, Inc. assumes no liability for any errors. Extreme Networks, Inc. reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

#### Documentation disclaimer

"Documentation" means information published in varying mediums which may include product information, operating instructions and performance specifications that are generally made available to users of products. Documentation does not include marketing materials. Extreme Networks shall not be responsible for any modifications, additions, or deletions to the original published version of Documentation unless such modifications, additions, or deletions were performed by or on the express behalf of Extreme Networks. End User agrees to indemnify and hold harmless Extreme Networks, Extreme Networks' agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

#### Link disclaimer

Extreme Networks is not responsible for the contents or reliability of any linked websites referenced within this site or Documentation provided by Extreme Networks. Extreme Networks is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Extreme Networks does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

#### Warranty

Extreme Networks provides a limited warranty on Extreme Networks hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Extreme Networks' standard warranty language, as well as information regarding support for this product while under warranty is available to Extreme Networks customers and other parties through the Extreme Networks Support website: <http://www.extremenetworks.com/support> under the link "Policies" or such successor site as designated by Extreme Networks. Please note that if You acquired the product(s) from an authorized Extreme Networks Channel Partner outside of the United States and Canada, the warranty is provided to You by said Extreme Networks Channel Partner and not by Extreme Networks.

"Hosted Service" means an Extreme Networks hosted service subscription that You acquire from either Extreme Networks or an authorized Extreme Networks Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Extreme Networks or Extreme Networks Channel Partner (as applicable) for more information.

#### Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN EXTREME NETWORKS HOSTED SERVICE SUBSCRIPTION FROM EXTREME NETWORKS OR AN EXTREME NETWORKS CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE EXTREME NETWORKS WEBSITE, <https://extremeportal.force.com> OR SUCH SUCCESSOR SITE AS DESIGNATED BY EXTREME NETWORKS, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU

REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

#### Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE EXTREME NETWORKS WEBSITE, <https://extremeportal.force.com> OR SUCH SUCCESSOR SITE AS DESIGNATED BY EXTREME NETWORKS, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS EXTREME NETWORKS SOFTWARE, PURCHASED FROM EXTREME NETWORKS, INC., ANY EXTREME NETWORKS AFFILIATE, OR AN EXTREME NETWORKS CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH EXTREME NETWORKS OR AN EXTREME NETWORKS CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY EXTREME NETWORKS IN WRITING, EXTREME NETWORKS DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN EXTREME NETWORKS, AN EXTREME NETWORKS AFFILIATE OR AN EXTREME NETWORKS CHANNEL PARTNER; EXTREME NETWORKS RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND EXTREME NETWORKS, INC. OR THE APPLICABLE EXTREME NETWORKS AFFILIATE ("EXTREME NETWORKS").

Extreme Networks grants You a license within the scope of the license types described below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License as set forth below in the Designated System(s) License (DS) section as applicable. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. "Software" means computer programs in object code, provided by Extreme Networks or an Extreme Networks Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. "Designated Processor" means a single stand-alone computing device. "Server" means a set of Designated Processors that hosts (physically or virtually) a software application to be accessed by multiple users. "Instance" means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine ("VM") or similar deployment.

#### License type(s)

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only: 1) on a number of Designated Processors up to the number indicated in the order; or 2) up to the number of Instances of the Software as indicated in the order, Documentation, or as authorized by Extreme Networks in writing. Extreme Networks may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Extreme Networks through electronic means established by Extreme Networks specifically for this purpose.

#### Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Extreme Networks. All content on this site, the documentation, Hosted Service, and the product provided by Extreme Networks including the selection, arrangement and design of the content is owned either by Extreme Networks or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part,

including any code and software unless expressly authorized by Extreme Networks. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Extreme Networks can be a criminal, as well as a civil offense under the applicable law.

### Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Note, unless otherwise stated, that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Extreme Networks Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

### Third Party Components

"Third Party Components" mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Extreme Networks' website at: <http://www.extremenetworks.com/support/policies/software-licensing> or such successor site as designated by Extreme Networks. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

The following applies only if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE [HTTP://WWW.MPEGLA.COM](http://WWW.MPEGLA.COM).

### Service Provider

THE FOLLOWING APPLIES TO EXTREME NETWORKS CHANNEL PARTNER'S HOSTING OF EXTREME NETWORKS PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN EXTREME NETWORKS CHANNEL PARTNER'S HOSTING OF EXTREME NETWORKS PRODUCTS MUST BE AUTHORIZED IN WRITING BY EXTREME NETWORKS AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE EXTREME NETWORKS CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE EXTREME NETWORKS CHANNEL PARTNER'S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE EXTREME NETWORKS CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE EXTREME NETWORKS CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE EXTREME NETWORKS CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE [WWW.SIPRO.COM/CONTACT.HTML](http://WWW.SIPRO.COM/CONTACT.HTML). THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR

THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE [HTTP://WWW.MPEGLA.COM](http://WWW.MPEGLA.COM).

### Compliance with Laws

You acknowledge and agree that it is Your responsibility for complying with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Extreme Networks product is used.

### Preventing Toll Fraud

"Toll Fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

### Security Vulnerabilities

Information about Extreme Networks' security support policies can be found in the Global Technical Assistance Center Knowledgebase at <https://gtacknowledge.extremenetworks.com/>.

### Downloading Documentation

For the most current versions of Documentation, see the Extreme Networks Support website: <http://documentation.extremenetworks.com>, or such successor site as designated by Extreme Networks.

### Contact Extreme Networks Support

See the Extreme Networks Support website: <http://www.extremenetworks.com/support> for product or Hosted Service notices and articles, or to report a problem with your Extreme Networks product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Extreme Networks Support website: <http://www.extremenetworks.com/support/contact/> (or such successor site as designated by Extreme Networks), scroll to the bottom of the page, and select Contact Extreme Networks Support.

### Contact Avaya Support

See the Avaya Support website: <https://support.avaya.com> for product or Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: <https://support.avaya.com> (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

### Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Extreme Networks are the registered or unregistered Marks of Extreme Networks, Inc., its affiliates, its licensors, its suppliers, or other third parties. Users are not permitted to use such Marks without prior written consent from Extreme Networks or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Extreme Networks or the applicable third party.

Extreme Networks is a registered trademark of Extreme Networks, Inc.

All non-Extreme Networks trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

For additional information on Extreme Networks trademarks, please see: <http://www.extremenetworks.com/company/legal/>

# Contents

<b>Chapter 1: Preface</b> .....	10
Purpose.....	10
Training.....	10
Providing Feedback to Us.....	10
Getting Help.....	10
Extreme Networks Documentation.....	11
Subscribing to service notifications.....	12
<b>Chapter 2: New in this document</b> .....	13
<b>Chapter 3: CLI command modes</b> .....	14
<b>Chapter 4: IP routing fundamentals</b> .....	16
IP addressing overview.....	16
Subnet addressing.....	17
IP routing.....	18
IP routing using VLANs.....	19
Local routes.....	19
Static routes.....	20
Layer 3 Non-Local Static Routes (IP NLSR).....	21
Default routes.....	22
Route scaling.....	23
Management VLAN.....	23
DHCP Server.....	24
DHCP Server usage examples.....	26
Related routing features.....	35
BootP DHCP relay.....	35
DHCP option 82 support.....	37
UDP broadcast forwarding.....	38
Directed broadcasts.....	39
ARP.....	40
Static ARP.....	40
Proxy ARP.....	40
IP blocking for stacks.....	41
<b>Chapter 5: IGMP fundamentals</b> .....	43
Overview of IP multicast.....	43
Multicast groups.....	44
Multicast addresses.....	45
IGMP overview.....	45
IGMPv1 operation.....	45
IGMPv2 operation.....	46
IGMPv3 operation.....	48

IGMP requests for comment.....	49
IGMP snooping.....	49
IGMPv3 snooping.....	51
IGMP proxy.....	51
IGMPv3 proxy.....	53
Forwarding of reports.....	53
Static mrouter port and nonquerier.....	53
Unknown multicast packet filtering.....	54
Robustness value.....	55
IGMP snooping configuration rules.....	55
Default IGMP values.....	56
IGMP snooping interworking with Windows clients.....	56
<b>Chapter 6: IP routing configuration using CLI.....</b>	<b>58</b>
IP routing configuration procedures.....	58
Configuring global IP routing status.....	58
Displaying global IP routing status.....	59
Configuring an IP address for a VLAN.....	59
Configuring IP routing status on a VLAN.....	60
Displaying the IP address configuration and routing status for a VLAN.....	61
Displaying IP routes.....	61
<b>Chapter 7: Static route configuration using CLI.....</b>	<b>63</b>
Configuring a static route.....	63
Displaying static routes.....	64
Configuring a management route.....	65
Displaying the management routes.....	66
<b>Chapter 8: DHCP relay configuration using CLI.....</b>	<b>67</b>
Prerequisites to DHCP relay configuration.....	67
DHCP relay configuration procedures.....	67
Enabling or disabling global DHCP relay.....	68
Setting global DHCP relay to default.....	68
Displaying the global DHCP relay status.....	68
Displaying IP DHCP client parameters.....	69
Specifying a local DHCP relay agent and remote DHCP server.....	69
Displaying the DHCP relay configuration.....	70
Configuring DHCP relay on a VLAN.....	70
Displaying the DHCP relay configuration for a VLAN.....	72
Displaying DHCP relay counters.....	72
Clearing DHCP relay counters for a VLAN.....	73
Configuring DHCP Relay Option 82 globally.....	73
Configuring DHCP Relay with Option 82 for a VLAN.....	74
Configuring DHCP Forwarding Maximum Frame size.....	74
Assigning a DHCP Relay Option 82 subscriber ID to a port.....	75
Displaying DHCP Relay.....	75

<b>Chapter 9: DHCP Server configuration using CLI</b> .....	77
Displaying the DHCP Server status.....	77
Displaying DHCP Server IP address pools.....	77
Displaying DHCP Server IP address leases.....	78
Enabling DHCP Server.....	79
Disabling the DHCP Server.....	80
Restoring the DHCP Server to default.....	80
Configuring DHCP Server IP address lease duration.....	81
Resetting DHCP Server lease duration to default .....	81
Configuring DHCP Server routers.....	82
Deleting DHCP Server routers.....	82
Configuring the Domain Name System server .....	83
Deleting DNS servers.....	84
Creating a DHCP Server IP address pool.....	85
Configuring DHCP Server IP address pool options.....	86
DHCP Server Option 43 vendor specific information.....	88
DHCP Server Option 241 parameters.....	91
Deleting Option 241 parameters for DHCP server pool .....	98
Deleting Option 242 parameters for DHCP server pool.....	99
Disabling DHCP Server IP address pools.....	100
Configuring static IP addresses.....	100
Creating the IP DHCP Server Pool for a Vendor Class Identifier.....	101
<b>Chapter 10: UDP broadcast forwarding configuration using CLI</b> .....	102
Prerequisites to UDP broadcast forwarding.....	102
UDP broadcast forwarding configuration procedures.....	102
Configuring UDP protocol table entries.....	103
Displaying the UDP protocol table.....	103
Configuring a UDP forwarding list.....	104
Applying a UDP forwarding list to a VLAN .....	104
Displaying the UDP broadcast forwarding configuration.....	106
Clearing UDP broadcast counters on an interface.....	107
<b>Chapter 11: Directed broadcasts configuration using CLI</b> .....	108
Configuring directed broadcasts.....	108
Displaying the directed broadcast configuration.....	108
<b>Chapter 12: Static ARP and Proxy ARP configuration</b> .....	110
Configuring a static ARP entry.....	110
Displaying ARP entries.....	111
Configuring a global timeout for ARP entries.....	112
Clearing the ARP cache.....	113
Configuring proxy ARP status.....	113
Displaying proxy ARP status on a VLAN.....	114
<b>Chapter 13: IP blocking configuration using CLI</b> .....	115
Configuring IP blocking for a stack.....	115

Configuring IP blocking mode to default value.....	115
Displaying IP blocking mode.....	116
Displaying IP blocking state.....	116
Clearing the IP blocking mode state.....	116
<b>Chapter 14: IGMP snooping configuration using CLI.....</b>	<b>118</b>
Configuring IGMP snooping on a VLAN.....	118
Configuring IGMP proxy on a VLAN.....	119
Configuring static mrouter ports on a VLAN.....	120
Configuring IGMP parameters on a VLAN.....	121
Displaying IGMP interface information.....	123
Displaying IGMP group membership information.....	124
Displaying IGMP cache Information.....	125
Flushing the IGMP router table.....	126
Configuring IGMP router alert on a VLAN.....	127
<b>Chapter 15: IP routing configuration using Enterprise Device Manager.....</b>	<b>128</b>
Configuring global IP routing status and ARP lifetime using EDM.....	128
Configuring an IP address and enabling routing for a VLAN.....	129
Displaying configured IP Addresses using EDM.....	130
<b>Chapter 16: Static route configuration using Enterprise Device Manager.....</b>	<b>132</b>
IP route management using EDM.....	132
Displaying IP routes using EDM.....	132
Filtering route information using EDM.....	133
Configuring static routes using EDM.....	134
Displaying TCP information for the switch using EDM.....	135
Displaying TCP Connections using EDM.....	136
Displaying TCP Listeners using EDM.....	137
Displaying UDP endpoints using EDM.....	138
<b>Chapter 17: DHCP relay configuration using Enterprise Device Manager.....</b>	<b>140</b>
DHCP relay configuration procedures.....	140
Configuring DHCP Forwarding.....	140
Enabling or disabling DHCP Forwarding.....	140
Configuring DHCP Forwarding maximum frame size globally.....	141
Configuring DHCP Relay using EDM.....	141
Configuring DHCP Relay with Option 82 globally using EDM.....	142
Configuring DHCP parameters on a VLAN using EDM.....	143
Displaying and graphing DHCP counters on a VLAN using EDM.....	144
Assigning a DHCP Relay Option 82 subscriber ID to a port using EDM.....	144
Displaying DHCP Relay counters information using EDM.....	145
<b>Chapter 18: DHCP Server configuration using Enterprise Device Manager.....</b>	<b>147</b>
Enabling DHCP Server.....	147
Configuring DHCP Server global options.....	148
Displaying the DHCP Server pool.....	149
Configuring a DHCP Server pool.....	150



DHCP Server Option 43 vendor specific information.....	153
Deleting a DHCP Server pool.....	155
Configuring DHCP Server pool options.....	156
Deleting DHCP Server pool options.....	157
Displaying DHCP Server Client information.....	158
<b>Chapter 19: UDP broadcast forwarding configuration using Enterprise Device Manager.....</b>	<b>159</b>
UDP broadcast forwarding configuration procedures.....	159
Configuring UDP protocol table entries using EDM.....	159
Configuring UDP forwarding entries using EDM.....	160
Configuring a UDP forwarding list using EDM.....	161
Applying a UDP forwarding list to a VLAN using EDM.....	161
<b>Chapter 20: Static ARP and Proxy ARP configuration using Enterprise Device Manager.....</b>	<b>163</b>
Configuring static ARP entries using EDM.....	163
Configuring Proxy ARP using EDM.....	164
<b>Chapter 21: IGMP snooping configuration using Enterprise Device Manager.....</b>	<b>165</b>
Managing IGMP snoop using EDM.....	165
Configuring IGMP snoop, proxy and static mrouter ports on a VLAN using EDM.....	165
Displaying IGMP groups using EDM.....	166
Displaying IGMP group information using EDM.....	167
Displaying IGMP cache information using EDM.....	168
Managing IP Address multicast filter tables using EDM.....	168
Specifying an IP address to be allowed to flood a VLAN using EDM.....	169
Displaying the IP Address Multicast Filter Table using EDM.....	169
Configuring IGMP interface parameters and flushing IGMP tables using EDM.....	170
Configuring VLAN snooping using EDM.....	172
Displaying the MAC Multicast Filter Table using EDM.....	174
<b>Chapter 22: IP Routing capabilities and limitations.....</b>	<b>175</b>

# Chapter 1: Preface

---

## Purpose

This document provides procedures and conceptual information to configure IP routing features on the Extreme Networks ERS 3500 Series, including static routes, Proxy ARP, DHCP Relay, and UDP forwarding. It also provides procedures and conceptual information to manage multicast traffic using IGMP snooping.

---

## Training

Ongoing product training is available. For more information or to register, you can access the Web site at [www.extremenetworks.com/education/](http://www.extremenetworks.com/education/).

---

## Providing Feedback to Us

We are always striving to improve our documentation and help you work better, so we want to hear from you! We welcome all feedback but especially want to know about:

- Content errors or confusing or conflicting information.
- Ideas for improvements to our documentation so you can find the information you need faster.
- Broken links or usability issues.

If you would like to provide feedback to the Extreme Networks Information Development team about this document, please contact us using our short [online feedback form](#). You can also email us directly at [internalinfodev@extremenetworks.com](mailto:internalinfodev@extremenetworks.com)

---

## Getting Help

### Product purchased from Extreme Networks

If you purchased your product from Extreme Networks, use the following support contact information to get help.

If you require assistance, contact Extreme Networks using one of the following methods:

- [GTAC \(Global Technical Assistance Center\) for Immediate Support](#)
  - Phone: 1-800-998-2408 (toll-free in U.S. and Canada) or +1 408-579-2826. For the support phone number in your country, visit: [www.extremenetworks.com/support/contact](http://www.extremenetworks.com/support/contact)
  - Email: [support@extremenetworks.com](mailto:support@extremenetworks.com). To expedite your message, enter the product name or model number in the subject line.
- [GTAC Knowledge](#) – Get on-demand and tested resolutions from the GTAC Knowledgebase, or create a help case if you need more guidance.
- [The Hub](#) – A forum for Extreme customers to connect with one another, get questions answered, share ideas and feedback, and get problems solved. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.
- [Support Portal](#) – Manage cases, downloads, service contracts, product licensing, and training and certifications.

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number and/or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any action(s) already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related RMA (Return Material Authorization) numbers

### **Product purchased from Avaya**

If you purchased your product from Avaya, use the following support contact information to get help.

Go to the Avaya Support website at <http://support.avaya.com> for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

---

## **Extreme Networks Documentation**

To find Extreme Networks product guides, visit our documentation pages at:

Current Product Documentation

[www.extremenetworks.com/documentation/](http://www.extremenetworks.com/documentation/)

*Table continues...*

Archived Documentation (for previous versions and legacy products)  
Release Notes

[www.extremenetworks.com/support/documentation-archives/](http://www.extremenetworks.com/support/documentation-archives/)

[www.extremenetworks.com/support/release-notes](http://www.extremenetworks.com/support/release-notes)

## Open Source Declarations

Some software files have been licensed under certain open source licenses. More information is available at: [www.extremenetworks.com/support/policies/software-licensing](http://www.extremenetworks.com/support/policies/software-licensing).

---

## Subscribing to service notifications

Subscribe to receive an email notification for product and software release announcements, Vulnerability Notices, and Service Notifications.

### About this task

You can modify your product selections at any time.

### Procedure

1. In an Internet browser, go to <http://www.extremenetworks.com/support/service-notification-form/>.
2. Type your first and last name.
3. Type the name of your company.
4. Type your email address.
5. Type your job title.
6. Select the industry in which your company operates.
7. Confirm your geographic information is correct.
8. Select the products for which you would like to receive notifications.
9. Click **Submit**.

## Chapter 2: New in this document

There are no new feature changes in this document.

# Chapter 3: CLI command modes

Command Line Interface (CLI) provides the following command modes:

- User EXEC
- Privileged EXEC
- Global Configuration
- Interface Configuration
- Application Configuration

Mode access is determined by access permission levels and password protection.

If no password is set, you can enter CLI in User EXEC mode and use the enable command to move to the next level (Privileged EXEC mode). However, if you have read-only access, you cannot progress beyond User EXEC mode, the default mode. If you have read-write access you can progress from the default mode through all of the available modes.

With sufficient permission, you can use the rules in the following table to move between the command modes.

**Table 1: CLI command modes**

Command mode and sample prompt	Entrance commands	Exit commands
User Executive Switch>	No entrance command, default mode	exit or logout
Privileged Executive Switch#	enable	exit or logout
Global Configuration Switch (config)#	From Privileged Executive mode, enter configure terminal	To return to Privileged Executive mode, enter end or exit To exit CLI completely, enter

*Table continues...*

Command mode and sample prompt	Entrance commands	Exit commands
		logout
<b>Interface Configuration</b> Switch (config-if)#	From Global Configuration mode: To configure a port, enter interface fastethernet <port number> To configure a VLAN, enter interface vlan <vlan number> To configure a loopback, enter interface loopback <loopback number>	To return to Global Configuration mode, enter exit To return to Privileged Executive mode, enter end To exit CLI completely, enter logout
<b>Application Configuration</b> Switch (config-app)#	From Global, or Interface Configuration mode, enter application	To return to Global Configuration mode, enter exit To return to Privileged Executive mode, enter end To exit CLI completely, enter logout

# Chapter 4: IP routing fundamentals

This chapter provides an introduction to IP routing and related features.

---

## IP addressing overview

An IP version 4 (IPv4) address consists of 32 bits expressed in a dotted-decimal format (XXX.XXX.XXX.XXX). The IPv4 address space is divided into classes, with classes A, B, and C reserved for unicast addresses, and accounting for 87.5 percent of the 32-bit IP address space. Class D is reserved for multicast addressing. The following table lists the breakdown of the IP address space by address range and mask.

Class	Address Range	Mask	Number of Networks	Nodes per Network
A	1.0.0.0 - 127.0.0.0	255.0.0.0	127	16 777 214
B	128.0.0.0 - 191.255.0.0	255.255.0.0	16 384	65 534
C	192.0.0.0 - 223.255.255.0	255.255.255.0	2 097 152	255
D	224.0.0.0 - 239.255.255.254			
E	240.0.0.0 - 240.255.255.255			

**\* Note:**  
Class D addresses are primarily reserved for multicast operations, although the addresses 224.0.0.5 and 224.0.0.6 are used by OSPF and 224.0.0.9 is used by RIP

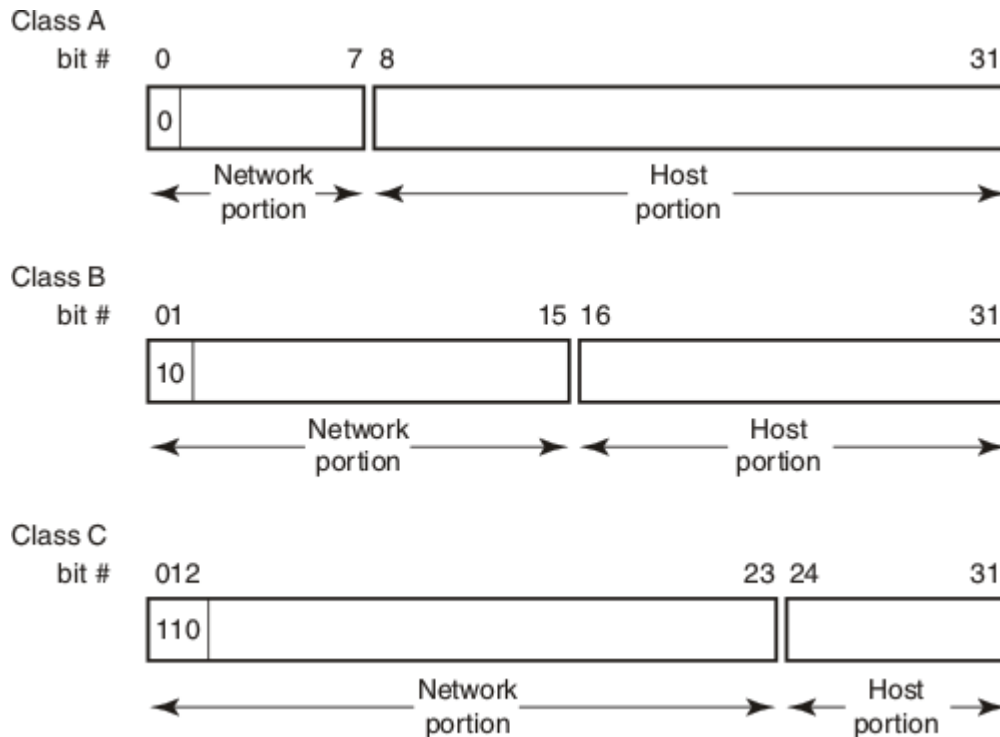
**\* Note:**  
Although technically part of Class A addressing, network 127 is reserved for loopback.

**\* Note:**  
Class E addresses are reserved for research purposes.

To express an IP address in dotted-decimal notation, each octet of the IP address is converted to a decimal number and separated by decimal points. For example, the 32-bit IP address 10000000 00100000 00001010 10100111 is expressed in dotted-decimal notation as 128.32.10.167.



Each IP address class, when expressed in binary notation, has a different boundary point between the network and host portions of the address, as shown in the following figure. The network portion is a network number field from 8 through 24 bits. The remaining 8 through 24 bits identify a specific host on the network.



**Figure 1: Network and host boundaries in IP address classes**

## Subnet addressing

Subnetworks (or subnets) are an extension of the IP addressing scheme. With subnets, organizations can use one IP address range for multiple networks. Subnets are two or more physical networks that share a common network-identification field (the network portion of the 32-bit IP address).

A subnet address is created by increasing the network portion to include a subnet address, thus decreasing the host portion of the IP address. For example, in the address 128.32.10.0, the network portion is 128.32, while the subnet is found in the first octet of the host portion (10). A subnet mask is applied to the IP address and identifies the network and host portions of the address.

The following table illustrates how subnet masks used with Class B and Class C addresses can create differing numbers of subnets and hosts. This example shows the use of the zero subnet, which is permitted on the switch.

Number of bits	Subnet Mask	Number of Subnets (Recommended)	Number of Hosts per Subnet
Class B			
2	255.255.192.0	2	16 382
3	255.255.224.0	6	8190
4	255.255.240.0	14	4094
5	255.255.248.0	30	2046
6	255.255.252.0	62	1022
7	255.255.254.0	126	510
8	255.255.255.0	254	254
9	255.255.255.128	510	126
10	255.255.255.192	1022	62
11	255.255.255.224	2046	30
12	255.255.255.240	4094	14
13	255.255.255.248	8190	6
14	255.255.255.252	16 382	2
Class C			
1	255.255.255.	0	126
2	255.255.255.192	2	62
3	255.255.255.224	6	30
4	255.255.255.240	14	14
5	255.255.255.248	30	6
6	255.255.255.252	62	2

Variable-length subnet masking (VLSM) is the ability to divide an intranet into pieces that match network requirements. Routing is based on the longest subnet mask or network that matches.

---

## IP routing

To configure IP routing on the switch, you must create virtual router interfaces by assigning an IP address to a virtual local area network (VLAN). The following sections provide more details about IP routing functionality.

For a more detailed description about VLANs and their use, see *Configuring VLANs, Spanning Tree, and MultiLink Trunking on Ethernet Routing Switch 3500 Series*.

---

## IP routing using VLANs

The switch supports wire-speed IP routing between VLANs. To create a virtual router interface for a specified VLAN, you must associate an IP address with the VLAN.

The virtual router interface is not associated with any specific port. The VLAN IP address can be reached through any of the ports in the VLAN. The assigned IP address also serves as the gateway through which packets are routed out of that VLAN. Routed traffic can be forwarded to another VLAN within the switch or stack.

When the switch is routing IP traffic between different VLANs, the switch is considered to be running in Layer 3 mode; otherwise, the switch runs in Layer 2 mode. When you assign an IP address to a Layer 2 VLAN, the VLAN becomes a routable Layer 3 VLAN.

You can assign a single and unique IP address to each VLAN. You can configure the global status of IP routing to be enabled or disabled on the switch. By default, IP routing is disabled.

The switch supports local routes and static routes (local and non-local static routes). With local routing, the switch automatically creates routes to each of the local Layer 3 VLAN interfaces. With static routing, you must manually enter the routes to the destination IP addresses.

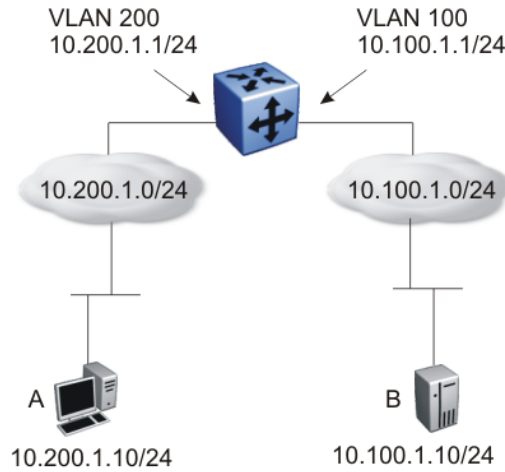
---

## Local routes

With routing globally enabled, if you assign an IP address to a VLAN, IP routing is enabled for that VLAN. In addition, for each IP address assigned to a VLAN interface, the Ethernet Routing Switch adds a directly connected or local route to its routing table based on the IP address/ mask assigned.

## Local routing example

The following figure shows how the Ethernet Routing Switch can route between Layer 3 VLANs. In this example, the Ethernet Routing Switch has two VLANs configured. IP Routing is enabled globally on the switch and on the VLANs, each of which has an assigned IP address.



Avaya Ethernet Routing Switch

**Figure 2: Local routes example**

IP address 10.100.1.1/24 is assigned to VLAN 100, and IP address 10.200.1.1/24 is assigned to VLAN 200. As IP Routing is enabled, two local routes become active on the Ethernet Routing Switch as described in the following table.

	Network	Net-mask	Next-hop	Type
1	10.100.1.0	255.255.255.0	10.100.1.1	LOCAL
2	10.200.1.0	255.255.255.0	10.200.1.1	LOCAL

At this stage, both hosts A (10.200.1.10) and B (10.100.1.10) are reachable from the Ethernet Routing Switch. However, to achieve Layer 3 connectivity between A and B, additional configuration is required. Host A must know how to reach network 10.100.1.0/24, and host B must know how to reach network 10.200.1.0/24.

On host A, you must configure a route to network 10.100.1.0/24 through 10.200.1.1, or configure 10.200.1.1 as the default gateway for the host.

On host B, you must configure a route to network 10.200.1.0/24 through 10.100.1.1, or configure 10.100.1.1 as the default gateway for the host.

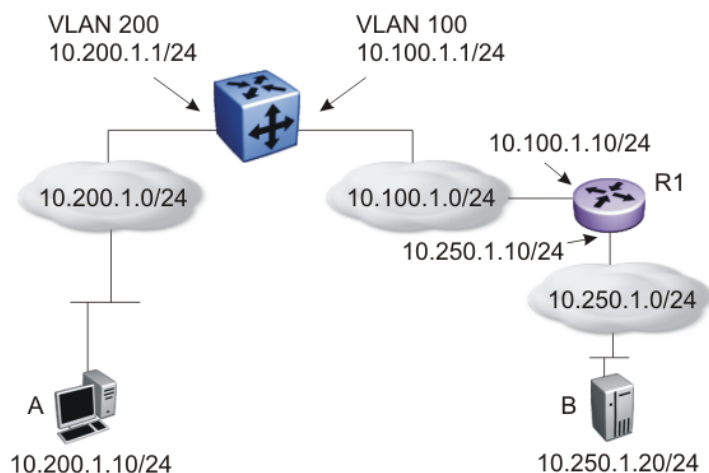
With these routes configured, the Ethernet Routing Switch can perform inter-VLAN routing, and packets can flow between hosts A and B.

## Static routes

After you create routable VLANs through IP address assignment, you can create static routes. With static routes, you can manually create specific routes to a destination IP address. Local and non-local static routes are supported.

## Static routing example

The following figure shows an example of static routing on the Ethernet Routing Switch.



**Figure 3: Static routes**

In this example, two Layer 3 devices are used to create a physical link between hosts A and B. This network contains an Ethernet Routing Switch and another Layer 3 router, R1.

In this setup, the local route configuration from [Local routing example](#) on page 19 still applies. However, in this case, network 10.100.1.0/24 stands in between networks 10.200.1.0/24 and 10.250.1.0/24. To achieve end-to-end connectivity, router R1 must know how to reach network 10.200.1.0/24, and the Ethernet Routing Switch must know how to reach network 10.250.1.0/24. On the Ethernet Routing Switch, you can accomplish this using static routing. With static routing, you can configure a route to network 10.250.1.0/24 through 10.100.1.10. In this case, the following routes are active on the Ethernet Routing Switch.

	Network	Net-mask	Next-hop	Type
1	10.100.1.0	255.255.255.0	10.100.1.1	LOCAL
2	10.200.1.0	255.255.255.0	10.200.1.1	LOCAL
3	10.250.1.0	255.255.255.0	10.100.1.10	STATIC

To obtain Layer 3 connectivity between the hosts, additional routes are required. Host A requires a route to 10.250.1.0/24 using 10.200.1.1 as the next hop, or with 10.200.1.1 as the default gateway. Host B requires a route to 10.200.1.0/24 using 10.250.1.10 as the next hop, or with 10.250.1.10 as the default gateway.

The configuration for router R1 to reach network 10.200.1.0/24 is dependent on the type of router used.

## Layer 3 Non-Local Static Routes (IP NLSR)

After you create routable VLANs through IP address assignment, you can create static routes.

You can manually create specific routes to destination IP addresses with static routes.

Local static routes have a next-hop that is on a directly-connected network.

Non-local routes (NLSR) have a next-hop that is not on a directly-connected network.

When you implement NLSR on the switch, if the corresponding next-hop IP address can be reached through any active route on the switch, a static route becomes active in the routing table.

The switch elects a support route as the most specific route through which the next-hop IP address can be reached. Then the switch links the NLSR route to an active support route. The NLSR becomes inactive if the support route becomes inactive and no alternative support route can be calculated.

The support route can be a static route or dynamic route (on switches that support dynamic routing), but it cannot be the default route (network 0.0.0.0 netmask 0.0.0.0) because, if NLSR reachability is allowed through the default route, then any route could change to active as NLSR reachable through the default route.

Advantages of IP NLSR:

- Where there are multiple paths to a network you can reduce the number of static routes by using only one route with a remote gateway
- Where the next-hop IP address cannot be reached directly from the switch, the system can use any host IP address that exists on the path to the destination network to configure an active and functional route, as long as the host can be reached through another active route on the switch
- You do not need to modify the NLSR route if an administrator changes the next-hop IP address
- If the support route is an ECMP route, and one of the next-hops becomes unreachable, the NLSR route remains active as long as the support route is active through at least one of the next-hops
- If the support route is an ECMP route, internally, the NLSR route uses the first of the ECMP route next-hops as the NLSR next-hop

Limitations of IP NLSR:

- Because static routes are not easily scalable, in a large or growing network this type of route management may not be the best option
- Because static routes cannot determine path failure, a router can still attempt to use a failed path

---

## Default routes

Default routes specify a route to all networks for which there are no explicit routes in the Forwarding Information Base or the routing table. This static default route is a route to the network address 0.0.0.0 as defined by the Institute of Electrical and Electronics Engineers (IEEE) Request for Comment (RFC) 1812 standard.

The Ethernet Routing Switch uses the default route 0.0.0.0/0.0.0.0 for all Layer 3 traffic that does not match a specific route. This traffic is forwarded to the next-hop IP address specified in the default route.

---

## Route scaling

The switch supports a maximum of 32 local routes and up to 32 static routes, including the default route (Destination = 0.0.0.0, Mask = 0.0.0.0).

---

## Management VLAN

With IP routing enabled on the switch or stack, you can use any of the virtual router IP addresses for device management over IP. Any routable Layer 3 VLAN can carry the management traffic for the switch, including Telnet, Simple Network Management Protocol (SNMP), BootP, and Trivial File Transfer Protocol (TFTP). Without routing enabled, the management VLAN is reachable only through the switch or stack IP address, and only through ports that are members of the management VLAN. The management VLAN always exists on the switch and cannot be removed.

When routing is enabled on the switches, the management VLAN behaves similar to other routable VLANs. The IP address is reachable through any virtual router interface, as long as a route is available.

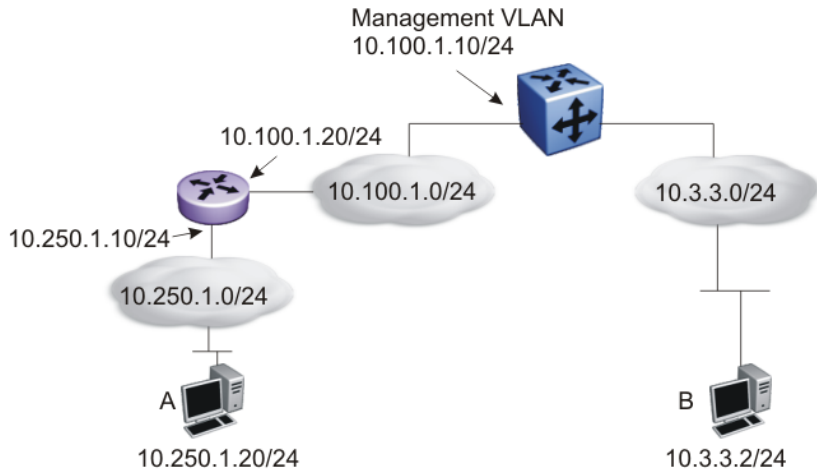
## Management route

On the Ethernet Routing Switch, you can configure a management route from the Management VLAN to a particular subnet. The management route is a static route that allows incoming management connections from the remote network to the management VLAN.

The management route transports traffic between the specified destination network and the Management VLAN only. It does not carry inter-VLAN routed traffic from the other Layer 3 VLANs to the destination network. This provides a management path to the router that is inaccessible from the other Layer 3 VLANs. While you can access the management VLAN from all static routes, other static routes cannot route traffic to the management route.

To allow connectivity through a management route, you must enable IP routing globally and on the management VLAN interface.

The following figure shows an example of a management route allowing access to the management VLAN interface.



**Figure 4: Management route**

As network 10.250.1.0/24 is not directly connected to the Ethernet Routing Switch, to achieve connectivity from host 10.250.1.20 to the management VLAN, the Ethernet Routing Switch must know how to reach network 10.250.1.0/24. On the Ethernet Routing Switch, you can configure a management route to network 10.250.1.0/24 through 10.100.1.20. In this case, the following management route is active on the Ethernet Routing Switch.

	Network	Net-mask	Next-hop	Type
1	10.250.1.0	255.255.255.0	10.100.1.20	MANAGEMENT

With this configured route, host A at 10.250.1.20 can perform management operations on the Ethernet Routing Switch. To do so, Host A also requires a route to 10.100.1.0/24 using 10.250.1.10 as the next hop, or with 10.250.1.10 as the default gateway.

If a Layer 3 VLAN is also configured for network 10.3.3.0/24, this provides a local route that host B at 10.3.3.2 can use to access the switch. However, host B cannot communicate with host A, as the route to network 10.250.1.0/24 is a management route only. To provide connectivity between the two hosts, you must configure a static route to 10.250.1.0/24.

## DHCP Server

If you require local provision of TCP/IP addresses and have no separate DHCP Server or other device available to provide the service to local hosts, DHCP Server is included on the switch. You can use the DHCP Server feature to provide and manage client IPv4 addresses in your network and eliminate manual TCP/IP configuration. DHCP Server is disabled by default.

Following is some of the information DHCP clients request from DHCP Server:

- IPv4 address – Note: IPv6 address allocation is not supported
- Subnet mask

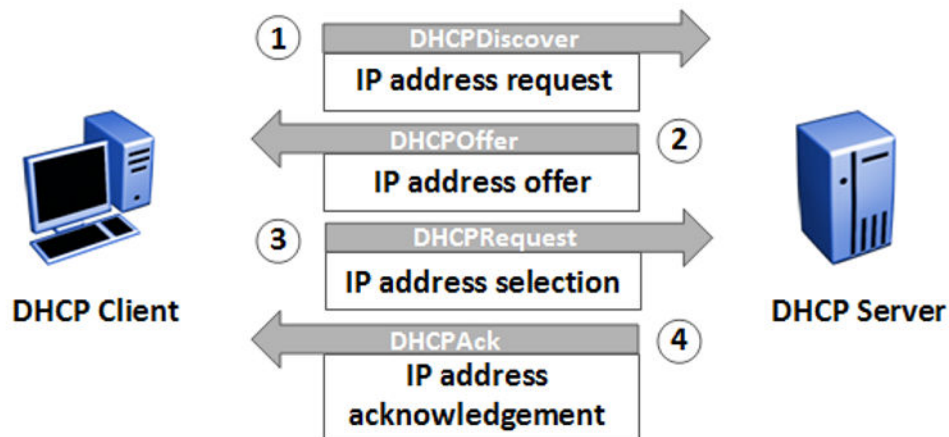


Additional configuration parameters, such as:

- a default gateway address
- Domain Name System (DNS) server addresses

You can define the information in the DHCP Server database available on your switch and the DHCP Server feature then provides it to your DHCP clients.

The following diagram illustrates the basic DHCP process.



Because DHCP Server on the switch is, by default, bound to the switch Management VLAN, the DHCP service uses the switch or stack IP.

You must also enable internal IP routing/forwarding globally on the switch and for the respective VLAN(s).

Although the switches support the configuration up to 256 VLANs, a maximum of 16 IP address pools with a maximum of 254 hosts per pool/per VLAN is supported.

Before you enable the DHCP Server, you must define at least one IP address pool with a network mask and Router (gateway) IP address.

**\* Note:**

The terms pool and scope refer to available IP addresses. While this documentation uses the term pool in most instances, you may also see the term scope used to refer to a pool of IP addresses.

For static devices like printers, you can enter MAC addresses and configure reserved IP addresses for the static devices. For example, you can specify a static IP address inside or outside an IP

address pool and enter the MAC of the device to force allocation of the same IP address to the device.

The switch supports manual configuration and entry of up to eight DNS server IP addresses. If required, the system forwards the DNS server IP address information to the DHCP Client.

You can also:

- create an IP address Pool Name that contains a maximum of 32 alpha-numeric characters
- create a maximum of 16 separate IP address Pools
- define a maximum of 8 DNS server IP addresses
- define a maximum of 8 router/gateway IP addresses
- enable either DHCP Server or DHCP Snooping, but they cannot operate simultaneously
- create a maximum of 1 IP address Pool per VLAN
- define a maximum range of 254 IP hosts per IP address Pool (~1000 per switch/stack)

When you enable DHCP Server, the default settings are:

- IP address pool based on the switch or stack Management IP address and the mask in the Management VLAN – example, if the switch or stack management address is 192.168.1.1/255.255.255.0, then pool 1 is comprised of the addresses 192.168.1.2 through 192.168.1.254 in VLAN 1
- Global switch or stack basis DHCP Server operation—the system assigns devices on all ports in the VLAN to an address pool that can participate in IP address lease assignment. You assign specified IP address lease duration to clients based on the number and type of hosts in your network to limit network congestion caused by too-frequent IP address requests
- All DHCP Server IP address pool options are set to 0—you must set each required pool option parameter manually on a per pool basis

**\* Note:**

The DHCP Server IP address pool Option-176 feature supports only IP Phones 4600 series for provisioning a number of parameters. When you create a DHCP Server IP Address Pool, Option 176 is automatically enabled with several default parameters, with the exception of the MCIPADD and TFTP Server IP address information.

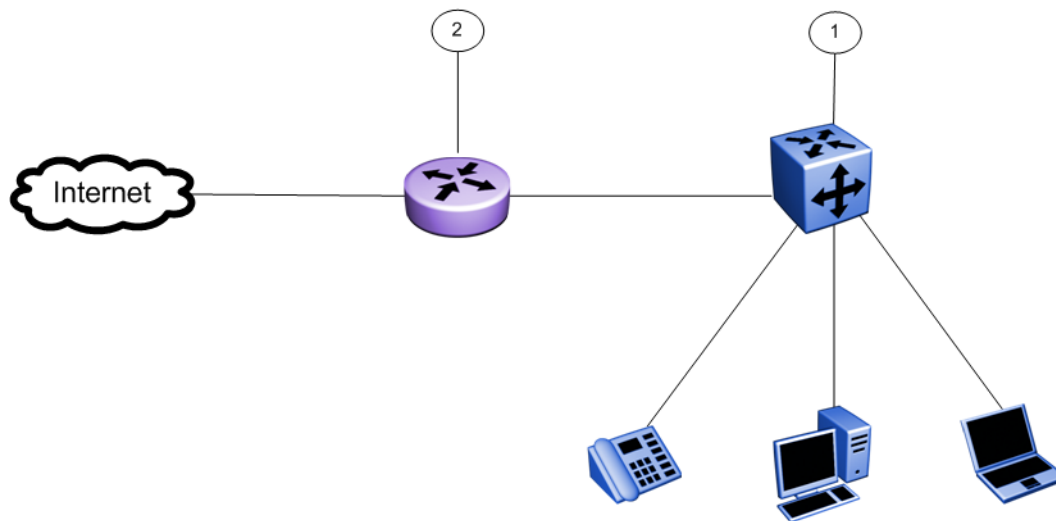
---

## DHCP Server usage examples

This section contains examples to help you use the DHCP Server feature.

### Single VLAN, single IP pool

The following example illustrates one switch with one VLAN. All switch ports and devices reside in VLAN 1, and the Management VLAN is VLAN 1.



#### Assumptions:

- Switch IP and DHCP Server IP address is 10.10.10.2/24 (Ethernet Routing Switch) callout item 1.
- DHCP server pool is 10.10.10.100 to 10.10.10.199
- Gateway IP address is 10.10.10.1/24 (router) callout item 2.
- DNS servers: 10.1.1.50 and 10.1.1.90
- Management VLAN is VLAN 1

#### \* Note:

IP multi-netting is not supported

#### CLI commands to create an IP Address pool for one VLAN:

1. Create starting and ending IP address range and mask

```
(config)# ip dhcp-server pool marketing range 10.10.10.100
10.10.10.199
```

```
(config)# ip dhcp-server pool marketing option-1 255.255.255.0
```

2. Create dhcp server options for the pool

```
(config)# ip dhcp-server pool marketing option-3 10.10.10.1
```

```
(config)# ip dhcp-server pool marketing option-6 10.1.1.50 10.1.1.90
```

3. Add other parameters to pool:

```
(config)# ip dhcp-server pool marketing option-120 10.1.2.200
```

```
(config)# ip dhcp-server pool marketing option-150 10.1.2.220
```

**4. View the configuration of the pool:**

```
(config)# show ip dhcp-server pool marketing
Start IP Address: 10.10.10.100
End IP Address: 10.10.10.199
Lease time: 86400
Subnet Mask: 255.255.255.0
DNS Servers: 10.1.1.50, 10.1.1.90
Routers: 10.10.10.1
Vendor-info:
SIP Servers: 10.1.2.200
TFTP Servers: 10.1.2.220
IP-Phones:
MCIPADD:
MCPOR: 1719
Tftpsrvr:
L2qvlan: 0
Vlantest: 60
L2qaud: 6
L2qsig: 6
```

**CLI commands to create an IP Address pool for one VLAN:**

**1. Create starting and ending IP address range and mask**

```
(config)# ip dhcp-server pool marketing range 10.10.10.100
10.10.10.199
(config)# ip dhcp-server pool marketing option-1 255.255.255.0
```

**2. Create dhcp server options for the pool**

```
config)# ip dhcp-server pool marketing option-3 10.10.10.1)
(config)# ip dhcp-server pool marketing option-6 10.1.1.50 10.1.1.90
```

**3. Add other parameters to pool:**

```
(config)# ip dhcp-server pool marketing option-120 10.1.2.200
(config)# ip dhcp-server pool marketing option-150 10.1.2.220
```

**4. View the configuration of the pool:**

```
(config)# show ip dhcp-server pool marketing
Start IP Address: 10.10.10.100
```

```
End IP Address: 10.10.10.199
Lease time: 86400
Subnet Mask: 255.255.255.0
DNS Servers: 10.1.1.50, 10.1.1.90
Routers: 10.10.10.1
Vendor-info:
SIP Servers: 10.1.2.200
TFTP Servers: 10.1.2.220
IP-Phones:
MCIPADD:
MCPORT: 1719
Tftpsrvr:
L2qvlan: 0
Vlantest: 60
L2qaud: 6
L2qsig: 6
```

#### **EDM steps to create an IP Address pool for one VLAN:**

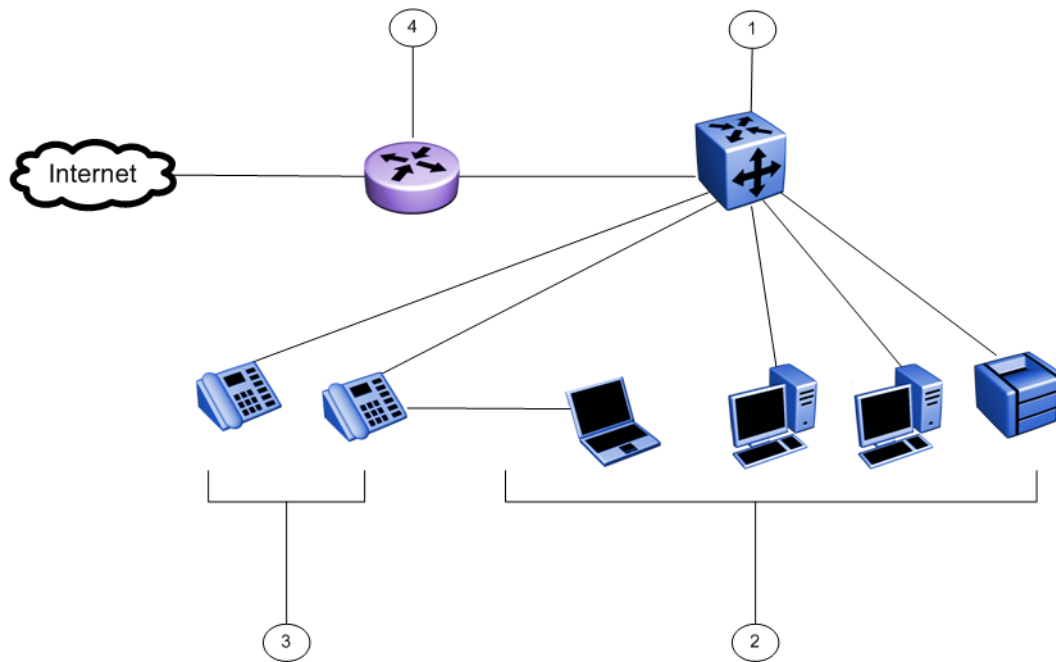
1. In the navigation tree, click **IP**.
2. In the IP tree, click **DHCP Server**.
3. Click the **DHCP Server Pool** tab.
4. On the toolbar, click **Insert**.
5. On the **Insert DHCP Server Pool** pane, enter the values to configure a pool.
6. Click **Insert** to add the DHCP Server pool and return to the DHCP Server Pool tab.
7. On the **DHCP Server Pool** toolbar, click **Refresh** to display the new DHCP Server Pool.

#### **Two VLANs, two IP pools**

In this example, there is one switch with two VLANs:

- VLAN 1 "DATA" - PC and printer devices (management VLAN)
- VLAN 2 "VOICE" – IP Phones

Following is a simple IP Office style example of the DHCP server function serving host PCs and IP Phones.



Assumptions:

- Switch IP and DHCP Server IP address is 10.10.10.5/24 (in management VLAN) on Ethernet Routing Switch , callout item 1
- DHCP server pools: DATA - 10.10.10.100 to 10.10.10.199 , callout item 2, VOICE – 10.10.20.100 to 10.10.20.220 , callout item 3.
- Gateway IP: 10.10.10.1/24 (router), callout item 4.
- DNS servers: 10.1.1.50 and 10.1.1.90
- Management VLAN: VLAN 1

**\* Note:**

IP multi-netting is not supported

**CLI commands to create two IP Address pools for two or more VLANs :**

1. Create second VLAN and add ports to VLAN-2:

```
(config)# vlan create 2 type port  
(config)# vlan members 2 <port-list>
```

2. Add IP gateway for VLAN-2 and globally enable routing (subnet 10.10.20.0/24):

```
(config)# interface vlan 2  
(config-if)# ip address 10.10.20.1 255.255.255.0  
(config)# ip routing
```

### 3. Create starting and ending IP address range and mask for 2 IP Pools:

```
(config)# ip dhcp-server pool marketing range 10.10.10.100
10.10.10.199
```

```
(config)# ip dhcp-server pool marketing option-1 255.255.255.0
```

```
(config)# ip dhcp-server pool sales range 10.10.20.100 10.10.20.220
```

```
(config)# ip dhcp-server pool sales option-1 255.255.255.0
```

### 4. Create DHCP Server options for the pool

```
(config)# ip dhcp-server pool marketing option-3 10.10.10.1
```

```
(config)# ip dhcp-server pool marketing option-6 10.1.1.50 10.1.1.90
```

```
(config)# ip dhcp-server pool sales option-3 10.10.20.1
```

```
(config)# ip dhcp-server pool sales option-6 10.1.1.50 10.1.1.90
```

### 5. Optionally configure any additional DHCP server Pool options:

```
(config)# ip dhcp-server pool marketing option-120 10.1.2.200
```

```
(config)# ip dhcp-server pool marketing option-150 10.1.2.220
```

### 6. Enable the embedded DHCP Server:

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

To support additional IP Pools, repeat these steps to add more

- VLANs
- Ports
- Gateway IP & routing for VLANs
- DHCP Pools for the corresponding IP subnet in the VLANs

### EDM steps to create two IP Address pools for two or more VLANs:

Create a second DHCP Server Pool :

1. In the navigation tree, click **IP**.
2. In the IP tree, click **DHCP Server**.
3. Click the **DHCP Server Pool** tab.
4. On the toolbar, click **Insert**.
5. On the **Insert DHCP Server Pool** pane, enter the values to configure a pool.
6. Click **Insert** to add the DHCP Server pool and return to the DHCP Server Pool tab.
7. On the **DHCP Server Pool** toolbar, click **Refresh** to display the new DHCP Server Pool.

Create a second VLAN, add ports, create an IP gateway for VLAN, and enable routing:

1. From the navigation tree, click **VLAN**.
2. Click **VLANs**.
3. In the work area, click the **Basic** tab.

4. On the toolbar, click **Insert**.
5. Do one of the following:
  - a. In the **Id** field, type a value.
  - b. Accept the default ID for the VLAN.
6. Do one of the following:
  - a. In the **Name** field, type a value.
  - b. Accept the default name for the VLAN.
7. In the **Type** field, select **byPort**.
8. Click **Insert**.
9. In the VLAN row, double-click the cell in the **PortMembers** column.
10. Select ports to add to the VLAN.
11. Click **Ok**.
12. In the VLAN row, double-click the cell in the **Routing** column.
13. Select **true** to enable routing for the VLAN.
14. Click **Apply**.
15. In the work area, select the newly created VLAN.
16. On the toolbar, click **IP**.

The IP, VLAN dialog box appears with the IP Address tab selected.
17. On the toolbar, click **Insert**.

The Insert IP Address dialog box appears.
18. Type the IP address, subnet mask, and MAC address offset in the fields provided.
19. Click **Insert**.

Enable Global IP routing/forwarding:

1. From the navigation tree, click **IP**.
2. In the IP tree, click **IP**.
3. In the **Forwarding** box, select the option to enable routing.
4. Click **Apply**.

 **Note:**

Because the DHCP Server is embedded in the switch, it is not necessary to configure DHCP relay information when configuring multiple DHCP pools for multiple VLANs. DHCP requests will be received on any directly connected VLAN when a gateway IP address is configured and routing is enabled for that VLAN.

### How to use Option 176 for IP Phones 4600 Series

Option-176 provides provisioning of basic IP phone features to IP Phones 4600 Series.



When you create an IP address pool, option-176 is automatically enabled with default values for the following parameters:

- MCPORT (1719)
- L2qvlan (0)
- l2qaud (6)
- l2qsig (6)
- Vlantest (60)

Two other parameters, MCIPADD and TFTP server, are blank by default and, if you require option-176 capabilities, you must configure them.

Following is an CLI configuration example of a DHCP Server IP Pool with provisioning support for IP Phones 4600 Series.

### Configuring IP address information for option-176 using CLI:

Assumption: A DHCP Server Pool called Marketing exists.

1. Configure IP address information for option-176.

```
(config)# ip dhcp-server pool marketing option-176 mcipadd
10.10.200.95

(config)# ip dhcp-server pool marketing option-176 tftp-servers
10.10.200.98
```

2. Optional—Change mcport number and L2qvlan parameters for option-176

```
(config)# ip dhcp-server pool marketing option-176 mcport 9200
(config)# ip dhcp-server pool marketing option-176 l2qvlan 2
```

3. Display pool configuration for “marketing”.

```
(config)# show ip dhcp-server pool
Pool: marketing
Start IP address: 10.10.10.100
End IP address: 10.10.10.199
Lease time: 86400
Subnet Mask: 255.255.255.0
DNS Servers:
Routers: 10.10.10.1
Vendor-info:
SIP Servers:
TFTP Servers:
IP-Phones:
MCIPADD: 10.10.200.95
MCPORT: 9200
```

```
Tftpsrvr: 10.10.200.98
L2qvlan: 2
Vlantest: 60
L2qaud: 6
L2qsig: 6
```

To configure Option 176 for IP Phones using EDM, see [Configuring DHCP Server Pool Options EDM](#) on page 156.

## How to use Option 241 for IP phones

You can provide Voice VLAN information to IP Phones 1100, 1200 and 2000 Series using DHCP options assigned to the data VLAN as well as extended options.

The IP Phone options are defined as a string and contain parameters and values separated by semicolons. For option 241, only the Nortel specific option of **Nortel-i2004-B** will be supported. As one or more parameters are defined for this option, they are appended to the **Nortel-i2004-B** specific option. You can also remove specific parameters from an existing string. When adding or removing parameters, the use of **Nortel-i2004-B** specific option at the beginning of the string is optional.

Although all specified parameters are supported, the maximum option length of the Option 241 string is 255 characters. The input string for option 241 is validated to verify the parameters from the string are valid, however, there is no check for their values, or whether a specific parameter is entered more than once in the same command.

A parameter is considered to be the value between the equals sign and semicolon from the input string. You will receive an error message if an invalid parameter is found in the input string. For a list of the supported parameters, see [DHCP Server Option 241 parameters](#) on page 91.

Following is an CLI configuration example of a DHCP Server IP Pool with provisioning support for IP Phones 1100, 1200, and 2000 Series.

### Configuring IP address information for option-241 using CLI:

Assumption: A DHCP Server Pool called Marketing exists.

1. Configure IP address information for option-241

```
(config)# ip dhcp-server pool marketing option-241 Nortel-i2004-B,slip=47.11.62.20;p1=4100;a1=1;r1=255;
```

Note: When adding parameters, the format for the parameter list is: Nortel-i2004-B,param1=value;param2=value2;param3=value3;...

2. Optional—Remove individual parameters s2ip and p2 for option-241

```
(config)# no ip dhcp-server pool marketing option-241 s2ip,p2
```

Note: When removing parameters, the format for the parameter list is: Nortel-i2004-B,param1,param2,param3,...

To configure Option 241 for IP Phones using EDM, see [Configuring DHCP Server Pool Options EDM](#) on page 156.

## How to use Option 242 for IP Phones

The embedded DHCP Server for this option supports the configuration and provisioning of selected parameters for IP Phones 1600 and 9600 Series.

The following parameters are supported:

- HTTPPORT
- HTTPSRVR
- MCIPADD

When DHCP Server Option 242 is enabled for a specific IP pool, note the following default values:

- HTTPPORT (default port = 80)
- HTTPSRVR (default IP address = blank) — up to eight (8) IP addresses are supported in the configuration of this parameter
- MCIPADD (default IP address = blank) — up to eight (8) Call Server IP addresses are supported in the configuration of this parameter. This is used as a backup for the IP phone in case the HTTP Server is unavailable, in which case the IP phone can reach the Call Server.

Following is an CLI configuration example of a DHCP Server IP Pool with provisioning support for IP Phones 1600 and 9600 Series.

### Configuring IP address information for option-242 using CLI:

Assumption: A DHCP Server Pool called Marketing exists.

1. Configure IP address information for option-242

```
(config)# ip dhcp-server pool marketing option-242 mcipadd
10.10.200.95
```

```
(config)# ip dhcp-server pool marketing option-242 httpsrvr
10.10.200.98
```

To configure Option 242 for IP Phones using EDM, see [Configuring DHCP Server Pool Options EDM](#) on page 156.

---

## Related routing features

The following sections describe features that are related to and dependent on the IP routing functionality.

---

### BootP DHCP relay

Dynamic Host Configuration Protocol (DHCP) is a mechanism to assign network IP addresses on a dynamic basis to clients who request an address. DHCP is an extension of the Bootstrap protocol (BootP). BootP/DHCP clients (workstations) generally use User Datagram Protocol (UDP) broadcasts to determine their IP addresses and configuration information. If such a host is on a

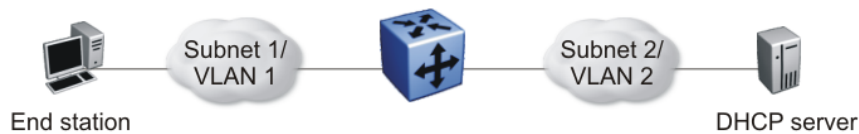
VLAN that does not include a DHCP server, the UDP broadcasts are by default not forwarded to servers located on different VLANs.

The switch can resolve this issue using DHCP relay by forwarding the DHCP broadcasts to the IP address of the DHCP server. Network managers prefer to configure a small number of DHCP servers in a central location to lower administrative overhead. Routers must support DHCP relay so that hosts can access configuration information from servers several router hops away.

With DHCP relay enabled, the switch can relay client requests to DHCP servers on different Layer 3 VLANs or in remote networks. It also relays server replies back to the clients.

To relay DHCP messages, you must create two Layer 3 VLANs: one connected to the client and the other providing a path to the DHCP server. You can enable DHCP relay on a per-VLAN basis.

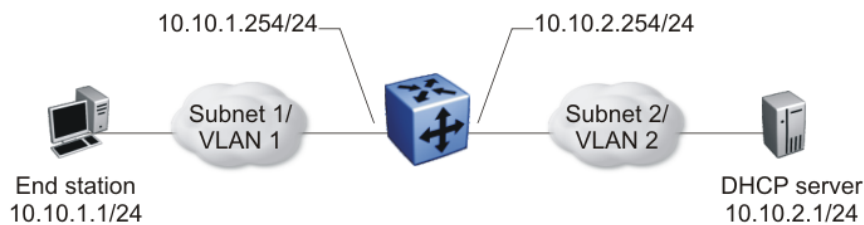
The following figure shows a DHCP relay example, with an end station connected to subnet 1, corresponding to VLAN 1. The switch connects two subnets by means of the virtual routing function. When the end station generates a DHCP request as a limited UDP broadcast to the IP address of all 1s (that is, 255.255.255.255), with the DHCP relay function enabled, the switch forwards the DHCP request to the host address of the DHCP server on VLAN 2.



**Figure 5: DHCP relay operation**

## Forwarding DHCP packets

In the following figure, the DHCP relay agent address is 10.10.1.254. To configure the switch to forward DHCP packets from the end station to the server, use 10.10.2.1 as the server address.



**Figure 6: Forwarding DHCP packets**

All BootP and DHCP broadcast packets that appear on the VLAN 1 router interface (10.10.1.254) are then forwarded to the DHCP server. In this case, the DHCP packets are forwarded as unicast to the DHCP server IP address.

## Differences between DHCP and BootP

With DHCP relay, the switch supports the relay of DHCP and the Bootstrap protocol (BootP). The following differences between DHCP and BootP are specified in RFC 2131:

- BootP enables the retrieval of an American Standard Code for Information Interchange (ASCII) configuration file name and configuration server address.
- A properly configured BootP server enables the switch to automatically learn its assigned IP address, subnet mask, and the IP address of the default router (default gateway).
- DHCP defines mechanisms through which clients can be assigned a network address for a finite lease (allowing for reuse of IP addresses).
- DHCP provides the mechanism for clients to acquire all of the IP configuration parameters they need to operate.

DHCP uses the BootP message format defined in RFC 951. The remainder of the options field consists of a list of tagged parameters that are called options (RFC 2131).

---

## DHCP option 82 support

DHCP option 82 support is an extension of Dynamic Host Configuration Protocol (RFC3046 and RFC3993) that enables the switch to send information about DHCP clients to the authenticating DHCP server. When you enable option 82, in either Layer 2 or Layer 3 mode, the switch inserts additional port-based identification information into the DHCP packets traversing the switch enroute to the DHCP server. The DHCP server stores this additional identification information within the IP allocation record to assist in tracking of end device locations; for example, to provide location-based information for emergency services applications.

When a VLAN is operating in Layer 2 mode, DHCP Snooping must be enabled for DHCP Option 82 to function, both globally and on each client VLAN. For more information about DHCP Snooping, see *Configuring Security on Ethernet Routing Switch 3500 Series*.

When a VLAN is operating in Layer 3 (IP Routing) mode, the DHCP Option 82 function requires that DHCP Relay is appropriately configured. To use DHCP Option 82 with DHCP relay, you must enable DHCP relay globally on the switch and client VLANs. And you must configure at least one forward path.

If you configure two DHCP Servers (one in the same VLAN with the DHCP Client and one in another VLAN) and you enable both DHCP Snooping Option 82 and DHCP Relay Option 82, the system adds the option for both servers.

### DHCP Relay Packet Size

In accordance with RFC3046, you can specify the maximum frame size the DHCP relay agent can forward to the DHCP server. While the switch implementation permits configuration of the maximum DHCP packet size up to 1536 bytes, the default maximum size is 576 bytes. If the DHCP frame received is larger than the configured frame size, the switch does not relay the packet. If the DHCP packet exceeds the maximum configured size, the DHCP Option 82 information is not appended to the message.

## UDP broadcast forwarding

By default, User Datagram Protocol (UDP) broadcast frames received on one VLAN are not routed to another VLAN. To allow UDP broadcasts to reach a remote server, the Ethernet Routing Switch supports UDP broadcast forwarding, which forwards the broadcasts to the server through a Layer 3 VLAN interface.

UDP broadcast forwarding is a general mechanism for selectively forwarding limited UDP broadcasts received on an IP interface to a configured IP address. The packet is sent as a unicast packet to the server.

When a UDP broadcast is received on a router interface, it must meet the following criteria to be considered for forwarding:

- It must be a MAC-level broadcast.
- It must be an IP-limited broadcast.
- It must be for a configured UDP protocol.
- It must have a time-to-live (TTL) value of at least 2.

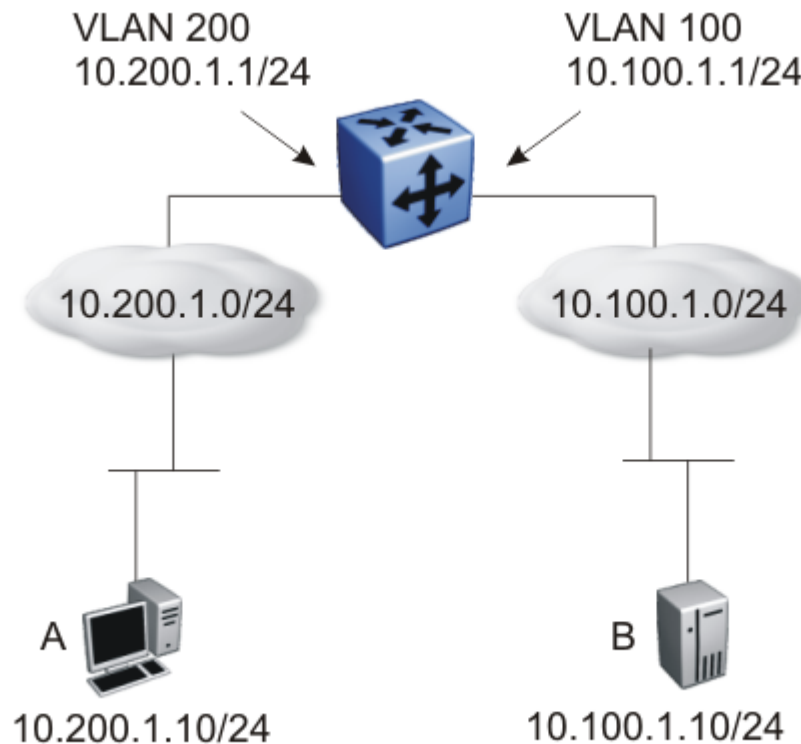
For each ingress interface and protocol, the UDP broadcast packets are forwarded only to a unicast host address (for example, to the unicast IP address of the server).

When the UDP forwarding feature is enabled, a filter is installed that compares the UDP destination port of all packets against all the configured UDP forwarding entries. If a match occurs, the destination IP of the incoming packet is checked for consistency with the userconfigured broadcast mask value for this source VLAN. If these conditions are met, the TTL field from the incoming packet is overwritten with the user-configured TTL value, the destination IP of the packet is overwritten with the configured destination IP, and the packet is routed to the destination as a unicast frame.

## UDP forwarding example

The following figure shows an example of UDP broadcast forwarding. In this case, if host A (10.200.1.10) needs a certain service (for example, a custom application that listens on UDP port 12345), it transmits a UDP broadcast frame. By default, the Ethernet Routing Switch does not forward this frame to VLAN 100, and because server B (10.100.1.10) is not on VLAN 200, the host cannot access that service.

With UDP broadcast forwarding enabled, the host can access the service. In this case, you must list port 12345 as a valid forwarding port, and specify VLAN 200 as the source VLAN.



**Figure 7: UDP forwarding example**

When the switch receives an incoming packet on VLAN 200 that matches the configured UDP destination port (12345), and the destination IP is consistent with the broadcast mask value for the VLAN, then the switch applies the new destination IP (here, 10.100.1.10) to the packet and routes it to the destination as a unicast frame.

## Directed broadcasts

With the directed broadcasts feature enabled, the Ethernet Routing Switch can determine if an incoming unicast frame is a directed broadcast for one of its interfaces. If so, the switch forwards the datagram onto the appropriate network using a link-layer broadcast.

With IP directed broadcasting enabled on a VLAN, the Ethernet Routing Switch forwards direct broadcast packets in the following two ways:

- through a connected VLAN subnet to another connected VLAN subnet
- through a remote VLAN subnet to the connected VLAN subnet

This feature is disabled by default.

## ARP

The Address Resolution Protocol (ARP) allows the Ethernet Routing Switch to dynamically learn Layer 2 Media Access Control (MAC) addresses, and to build a table with corresponding Layer 3 IP addresses.

Network stations using the IP protocol need both a physical (MAC) address and an IP address to transmit a packet. If a network station knows only the IP address of a network host, ARP enables the network station to determine the physical address of the network host and bind the 32-bit IP address to a 48-bit MAC address. A network station can use ARP across a single network only, and the network hardware must support physical broadcasts.

If a network station wants to send a packet to a host but knows only the host IP address, the network station uses ARP to determine the physical address of the host as follows:

1. The network station broadcasts a special packet, called an ARP request, that asks the host at the specified IP address to respond with its physical address.
2. All network hosts receive the broadcast message.
3. Only the specified host responds with its hardware address.
4. The network station then maps the host IP address to its physical address and saves the results in an address resolution table for future use.
5. The network station ARP table displays the association of the known MAC addresses to IP addresses.

The lifetime for the learned MAC addresses is a configurable parameter. The switch executes ARP lookups after this timer expires.

The default timeout value for ARP entries is 6 hours.

---

## Static ARP

In addition to the dynamic ARP mechanism, the Ethernet Routing Switch supports a static mechanism that allows for static ARP entries to be added. With Static ARP, you can manually associate a device MAC address to an IP address. You can add and delete individual static ARP entries on the switch.

---

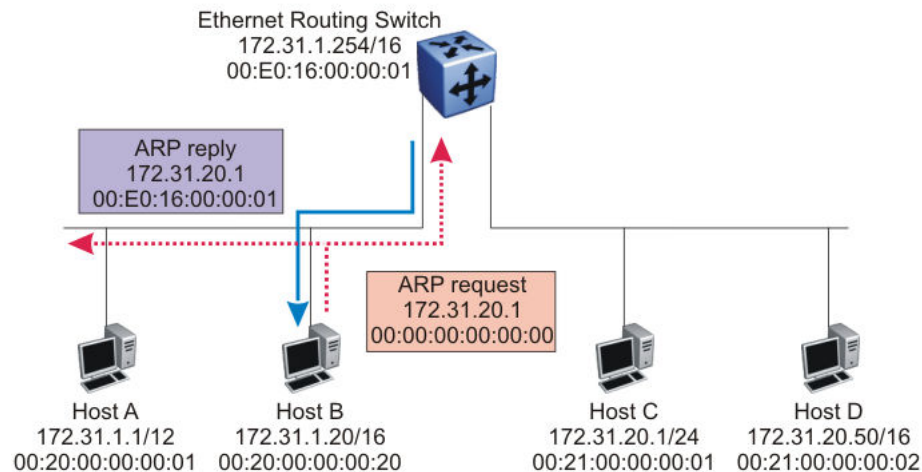
## Proxy ARP

Proxy ARP allows the switch to respond to an ARP request from a locally attached host that is intended for a remote destination. It does so by sending an ARP response back to the local host with the MAC address of the switch interface that is connected to the host subnet. The reply is generated only if the switch has an active route to the destination network.

With Proxy ARP enabled, the connected host can reach remote subnets without the need to configure default gateways.



The following figure is an example of proxy ARP operation. In this example, host B wants to send traffic to host C, so host B sends an ARP request for host C. However, the switch is between the two hosts so the ARP message does not reach host C. To enable communication between the two hosts, the switch intercepts the message and responds to the ARP request with the IP address of host C but with the MAC address of the switch itself. Host B then updates its ARP table with the received information.



**Figure 8: Proxy ARP Operation**

It is recommended to use Proxy ARP as a temporary fix only, for example, if you are gradually moving hosts from one addressing scheme to another and you still want to maintain connectivity between the disparately-addressed devices. You do not want Proxy ARP running as a general rule because it causes hosts to generate ARP messages for every address that they want to reach on the Internet.

## IP blocking for stacks

IP blocking is a Layer 3 feature that provides safeguards for a stack where Layer 3 VLANs have port members across multiple stack units. IP blocking is used whenever a unit leaves a stack or is rebooting inside the context of a stack. Depending on the setting in use, Layer 3 functionality is either continued or blocked by this feature.

You can set the IP Blocking mode on the base unit to either none or full.

When IP blocking is set to full, if any units leave the stack, those units run in Layer 2 mode. No Layer 3 settings remain active on the units.

When IP blocking is set to none, if any units leave the stack, the Layer 3 configurations applied to the stack are still applied on the individual units.

In a stack environment of 2 units, use IP blocking mode none. In this case, you can expect the following functional characteristics:

- If either the stack base unit or non-base unit becomes non-operational, Layer 3 functionality continues to run on the remaining unit.

A disadvantage of this configuration is that if the non-operational unit does not rejoin the stack, address duplication occurs.

In stack environments of more than 2 units, use IP blocking mode full. In this case, you can expect the following functional characteristics:

- If the stack base unit becomes non-operational, the following occurs:
  - The temporary base unit takes over base unit duties.
  - The temporary base unit takes over responsibility to manage Layer 3 functionality in the stack. When this occurs, the system updates the MAC addresses associated with each routing interface to be offset from the temporary base unit MAC address (rather than the base unit MAC address). During this period, some minor disruption may occur to routing traffic until end stations update their ARP cache with the new router MAC addresses. The switch sends out gratuitous ARP messages on each routed VLAN for 5 minutes at 15 second intervals to facilitate quick failover in this instance.
  - If the non-operational base unit does not rejoin the stack, no Layer 3 functionality runs on the unit.
- If a stack non-base unit becomes non-operational, the following occurs:
  - The stack continues to run normally with the base unit controlling Layer 3 functionality.
  - If the non-operational non-base unit does not rejoin the stack, no Layer 3 functionality runs on the unit.

By default, the IP blocking mode is none (disabled).

To configure IP blocking, see [Configuring IP blocking for a stack](#) on page 115.

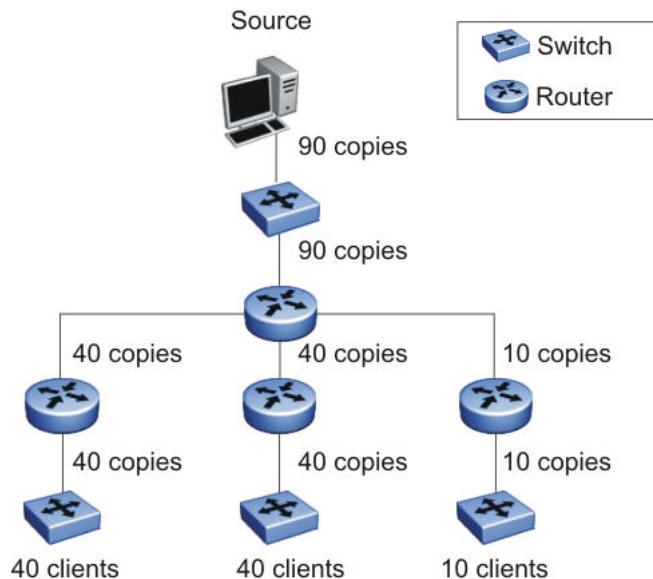
# Chapter 5: IGMP fundamentals

This chapter provides an overview of IP multicast and Internet Group Management Protocol (IGMP). To support multicast traffic, the switch provides support for IGMP snooping.

---

## Overview of IP multicast

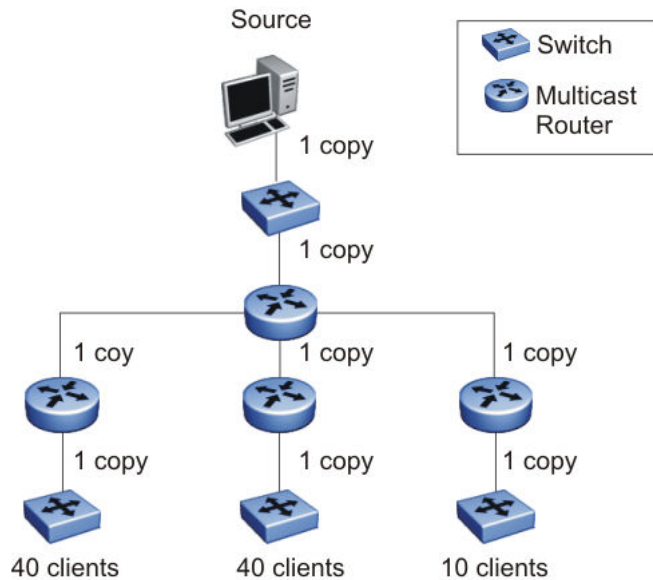
Most traditional network applications such as Web browsers and e-mail employ unicast connections in which each client sets up a separate connection to a server to access specific data. However, with certain applications such as audio and video streaming, more than one client accesses the same data at the same time. With these applications, if the server sends the same data to each individual client using unicast connections, the multiple connections waste both server and network capacity. For example, if a server offers a 1 Mbit/sec live video stream for each client, a 100 Mbit/sec network interface card (NIC) on the server could be completely saturated after 90 client connections. The following figure shows an example of this waste of resources.



**Figure 9: Wasteful propagation of multiple copies of the same unicast stream**

Multicasting provides the ability to transmit only one stream of data to all the interested clients at the same time. The following figure shows a simple example of how multicasting works. The source of the multicast data forwards only one stream to the nearest downstream router, and each

subsequent downstream router forwards a copy of the same data stream to the recipients who are registered to receive it.



**Figure 10: One stream replicated using multicasting**

This one-to-many delivery mechanism is similar to broadcasting except that, while broadcasting transmits to all hosts in a network, multicasting transmits only to registered host groups. Because multicast applications transmit only one stream of data, which is then replicated to many receivers, multicasting saves a considerable amount of bandwidth.

Clients that want to receive the stream must register with the nearest multicast router to become a part of the receiving multicast group.

One downside to multicasting is that the multicast streams transmit data using User Datagram Protocol (UDP) packets, which are not as reliable as Transmission Control Protocol (TCP) packets.

Applications that use multicasting to transmit data include the following:

- multimedia conferencing
- real-time data multicasts (such as stock tickers)
- gaming and simulations

---

## Multicast groups

To receive a multicast stream from a particular source, hosts must register with the nearest multicast router. The router adds all interested hosts to a multicast group, which is identified by a multicast IP address.

Multicast routers use Internet Group Membership Protocol (IGMP) to learn the existence of host group members on their directly attached subnets. To identify the hosts that want to be added to a

group, the querier router sends out IGMP queries to each local network. A host that wants to belong to the group sends a response in the form of an IGMP membership report.

Each multicast router maintains a multicast routing table that lists each source, group (S,G) pair, which identifies the IP address of the source and the multicast address of the receiving group. For each (S,G) pair, the router maintains a list of downstream forwarding ports to which the multicast traffic is forwarded, and the upstream port where the multicast traffic is received.

---

## Multicast addresses

Each multicast host group is assigned a unique multicast address. To reach all members of the group, a sender uses the multicast address as the destination address of the datagram.

An IP version 4 multicast address is a Class D address (the high-order bits are set to 1110) from 224.0.1.0 to 239.255.255.255. These addresses are assigned statically for use by permanent groups and dynamically for use by transient groups.

You cannot use 24-bit subnets, such as 224.0.0.0/24 and 224.128.0.0/24 for multicast data traffic. This restriction applies to the entire multicast address range from 224.0.0.0/8 to 239.128.0.0/8.

---

## IGMP overview

IGMP is the Layer 3 protocol used by IP multicast routers to learn the existence of multicast group members on their directly attached subnets (see RFC 2236). With IGMP, hosts can register their desired group memberships to their local querier router. A multicast querier router communicates with hosts on a local network by sending IGMP queries. The router periodically sends a general query message to each local network of the router.

A host that wants to join a multicast group sends a response in the form of a membership report requesting registration with a group. After the querier router registers hosts to a group, it forwards all incoming multicast group packets to the registered host networks. As long as any host on a subnet continues to participate in the group, all hosts, including nonparticipating end stations on that subnet, receive the IP Multicast stream.

IGMP versions are backward compatible and can all exist together on a multicast network.

The following sections provide more details about the differences between the different IGMP versions.

---

## IGMPv1 operation

IGMP version 1 is the simplest of the IGMP versions and is widely deployed.

IGMPv1 supports the following two message types:

- 0x11 – Membership Query message. Packets are sent to the all-systems multicast group (224.0.0.1).
- 0x12 – Membership Report message. Packets are sent to the group that the host intends to join.

The IGMPv1 router periodically sends host membership queries (also known as general queries) to its attached local subnets to inquire if any hosts are interested in joining any multicast groups. The interval between queries is a configurable value on the router. A host that wants to join a multicast group sends a membership report message to the nearest router, one report for each joined multicast group. After receiving the report, the router adds the Multicast IP address and the host port to its forwarding table. The router then forwards any multicast traffic for that multicast IP address to all member ports.

The router keeps a list of multicast group memberships for each attached network, and a Group Membership Interval timer for each membership. Repeated IGMP membership reports refresh the timer. If no reports are received before the timer expires, the router sends a query message.

In some cases, the host does not wait for a query before it sends report messages to the router. Upon initialization, the host can immediately issue a report for each of the multicast groups that it supports. The router accepts and processes these asynchronous reports the same way it accepts requested reports.

## IGMPv1 leave process

After hosts and routers are in a steady state, they communicate in a way that minimizes the exchange of queries and reports. The designated routers set up a path between the IP Multicast stream source and the end stations, and periodically query the end stations to determine whether they want to continue to participate. As long as any host on the subnet continues to participate, all hosts, including nonparticipating end stations on the subnet, receive the IP Multicast stream.

If all hosts on the subnet leave the group, the router continues to send general queries to the subnet. If no hosts send reports after three consecutive queries, the router determines that no group members are present on the subnet.

---

## IGMPv2 operation

IGMPv2 extends the IGMPv1 features by implementing a host leave message to quickly report group membership termination to the routing protocol. Instead of routers sending multiple queries before determining that hosts have left a group, the hosts can send a leave message. This feature is important for multicast groups with highly volatile group membership.

The IGMPv2 join process is similar to the IGMPv1 join process.

IGMPv2 also implements a querier election process.

IGMPv2 adds support for the following three new message types:

- 0x11 – General Query and Group Specific Query message.

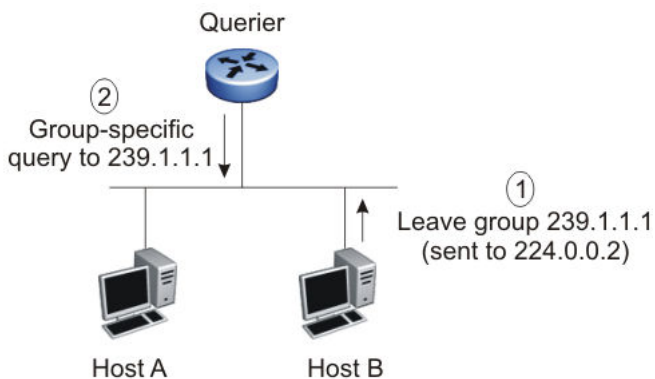
- 0x16 – Version 2 Membership Report (sent to the destination IP address of the group being reported)
- 0x17 – Version 2 Membership Leave message (sent to all-router [224.0.0.2] multicast address)

IGMPv2 also supports IGMPv1 messages.

## Host leave process

With IGMPv2, if the host that issued the most recent report leaves a group, the host issues a leave message. The multicast router on the network then issues a group-specific query to determine whether other group members are present on the network. In the group-specific query message, the Group Address field is the group being queried (the Group Address field is 0 for the General Query message). If no host responds to the query, the router determines that no members belonging to that group exist on that interface.

The following figure shows an example of how IGMPv2 works.



**Figure 11: IGMPv2**

In this example, the following occurs:

- The host sends a leave message (to 224.0.0.2).
- The router sends a group-specific query to group 239.1.1.1.
- No IGMP report is received.
- Group 239.1.1.1 times out.

## Querier election process

Normally only one querier exists for each subnet. When multiple IGMPv2 routers are present on a network, the router with the lowest IP address is elected to send queries. All multicast routers start up as a querier on each attached network. If a multicast router receives a query message from a router with a lower IP address, the router with the higher IP address becomes a nonquerier on that network.

---

## IGMPv3 operation

IGMPv3 adds support for source filtering. The IGMPv3 host can report its interest in receiving multicast packets from only specific source addresses, or the host can report its interest in receiving multicast packets from all but specific source addresses.

IGMPv3 is mostly used in voice and video conferences where multiple people can be part of the same conference. The IGMPv3 packet format adds a v3 Report message type (0x22) and includes Source-and-Group-specific Query messages.

The message type for Source-and-Group-specific Query message is 0x11, the same as IGMPv1 and IGMPv2. The different Query message versions are identified as follows:

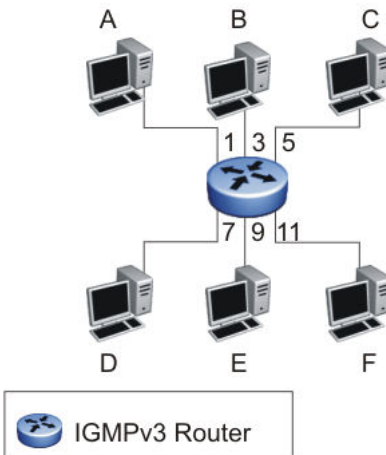
- If the size of the IGMP message type is 8, then it is a v1 or v2 Query message.
- If the Group Address field is 0, then it is a General Query.
- If the Group Address field is a valid multicast IP address, then it is a Group-specific Query.
- If the Group Address field is a valid address and the Number of Sources field is nonzero, then it is a Group-and-Source specific Query message.

Each IGMPv3 Report contains a list of group records. The Group Record contains the multicast group address and the list of source addresses. The record type field specifies whether to INCLUDE or EXCLUDE the list of source addresses that are provided in the Source Address field. For example, to include packets from source 10.10.10.1, the report contains an INCLUDE(10.10.10.1) record.

The list of source addresses can be empty, which is represented by braces ({}), which means either to INCLUDE or EXCLUDE none. For example, the host that wants to receive packets from all group members can send a report with an EXCLUDE({}) record and a host that wants to leave a group can send a report with an INCLUDE({}) record, which is similar to a leave message.

In the following figure, hosts A, B, C, D, E, and F are part of a conference group G1. All hosts except F send a report for group G1 with the mode as INCLUDE(A, B, C, D, E, F) containing all the source addresses. Host F, which is not interested in listening to C and D, sends a report to group G1 with the mode as EXCLUDE(C, D).





**Figure 12: IGMPv3**

The router adds the multicast IP address and the list of sources in the forwarding table. The router forwards the packets from A, B, E, and F to all ports. If the packets are received from C and D, it is forwarded to all ports except port 11.

---

## IGMP requests for comment

For additional information about IGMP, see the following requests for comment (RFC):

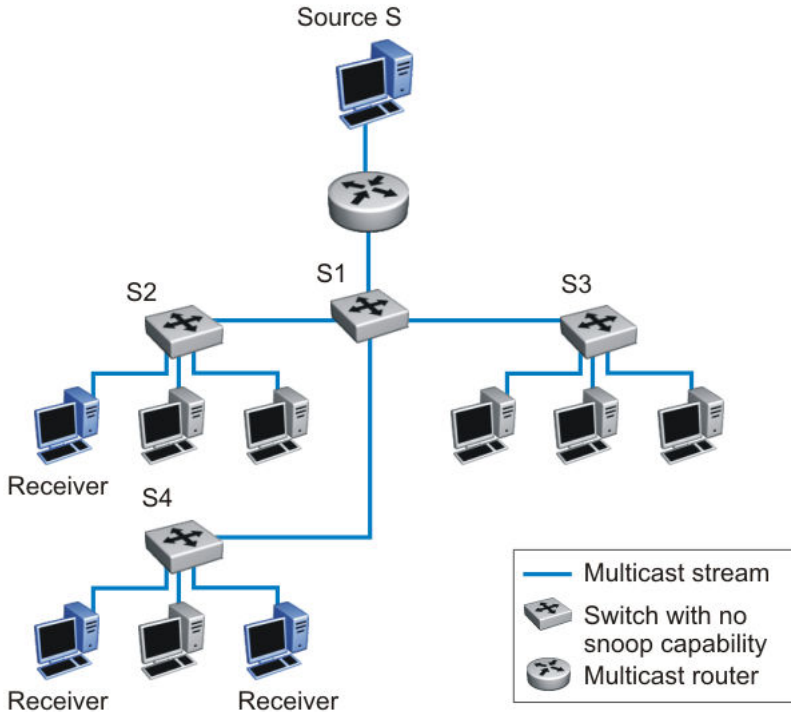
- For IGMPv1, see RFC 1112.
- For IGMPv2, see RFC 2236.
- For IGMPv3, see RFC 3376
- For IGMP snooping, see RFC 4541.
- For IGMP management information bases (MIB), see RFC 2933.

---

## IGMP snooping

If at least one host on a VLAN specifies that it is a member of a group, by default, the switch forwards to that VLAN all datagrams bearing the multicast address of that group. All ports on the VLAN receive the traffic for that group.

The following figure shows an example of this scenario. Here, the IGMP source provides an IP Multicast stream to a designated router. Because the local network contains receivers, the designated router forwards the IP Multicast stream to the network. Switches without IGMP snoop enabled flood the IP Multicast traffic to all segments on the local subnet. The receivers requesting the traffic receive the desired stream, but so do all other hosts on the network. Although the nonparticipating end stations can filter the IP Multicast traffic, the IP Multicast traffic still exists on the subnet and consumes bandwidth.

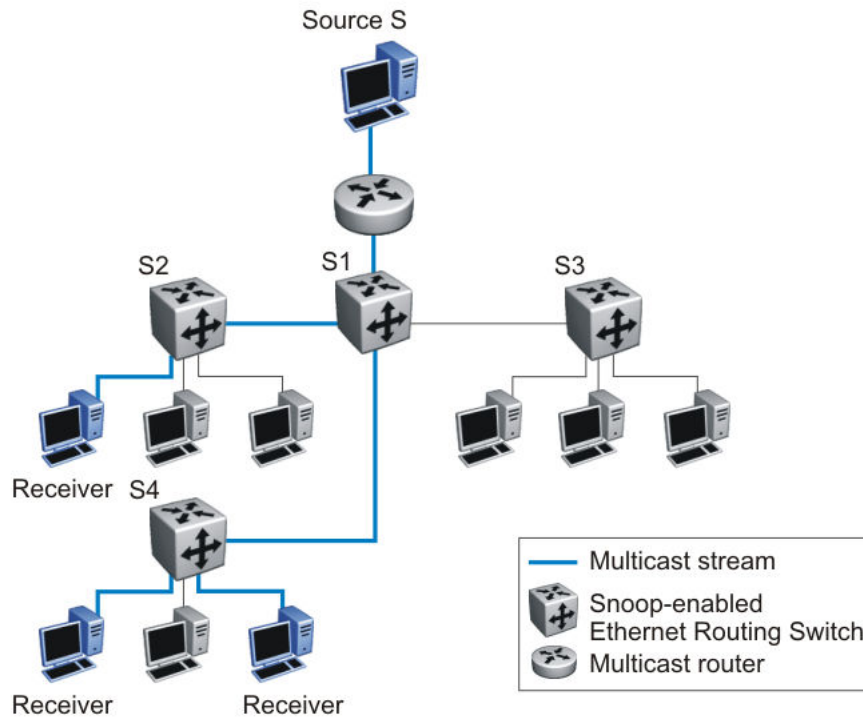


**Figure 13: IP multicast propagation on a LAN without IGMP snooping**

To prune ports that are not group members from receiving the group data, the switch supports IGMP snoop for IGMPv1, IGMPv2, and IGMPv3. With IGMP snoop enabled on a VLAN, the switch forwards the multicast group data to only those ports that are members of the group. When using IGMP snoop, VLANs can provide the same benefit as IP Multicast routers, but in the local area.

The switch identifies multicast group members by listening to IGMP packets (IGMP reports, leaves, and queries) from each port. The switch suppresses the reports by not forwarding them out to other VLAN ports, forcing the members to continuously send their own reports. The switch uses the information gathered from the reports to build a list of group members. After the group members are identified, the switch blocks the IP Multicast stream from exiting any port that does not connect to a group member, thus conserving bandwidth.

As shown in the following figure, after the switches learn which ports are requesting access to the IP Multicast stream, all other ports not responding to the queries are blocked from receiving the IP Multicast data.



**Figure 14: Ethernet Routing Switch running IGMP snooping**

The switch continues to forward the IGMP membership reports from the hosts to the multicast routers, and forwards queries from multicast routers to all port members of the VLAN.

---

## IGMPv3 snooping

In IGMPv3 snooping mode, the switch recognizes IGMPv3 reports and queries and can:

- recognize whether a source list is populated or blank
- identify the specific sources to filter
- understand and process all IGMPv3 record type

The following are supported:

- source filtering (INCLUDE, EXCLUDE, ALLOW, BLOCK of multicast sources)
- SSM (Source Specific Multicast)

---

## IGMP proxy

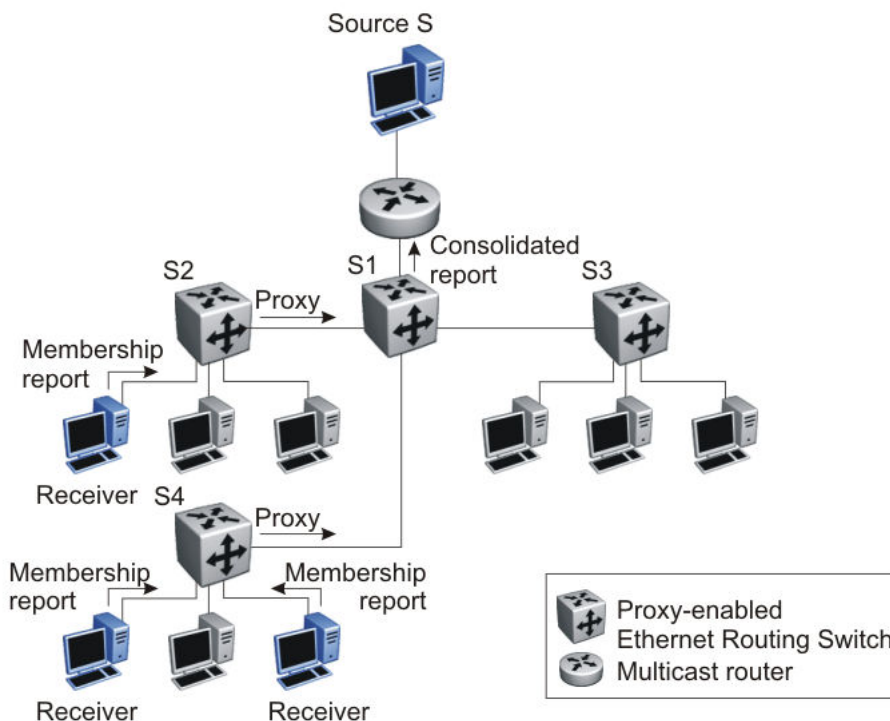
With IGMP snoop enabled, the switch can receive multiple reports for the same multicast group. Rather than forward each report upstream, the switch can consolidate these multiple reports by using the IGMP proxy feature. With IGMP proxy enabled, if the switch receives multiple reports for

the same multicast group, it does not transmit each report to the upstream multicast router. Instead, the switch forwards the first report to the querier and suppresses the rest. If new information emerges that another multicast group is added or that a query is received because the last report is transmitted upstream, the report is then forwarded to the multicast router ports.

To enable IGMP Proxy, you must first activate IGMP snooping.

In the figure that follows, switches S1 to S4 represent a local area network (LAN) connected to an IP Multicast router. The router periodically sends Host Membership Queries to the LAN and listens for a response from end stations. All of the clients connected to switches S1 to S4 are aware of the queries from the router.

One client, connected to S2, responds with a host membership report. Switch S2 intercepts the report from that port, and generates a proxy report to its upstream neighbor, S1. Also, two clients connected to S4 respond with host membership reports, causing S4 to intercept the reports and to generate a consolidated proxy report to its upstream neighbor, S1.



**Figure 15: Ethernet Routing Switch running IGMP proxy**

Switch S1 treats the consolidated proxy reports from S2 and S4 as if they were reports from any client connected to its ports, and generates a consolidated proxy report to the designated router. In this scenario, the router receives a single consolidated report from that entire subnet.

The consolidated proxy report generated by the switch remains transparent to Layer 3 of the International Standardization Organization, Open Systems Interconnection (ISO/OSI) model. (The VLAN IP address and the switch Media Access Control [MAC] address are used for the proxy report generation.) The last reporting IGMP group member in each VLAN represents all of the hosts in that VLAN and IGMP group.

---

## IGMPv3 proxy

With IGMPv3 proxy enabled, if the switch receives multiple reports for the same multicast group, it does not transmit each report to the upstream multicast router. Instead, the switch forwards the first report to the querier and suppresses the rest.

If new information emerges, for example if the switch adds another multicast group or receives a query since the last report was transmitted upstream, then the switch forwards a new report to the multicast router ports.

---

## Forwarding of reports

When forwarding IGMP membership reports from group members, the switch forwards the reports only to those ports where multicast routers are attached. To do this, the switch maintains a list of multicast querier routers and the multicast router (mrouter) ports on which they are attached. The switch learns of the multicast querier routers by listening to the queries sent by the routers where source address is not 0.0.0.0.

---

## Static mrouter port and nonquerier

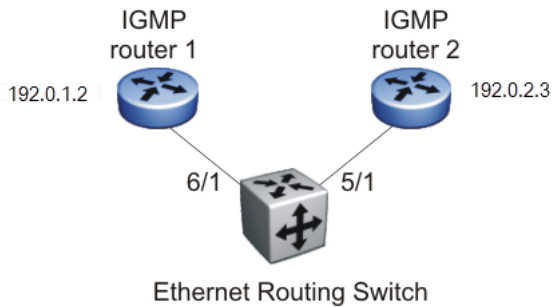
If two IGMP routers are active on a VLAN, the router with the lower IP address is the querier, and the router with the higher IP address operates as a nonquerier. Only querier routers forward IGMP queries on the VLAN; nonqueriers do not forward IGMP queries. IGMP snoop considers the port on which the IGMP query is received as the active IGMP multicast router (mrouter) port. IGMP snoop is not aware of nonquerier IGMP routers.

By default, IGMP snoop forwards reports to the IGMP querier router only. To allow the switch to forward reports to the nonquerier router as well, you can configure the port connected to the nonquerier as a static mrouter port.

The following figure shows how static mrouter ports operate. In this case, the switch has port members 5/1 and 6/1 connected to IGMP routers in VLAN 10. Router 1 is the IGMP querier because it has a lower IP address than router 2. Router 2 is then considered the nonquerier.

By default, the switch learns of the multicast querier routers by listening to the IGMP queries. In this case, port 6/1 connected to querier router 1 is identified as an mrouter port.

To forward reports to IGMP router 2 as well, you can configure port 5/1 on the switch as a static mrouter port. In this case, the IGMP reports are forwarded to both routers.



**Figure 16: Static mrouter port and nonquerier**

## Unknown multicast packet filtering

With IGMP snoop enabled, if the switch receives multicast packets with destination addresses that it has not already registered using IGMP reports, the switch floods all such packets to all ports on the VLAN. All unknown multicast streams of a group are flooded on the VLAN until at least one port in the VLAN becomes a member of that group.

On the switch, you can enable the unknown multicast filtering feature so that the unknown multicast packets are not flooded on the VLAN. To enable unknown multicast filtering, you can use the `vlan igmp unknown-mcast-no-flood` CLI command.

With this feature enabled, the switch forwards all unknown multicast traffic to IGMP static mrouter ports only. The traffic is not forwarded to dynamically discovered mrouter ports.

If you require unknown multicast traffic to be forwarded to certain ports (for example, to forward Layer 3 multicast routing traffic), set the ports as static mrouter ports. Extreme Networks recommends that you enable this feature after IGMP snooping is enabled. User settings for the unknown multicast filtering feature are stored in NVRAM.

Allowing a multicast MAC address to flood all VLANs The unknown multicast filtering feature introduces a potential problem after a Layer 2 VLAN is placed between two Layer 3 switches that are exchanging protocol packets such as OSPF. Since the protocols do not join a multicast group, the associated MAC addresses cannot be identified by the IGMP snooping process. These packets are dropped by the Layer 2 switch because the unknown multicast filtering feature is enabled. The two Layer 3 switches can never establish adjacencies and the OSPF protocol fails.

Using the `vlan igmp unknown-mcast-allow-flood` CLI command, you can specify MAC addresses or multicast IP addresses that need to be flooded on the switch even when the unknown multicast filtering feature is enabled. The specified multicast MAC or IP addresses are added to the allow-flood table for the specified VLAN. Any matching packets are flooded on all ports of that VLAN.

### \* Note:

Multicast MAC addresses used with the allow-flood cannot be from the 01:00:5E:XX:XX:XX family — you must use a corresponding multicast IP address.

---

## Robustness value

As part of the IGMP snooping configuration, use the robustness value to configure the switch to offset expected packet loss on a subnet. If you expect a network to lose query packets, increase the robustness value.

This value is equal to the number of expected query packet losses for each query interval, plus 1. The range is from 2 to 255, and the default is 2. The default value of 2 means that one query for each query interval can be dropped without the querier aging out.

---

## IGMP snooping configuration rules

The IGMP snooping feature operates according to specific configuration rules. When configuring your switch for IGMP snooping, consider the following rules that determine how the configuration reacts in any network topology:

- The switch supports up to 59 multicast groups.  
If the multicast group table reaches its limit, a new entry cannot be added with a JOIN message or a new sender identifying a new group. The multicast stream from the new sender is discarded by the hardware. New entries can be added again when the table is not full.
- You cannot configure port mirroring on a static mrouter port.
- IGMP v1 and v2 reports use up one entry in the table. IGMP v3 reports use up an entry for each group address, as well as an entry for each source specified in the group record, whether it be Exclude or Include.
- Exclude reports for the same group with specified source(s) will make Include reports from other sources redundant and as such these are eliminated.
- If you configure a Multi-Link Trunk member as a static mrouter port, all the Multi-Link Trunk members become static mrouter ports. Also, if you remove a static mrouter port that is a Multi-Link Trunk member, all Multi-Link Trunk members are automatically removed as static mrouter port members.
- All IGMP settings are configured per VLAN.
- When you specify MAC or IP addresses to be flooded on the switch, the specified addresses are flooded only on the VLAN specified within the CLI command. This way, you can flood MAC or IP addresses for specific VLANs only.
- When Spanning Tree is enabled, the switch learns IGMP groups only on ports that are not in Listening or Blocking Spanning Tree states (or, when in RSTP/MSTP mode, only on ports that are in the Designated state). The switch also learns the groups if STP is disabled on a port.
- The IGMP snooping feature is not Rate Limiting-dependent.
- You must enable the IGMP snooping feature before you can enable the IGMP proxy feature.

**! Important:**

Because IGMP snooping is set up per VLAN, all IGMP changes are implemented according to the VLAN configuration for the specified ports.

---

## Default IGMP values

The following table lists the default IGMP values on the Ethernet Routing Switch.

Parameters	Range	Default Value
Snooping	Enable/Disable	Disable
Version	1-3	2
Proxy	Enable/Disable	Disable
Query Interval	0-65535	125
Robustness Value	2-255	2

---

## IGMP snooping interworking with Windows clients

This section describes an interworking issue between Windows clients and the switches when IGMP snoop is enabled for multicast traffic.

Under normal IGMP snoop operation, as soon as a client joins a specific multicast group, the group is no longer unknown to the switch, and the switch sends the multicast stream only to the ports which request it.

To force a Windows client to only use IGMPv1 or IGMPv2 reports, change the TCP/IP settings in the Windows Registry located under the following registry key:

**\* Note:**

The following settings are only required if you are using IGMPv1 or IGMPv2.

```
HKEY_LOCAL_MACHINE
\SYSTEM
\CurrentControlSet
\Services
\Tcpip
\Parameters
```

The specific parameter which controls the IGMP Version is:

```
IGMPVersion
Key: Tcpip\Parameters
Value Type: REG_DWORD-Number
Valid Range: 2, 3, 4
Default: 4
```

To set the Windows Client to only utilize IGMPv2, change the IGMPVersion parameter to 3 (2 specifies IGMPv1, 3 specifies IGMPv2, and 4 specifies IGMPv3).



The IGMPVersion parameter may not be present in the list of the TCP/IP parameters. By default, the system assumes the IGMPv3 value (4). To configure the system for IGMPv2, create the parameter as a DWORD key in the registry and specify Decimal 3.

 **Important:**

If you edit the Windows registry incorrectly, you can severely damage your system. As a minimal safeguard, back up your system data before undertaking changes to the registry.

# Chapter 6: IP routing configuration using CLI

The ERS 3500 Series are Layer 3 switches. This means that a regular Layer 2 VLAN becomes a routable Layer 3 VLAN if an IP address is attached to the VLAN. When routing is enabled in Layer 3 mode, every Layer 3 VLAN is capable of routing and carrying the management traffic. You can use any Layer 3 VLAN instead of the Management VLAN to manage the switch.

For more information about creating and configuring VLANs, see *Configuring VLANs, Spanning Tree, and MultiLink Trunking on Ethernet Routing Switch 3500 Series*.

---

## IP routing configuration procedures

To configure inter-VLAN routing on the switch, perform the following steps:

### Procedure

1. Enable IP routing globally.
2. Assign IP addresses to multiple VLANs.

Routing is automatically enabled on the VLAN after you assign an IP address to it.

In the preceding procedure, you are not required to enable IP routing as the first step. You can configure all IP routing parameters on the switch before you enable routing.

---

## Configuring global IP routing status

Use this procedure to enable and disable global routing at the switch level. By default, routing is disabled.

### Procedure

1. Enter Global Configuration mode:

```
enable
```

```
configure terminal
```

- At the command prompt, enter the following command:

```
[no] ip routing
```

---

## Variable definitions

The following table describes the parameters for the `ip routing` command.

Variable	Value
no	Disables IP routing on the switch.

---

## Displaying global IP routing status

Use this procedure to display the status of IP routing on the switch.

### Procedure

- Log on to CLI to enter User EXEC mode.
- At the command prompt, enter the following command:

```
show ip routing
```

---

## Configuring an IP address for a VLAN

To enable routing on a VLAN, you must first configure an IP address on the VLAN.

### Procedure

- Enter VLAN Interface Configuration mode:
 

```
enable
configure terminal
interface vlan <vlan ID>
```
- At the command prompt, enter the following command:
 

```
[no] ip address <ipaddr> <mask> [<MAC-offset>]
```

---

## Variable definitions

The following table describes the parameters for the `ip address` command.

Variable	Value
[no]	Removes the configured IP address and disables routing on the VLAN.
<ipaddr>	Specifies the IP address to attach to the VLAN.
<mask>	Specifies the subnet mask to attach to the VLAN.
[<MAC-offset>]	Specifies the value used to calculate the VLAN MAC address, which is offset from the switch MAC address.  RANGE: The valid range is 1-256.  Specify the value 1 for the Management VLAN only. If no MAC offset is specified, the switch applies one automatically.

---

## Configuring IP routing status on a VLAN

Use this procedure to enable and disable routing for a particular VLAN.

### Procedure

1. Enter VLAN Interface Configuration mode:

```
enable
configure terminal
interface vlan <vlan ID>
```

2. At the command prompt, enter the following command:

```
[default] [no] ip routing
```

---

## Variable definitions

The following table describes the parameters for the `ip routing` command.

Variable	Value
default	Disables IP routing on the VLAN.
no	Disables IP routing on the VLAN.

---

## Displaying the IP address configuration and routing status for a VLAN

Use this procedure to display the IP address configuration and the status of routing on a VLAN.

### Procedure

1. Enter Privileged EXEC mode:

```
enable
```

2. At the command prompt, enter the following command:

```
show vlan ip [vid <vid>]
```

The following information is displayed:

- Vid — Specifies the VLAN ID
- ifIndex — Specifies an index entry for the interface
- Address — Specifies the IP address associated with the VLAN
- Mask — Specifies the mask
- MacAddress — Specifies the MAC address associated with the VLAN
- Offset — Specifies the value used to calculate the VLAN MAC address, which is offset from the switch MAC address
- Routing — Specifies the status of routing on the VLAN: enabled or disabled

---

## Variable definitions

The following table describes the parameters for the `show vlan ip` command.

Variable	Value
[vid<vid>]	Specifies the VLAN ID of the VLAN to be displayed. RANGE: 1–4094.

---

## Displaying IP routes

Use this procedure to display all active routes on the switch.

### Procedure

1. Log on to CLI to enter User EXEC mode.

2. At the command prompt, enter the following command:

```
show ip route [<dest-ip>] [-s <subnet> <mask>]
```

The following information is displayed:

- DST — Identifies the route destination
- MASK — Identifies the route mask
- NEXT — Identifies the next hop in the route
- COST — Identifies the route cost
- VLAN — Identifies the VLAN ID on the route
- PORT — Specifies the ports
- PROT — Specifies the routing protocols. Options are LOC (local route) or STAT (static route)
- TYPE — Indicates the type of route as described by the Type Legend
- PRF — Specifies the route preference

---

## Variable definitions

The following table describes the parameters for the `show ip route` command.

Variable	Value
<dest-ip>	Specifies the destination IP address of the routes to display.
[-s<subnet><mask>]	Specifies the destination subnet of the routes to display.

# Chapter 7: Static route configuration using CLI

This chapter describes the procedures you can use to configure static routes using the CLI.

---

## Configuring a static route

Create static routes to manually configure a path to destination IP address prefixes.

### Before you begin

- Enable IP routing globally.
- Enable IP routing and configure an IP address on the VLANs to be routed.

### Procedure

1. Enter Global Configuration mode:

```
enable  
configure terminal
```

2. At the command prompt, enter the following command:

```
[no] ip route <dest-ip> <mask> <next-hop> [<cost>] [disable]  
[enable] [weight <cost>]
```

---

## Variable definitions

The following table describes the parameters for the `ip route` command.

Variable	Value
[no]	Removes the specified static route.
<dest-ip>	Specifies the destination IP address for the route being added. DEFAULT:

*Table continues...*

Variable	Value
	0.0.0.0 is considered the default route.
<mask>	Specifies the destination subnet mask for the route being added.
<next-hop>	Specifies the next hop IP address for the route being added.
[<cost>]	Specifies the weight, or cost, of the route being added.  RANGE: 1–65535
[enable]	Enables the specified static route.
[disable]	Disables the specified static route.
[weight<cost>]	Changes the weight, or cost, of an existing static route.  RANGE: 1–65535

---

## Displaying static routes

Use this procedure to display all static routes, whether these routes are active or inactive.

### Procedure

1. Log on to CLI to enter User EXEC mode.
2. At the command prompt, enter the following command:

```
show ip route static [<dest-ip>] [-s <subnet> <mask>]
```

The following information is displayed:

- DEST — Identifies the route destination
- MASK — Identifies the route mask.
- NEXT — Identifies the next hop in the route.
- COST — Identifies the route cost.
- PREF — Specifies the route preference.
- LCNHOP — Specifies the local next hop status.
- STATUS — Specifies the static route status. Options are ACTIVE (in use and present in routing table) or INACTV (not in use and not present in routing table).
- ENABLE — Specifies the administrative state of the static route. Options are TRUE (administratively enabled) or FALSE (administratively disabled).



---

## Variable definitions

The following table describes the parameters for the `show ip route static` command.

Variable	Value
<dest-ip>	Specifies the destination IP address of the static routes to display.
[-s <subnet> <mask>]	Specifies the destination subnet of the routes to display.

---

## Configuring a management route

Use this procedure to create a management route to the far end network, with a next-hop IP address from the management VLAN's subnet. You can configure a maximum of four management routes on the switch.

### Before you begin

- Enable IP routing globally.
- Enable IP routing and configure an IP address on the management VLAN interface.

### Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. At the command prompt, enter the following command:

```
[no] ip mgmt route <dest-ip> <mask> <next-hop>
```

---

## Variable definitions

The following table describes the parameters for the `ip mgmt route` command.

Variable	Value
[no]	Removes the specified management route.
<dest-ip>	Specifies the destination IP address for the route being added.
<mask>	Specifies the destination subnet mask for the route being added.

*Table continues...*

Variable	Value
<next-hop>	Specifies the next hop IP address for the route being added.

---

## Displaying the management routes

Use this procedure to display the static routes configured for the management VLAN.

### Procedure

1. Log on to CLI to enter User EXEC mode.
2. At the command prompt, enter the following command:

```
show ip mgmt route
```

The following information is displayed:

- Destination IP — Identifies the route destination.
- Subnet Mask — Identifies the route mask.
- Gateway IP — Identifies the next hop in the route.
- Status — Displays
  - ACTIVE if:
    - the management IP address is configured
    - the management route next-hop resides in the same network as the management IP address
    - the management VLAN is active — at least one member port is up
  - INACTIVE under all other circumstances

# Chapter 8: DHCP relay configuration using CLI

This chapter describes the procedures you can use to configure Dynamic Host Configuration Protocol (DHCP) relay.

**! Important:**

DHCP relay uses a hardware resource that is shared by switch Quality of Service applications. When DHCP relay is enabled globally, the Quality of Service filter manager will not be able to use precedence 3 for configurations. For the filter manager to be able to use this resource, DHCP relay must be disabled for the entire unit.

---

## Prerequisites to DHCP relay configuration

- Enable IP routing globally.
- Enable IP routing and configure an IP address on the VLAN to be set as the DHCP relay agent.
- Ensure that a route (local or static) to the destination DHCP server is available on the switch.

---

## DHCP relay configuration procedures

Use the following procedure to configure DHCP relay.

### Procedure

1. Ensure that DHCP relay is enabled globally. (DHCP relay is enabled by default).
2. Configure the DHCP relay forwarding path by specifying a local VLAN as the DHCP relay agent and the remote DHCP server as the destination.
3. Enable DHCP relay for the specific VLAN.

## Enabling or disabling global DHCP relay

Use the following procedure to enable or disable global DHCP relay. DHCP relay is enabled by default.

### Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. At the command prompt, enter the following command:

```
ip dhcp-relay to enable
OR
no ip dhcp-relay to disable
```

---

## Setting global DHCP relay to default

Use the following procedure to set DHCP relay to default settings for the switch. DHCP relay is enabled by default.

### Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. At the command prompt, enter the following command:

```
default ip dhcp-relay
```

---

## Displaying the global DHCP relay status

Use this procedure to display the current DHCP relay status for the switch.

### Procedure

1. Log on to CLI to enter User EXEC mode.
2. At the command prompt, enter the following command:

```
show ip dhcp-relay
```

---

## Variable definitions

The following table describes the parameters for the `ip dhcp-relay` command.

Variable	Value
default	Sets DHCP relay to default settings.
no	Disables DHCP relay.
show	Shows the status of the DHCP relay.

---

## Displaying IP DHCP client parameters

Use the following procedure to display IP DHCP client parameters for the switch.

### Procedure

1. Enter Global Configuration mode:
 

```
enable
configure terminal
```
2. At the command prompt, enter the following command:
 

```
show ip dhcp client lease
```

---

## Specifying a local DHCP relay agent and remote DHCP server

Use this procedure to specify a local VLAN as a DHCP relay agent on the forwarding path to a remote DHCP server. The DHCP relay agent can forward DHCP client requests from the local network to the DHCP server in the remote network.

The DHCP relay feature is enabled by default, and the default mode is BootP-DHCP.

### Procedure

1. Enter Global Configuration mode:
 

```
enable
configure terminal
```
2. At the command prompt, enter the following command:

```
[no] ip dhcp-relay fwd-path <relay-agent-ip> <DHCP-server> [enable]
[disable] [mode {bootp | bootp-dhcp | dhcp}]
```

---

## Variable definitions

The following table describes the parameters for the `ip dhcp-relay fwd-path` command.

Variable	Value
[no]	Removes the specified DHCP forwarding path.
<relay-agent-ip>	Specifies the IP address of the VLAN that serves as the local DHCP relay agent.
<DHCP-server>	Specifies the address of the remote DHCP server to which DHCP packets are to be relayed.
[enable]	Enables the specified DHCP relay forwarding path.
[disable]	Disables the specified DHCP relay forwarding path.
[mode {bootp   bootp-dhcp   dhcp}]	Specifies the DHCP relay mode: <ul style="list-style-type: none"> <li>• BootP only</li> <li>• BootP and DHCP</li> <li>• DHCP only</li> </ul> If you do not specify a mode, the default DHCP and BootP is used.

---

## Displaying the DHCP relay configuration

Use this procedure to display the current DHCP relay agent configuration.

### Procedure

1. Log on to CLI to enter User EXEC mode.
2. At the command prompt, enter the following command:

```
show ip dhcp-relay fwd-path
```

---

## Configuring DHCP relay on a VLAN

Use this procedure to configure the DHCP relay parameters on a VLAN.

To enable DHCP relay on the VLAN, enter the command with no optional parameters.

## Procedure

1. Enter VLAN Interface Configuration mode:

```
enable
configure terminal
interface vlan <vlan ID>
```

2. At the command prompt, enter the following command:

```
[no] ip dhcp-relay [broadcast][clear counters][min-sec <min-sec>]
[mode {bootp | dhcp | bootp_dhcp}][Option-82]
```

## Variable definitions

The following table describes the parameters for the `ip dhcp-relay` command.

Variable	Value
[no]	Disables DHCP relay on the specified VLAN.
[broadcast]	Enables the broadcast of DHCP reply packets to the DHCP clients on this VLAN interface.
[Clear Counters]	Clear the existing number of counters and restart the counters.
min-sec<min-sec>	Indicates the min-sec value. The switch immediately forwards a BootP/DHCP packet if the secs field in the BootP/DHCP packet header is greater than the configured min-sec value; otherwise, the packet is dropped.  RANGE: 0–65535  DEFAULT: The default is 0.
mode {bootp   dhcp   bootp_dhcp}	Specifies the type of DHCP packets this VLAN supports: <ul style="list-style-type: none"> <li>• bootp - Supports BootP only</li> <li>• dhcp - Supports DHCP only</li> <li>• bootp_dhcp - Supports both BootP and DHCP</li> </ul>
[Option-82]	Specifies the DHCP Option 82 subscriber ID for the port.

---

## Displaying the DHCP relay configuration for a VLAN

Use this procedure to display the current DHCP relay parameters configured for a VLAN.

### Procedure

1. Enter Privileged EXEC mode:
2. At the command prompt, enter the following command:

```
enable
show vlan dhcp-relay [<vid>]
```

The following information is displayed:

- IfIndex — Indicates the VLAN interface index.
- MIN\_SEC — Indicates the min-sec value. The switch immediately forwards a bootP/DHCP packet if the secs field in the BootP/DHCP packet header is greater than the configured min-sec value; otherwise, the packet is dropped.
- ENABLED — Indicates whether DHCP relay is enabled on the VLAN.
- MODE — Indicates the type of DHCP packets this interface supports. Options include none, BootP, DHCP, and both.
- ALWAYS\_BROADCAST — Indicates whether DHCP reply packets are broadcast to the DHCP client on this VLAN interface.

---

## Variable definitions

The following table describes the parameters for the `show vlan dhcp-relay` command.

Variable	Value
[<vid>]	Specifies the VLAN ID of the VLAN to be displayed. RANGE: 1–4094

---

## Displaying DHCP relay counters

Use this procedure to display the current DHCP relay counters. This includes the number of requests and the number of replies.

### Procedure

1. Log on to CLI to enter User EXEC mode.
2. At the command prompt, enter the following command:



```
show ip dhcp-relay counters
```

The following information is displayed:

- INTERFACE — Indicates the interface IP address of the DHCP relay agent.
- REQUESTS — Indicates the number of DHCP requests.
- REPLIES — Indicates the number of DHCP replies.

---

## Clearing DHCP relay counters for a VLAN

Use this procedure to clear the DHCP relay counters for a VLAN.

### Procedure

1. Enter VLAN Interface Configuration mode:

```
enable  
configure terminal  
interface vlan <vlan ID>
```

2. At the command prompt, enter the following command:

```
ip dhcp-relay clear-counters
```

---

## Configuring DHCP Relay Option 82 globally

To enable or disable the DHCP Relay Option 82 at the switch level, you can configure Option 82 for DHCP relay globally.

### Procedure

1. Enter Global Configuration mode:

```
enable  
configure terminal
```

2. At the command prompt, enter the following command:

```
[no|default] ip dhcp-relay option82
```

---

## Variable definitions

The following table describes the parameters for the `ip dhcp-relay option82` command.

Variable	Value
default	Resets DHCP Relay Option 82 to default values. DEFAULT: Default value is disabled.
no	Disables DHCP Relay Option 82 for the switch.

---

## Configuring DHCP Relay with Option 82 for a VLAN

Perform the following procedure to configure DHCP Relay with Option 82 for a VLAN.

### Procedure

1. Enter VLAN Interface Configuration mode:
 

```
enable
configure terminal
interface vlan <vlan ID>
```
2. At the command prompt, enter the following command:
 

```
ip dhcp-relay option82
```

---

## Configuring DHCP Forwarding Maximum Frame size

You can specify the maximum frame size the DHCP relay agent can forward to the DHCP server. While the switch implementation permits configuration of the maximum DHCP packet size up to 1536 bytes, the default maximum size is 576 bytes.

Use the following procedure to configure DHCP Forwarding maximum frame size.

### Procedure

1. Enter Global Configuration mode:
 

```
enable
configure terminal
```
2. At the command prompt, enter the following command:
 

```
ip dhcp-relay max-frame <576-1536>
```

---

## Assigning a DHCP Relay Option 82 subscriber ID to a port

To associate an alphanumeric character string with the Option 82 function for a port, you can assign a DHCP Relay Option 82 subscriber ID to the port.

### Procedure

1. Enter Interface Configuration mode:

```
enable
configure terminal
interface fastEthernet <port>
```

2. At the command prompt, enter the following command:

```
[no|default] ip dhcp-relay option82-subscriber-id <Word 1-255>
```

---

## Variable definitions

The following table describes the parameters for the `ip dhcp-relay option 82-subscriber-id` command.

Variable	Value
default	Resets DHCP Relay Option 82 subscriber ID to the default value.  DEFAULT: The default is disabled.
no	Removes DHCP Relay Option 82 subscriber ID from a port.
Word	Specifies the DHCP Relay Option 82 subscriber ID for the port. The value is a character string between 1 and 255 characters.

---

## Displaying DHCP Relay

Use the following procedure to display the state of the DHCP Relay, DHCP Relay Option 82, and DHCP Relay maximum frame size.

### Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. At the command prompt, enter the following command:

```
show ip dhcp-relay
```

### Example

```
Switch>enable
Switch#configure
Configuring from terminal or network [terminal]? terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)#show ip dhcp-relay
=====
      DHCP Relay Global
=====
DHCP relay is enabled
DHCP relay option82 is disabled
DHCP relay max-frame is 576
Switch(config)#
```

# Chapter 9: DHCP Server configuration using CLI

If you have no separate DHCP server or other device available to provide the service to local hosts, you can use the procedures in this chapter to configure the DHCP Server feature to provide and manage IPv4 addresses in your network and eliminate manual TCP/IP configuration.

---

## Displaying the DHCP Server status

Use this procedure to display the DHCP server status.

### Procedure

1. Enter Privileged EXEC mode:  
`enable`
2. At the prompt, enter the following command:  
`show ip dhcp-server`

### Example

The following figure displays a sample output for the `show ip dhcp-server` command.

```
Switch(config)#show ip dhcp-server
DHCP Server: Enabled
Lease time: 1 day 12 hours 30 minutes
DNS servers: 10.10.10.3 10.10.10.4
Routers: 11.11.11.5 11.11.11.6
Switch(config)#
```

---

## Displaying DHCP Server IP address pools

Use this procedure to display all DHCP Server IP address pools, or a specific pool.

### Procedure

1. Enter Privileged EXEC mode:

```
enable
```

2. At the prompt, enter the following command:

```
show ip dhcp-server pool <WORD>
```

### Example

The following displays a sample output for the **show ip dhcp-server pool** command.

```
Switch(config)#show ip dhcp-server pool
Pool: myPool
-----
Start IP Address: 198.0.2.1
End IP Address: 192.0.2.14
Lease time: 1d:0h:0m
Subnet Mask: 255.255.255.0
DNS Servers:
Routers:
Vendor-info:
SIP Servers:
TFTP Servers:
  IP-Phone(176):
    MCIPADD:
    MCPORT: 1719
    Tftpsrvr:
    L2qvlan: 0
    Vlantest: 60
    L2quad: 6
    L2qsig: 6
  IP-Phone(241):
    Vendor type: IP Phone
    String:
  IP-Phone(242):
    MCIPADD:
    HTTP Server:
    HTTP Port: 80
Switch(config)#
```

---

## Variable definitions

The following table describes the parameters for the **show ip dhcp-server pool** command.

Variable	Value
<i>WORD</i>	Specifies a specific IP address pool to display. IP address pool names can be up to 32 alphanumeric characters long. You can define up to 32 separate pools.

---

## Displaying DHCP Server IP address leases

Use this procedure to display IP address lease duration.

## Procedure

1. Enter Privileged EXEC mode:  
enable
2. At the prompt, enter the following command:  
show ip dhcp-server leases

## Example

The following figure displays a sample output for the `show ip dhcp-server leases` command.

```
Switch#show ip dhcp-server
```

```
Pool: Marketing
```

Name	IP Address	MAC Address	Lease Exp	Subnet Mask
HP-Laptop	10.10.10.100	00:1e:68:40:af:09	0:22:49	255.255.255.0
LA091693A	10.10.10.113	00:27:13:6a:0f:4b	0:23:59	255.255.255.0
D600-Laptop	10.10.10.114	00:0b:db_a6:b4:ea	0:23:58	255.255.255.0
Green-Toshiba	10.10.10.115	00:26:6c:52:e0:2e	0:23:58	255.255.255.0

```
Pool: Sales
```

Name	IP Address	MAC Address	Lease Exp	Subnet Mask
Green-Toshiba	10.10.20.200	00:26:6c:52:e0:2e	0:20:35	255.255.255.0

## Enabling DHCP Server

Use this procedure to enable DHCP Server on your switch or stack

### Before you begin

For a single VLAN configuration:

- Configure or change the IPv4 address configuration according to your setup on the switch or stack (Management VLAN) so the DHCP server can offer an address to the client in that VLAN
- Define at least one IP address pool range or host with a valid network mask
- Enable DHCP

### \* Note:

When IP routing is disabled, the DHCP Server IP is bound to the Management VLAN IP. When IP routing is enabled, the DHCP Server is bound on all the VLAN IPs from the switch or stack..

When adding a second or subsequent VLAN to which you want to assign DHCP Server pools:

- Enable IP routing/forwarding on the switch or stack

In order for the DHCP Server to function on a VLAN IP or Management VLAN, the configured subnet mask must be identical to the subnet class of the VLAN IP (Management or other VLAN subnet mask configured) and the subnet mask from the DHCP Server IP pool (range or host).

**\* Note:**

When you enable the DHCP Server, DHCP Snooping functionality is disabled, even if the configuration indicates that DHCP Snooping is enabled.

**Procedure**

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. At the prompt, enter the following command:

```
ip dhcp-server enable
```

---

## Disabling the DHCP Server

Use this procedure to disable the DHCP Server and erase the global parameters.

**Procedure**

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. At the prompt, enter the following command:

```
no ip dhcp-server
```

---

## Restoring the DHCP Server to default

Use this procedure to disable the DHCP Server and set all global parameters for the DHCP Server to default (while the IP pools remain the same).

**Procedure**

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. At the prompt, enter the following command:

```
default ip dhcp-server
```



## Configuring DHCP Server IP address lease duration

Use this procedure to set DHCP Server IP address lease duration.

### About this task

You assign specified IP address lease duration to clients, based on the number and type of hosts in your network, to limit network congestion caused by too-frequent IP address requests.

### Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. At the prompt, enter the following command:

```
ip dhcp-server lease {[days <1-49710>] | [hours <0-23>] | [minutes
<0-59>] | infinite }
```

### Example

The following displays an example of the **ip dhcp-server lease** command.

```
ip dhcp-server lease days 1 hours 5 minutes 3
```

#### Note:

You can specify the lease time for IP range type pools only. For the host pools, the lease time is infinite.

## Variable definitions

The following table describes the parameters for the **ip dhcp-server lease** command.

Variable	Value
days<1-49710>	Enter a value from 1 to 49710 days. Default: 1 day.
hours<0-23>	Enter a value from 0 to 23. Default: 0 hours.
minutes<0-59>	Enter a value from 0 to 59. Default: 0 minutes.
infinite	Specifies that the lease does not expire.

## Resetting DHCP Server lease duration to default

Use this procedure to set DHCP Server IP address lease duration to the default value of 1 day 0 hours 0 minutes.

### Procedure

1. Enter Global Configuration mode:  
`enable`  
`configure terminal`
2. At the prompt, enter the following command:  
`default ip dhcp-server lease`

---

## Configuring DHCP Server routers

Use this procedure to configure the IP address of a host default gateway for DHCP Server. You can specify up to 8 routers for DHCP Server.

### Procedure

1. Enter Global Configuration mode:  
`enable`  
`configure terminal`
2. At the prompt, enter the following command:  
`ip dhcp-server option-3 <IPv4AddrList>`

### Example

The following displays an example of the **ip dhcp-server option-3** command.

```
Switch(config)#ip dhcp-server option-3 192.0.2.1 192.0.2.10
```

---

## Variable Definitions

The following table describes the parameters for the **ip dhcp-server option-3** command.

Variable	Value
<i>IPv4AddrList</i>	Enter the IPv4 address of a host default gateway. If entering multiple routers, separate the entries with a space.

---

## Deleting DHCP Server routers

Use this procedure to remove a router from the DHCP server router list, or to clear the DHCP server router list.

**Procedure**

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. At the prompt, enter the following command:

```
no ip dhcp-server option-3 <IPv4AddrList>
```

OR

```
default ip dhcp-server option-3
```

**Example**

The following displays an example of the **no ip dhcp-server option-3** command.

```
Switch(config)#no ip dhcp-server option-3 192.0.2.1
```

---

**Variable definitions**

The following table describes the parameters for the **ip dhcp-server option-3** command.

Variable	Value
no	Deletes routers from the DHCP Server router list.
default	Returns the router list to the default condition, which is empty.
<i>&lt;IPv4AddrList</i>	Specifies an IPv4 address or list of addresses to remove from the DHCP Server router list. If entering multiple routers, separate the entries with a space. If this parameter is not specified, the system clears the router list.

---

**Configuring the Domain Name System server**

Use this procedure to configure up to eight DNS servers.

**Procedure**

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. At the prompt, enter the following command:

```
ip dhcp-server option-6 <IPv4AddrList>
```

---

## Variable Definitions

The following table describes the parameters for the `ip dhcp-server option-6` command.

Variable	Value
<code>IPv4AddrList</code>	Enter the DNS server IP address or list of addresses. If entering multiple servers, separate the entries with a space.

---

## Deleting DNS servers

Use this procedure to remove DNS servers from the server list, or to clear the DNS server list.

### Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. At the prompt, enter the following command:

```
no ip dhcp-server option-6 <IPv4AddrList>
```

OR

```
default ip dhcp-server option-6
```

### Example

Configure five DNS servers:

```
ip dhcp-server option-6 1.1.1.1 2.2.2.2 3.3.3.3 4.4.4.4 5.5.5.5
```

Delete two of the DNS servers:

```
no ip dhcp-server option-6 2.2.2.2 4.4.4.4
```

---

## Variable definitions

The following table describes the parameters for the `ip dhcp-server option-3` command.

Variable	Value
<code>no</code>	Deletes servers from the DNS Server list.
<code>default</code>	Returns the server list to the default condition, which is empty.

*Table continues...*

Variable	Value
<i>&lt;IPv4AddrList&gt;</i>	Specifies an IPv4 address or list of addresses to remove from the DNS Server list. If entering multiple servers, separate the entries with a space. If this parameter is not specified, the system clears the DNS server list.

## Creating a DHCP Server IP address pool

Use this procedure to create a DHCP Server IP address pool.

### Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. At the prompt, enter the following command:

```
ip dhcp-server pool <poolName> { range { <start_addr> <end_addr>} |
host <A.B.C.D> <xx:xx:xx:xx:xx:xx> }
```

### Example

The following command creates a range type pool:

```
ip dhcp-server pool myRangePool range 192.168.0.100 192.168.0.200
```

The following command creates a host type pool:

```
ip dhcp-server pool myHostPool host 192.168.0.10 11:22:33:44:55:66
```

## Variable definitions

The following table describes the parameters for the **ip dhcp-server pool** command.

Variable	Value
<i>poolName</i>	Specifies the name of the pool to be created, from 1 to 32 characters.
range <start_addr> <end_addr>	Specifies the start and end of the IP address allocation list.
host <A.B.C.D> <xx:xx:xx:xx:xx:xx>	Specifies the static IP allocation, the host IP address.

## Configuring DHCP Server IP address pool options

Use this procedure to configure optional settings for DHCP Server IP address pools.

### About this task

You must create or add pool options on a per pool basis. This is not a global function.

#### \* Note:

The DHCP Server IP address pool Option-176 feature supports only IP Phones 4600 series for provisioning a number of parameters. When you create a DHCP Server IP Address Pool, Option 176 is automatically enabled with several default parameters, with the exception of the MCIPADD and TFTP Server IP address information.

### Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. At the prompt, enter the following command (include only the options that you need):

```
ip dhcp-server pool <poolName> [host <A.B.C.D> <xx:xx:xx:xx:xx:xx> |
range <A.B.C.D> <A.B.C.D>] | [option-60 <WORD>] | [lease { {[days
<1-49710>] [hours <0-23>] [minutes <0-59>]} | infinite }} |
[option-1 {<0-32> | <A.B.C.D> }] | [option-43 <WORD>] | [option-3
<ipv4AddrList>] | [option-6 <ipv4AddrList>] | [option-120
<ipv4AddrList>|<DNSName>] | [option-150 <ipv4AddrList>] |
[option-176 {[mcipadd <ipv4AddrList>] [mcport <1-65535>] [tftp-
servers <ipv4AddrList>][[l2qvlan <0-4096>] [vlantest <0-180>] |
[l2qaud <0-7> [l2qsig <0-7>]]}] | [option-241 <parametersList>] |
[option-242 {[mcipadd <ipv4AddrList>] | [httpsrvr <ipv4AddrList>] |
[httpport <1-65535>]}]
```

### Example

```
Switch(config)#ip dhcp-server pool myPool range 192.0.2.1 192.0.2.3 lease days 3 option-1
255.255.255.0 option-3 192.0.2.4 option-6 192.0.2.5 option-150 192.0.2.6 option-242
httpport 8080
```

## Variable definitions

The following table describes the options for the `ip dhcp-server pool` command.

Variable	Value
host <A.B.C.D> <xx:xx:xx:xx:xx:xx>	Specifies the static IP allocation, the host IP address.

*Table continues...*

Variable	Value
lease	Specifies the pool lease duration in: <ul style="list-style-type: none"> <li>• days – the number of days the lease is active from 1 to 49710. The default is 1.</li> <li>• hours – the number of hours the lease is active from 0 to 23. The default is 0.</li> <li>• infinite – no lease expiry</li> <li>• minutes – the number of minutes the lease is active from 0 to 59. The default is 0.</li> </ul>
option-1 <0–32>   <A.B.C.D>	Specifies the subnet mask associated with this address pool as a value from 0 to 32, or using dot-decimal notation.
option-3 <ipv4AddrList>	Specifies the list of routers as a list of IPv4 addresses, separated by spaces.
option-6 <ipv4AddrList>	Specifies the list of DNS servers as a list of IPv4 addresses, separated by spaces.
option-43 <WORD>	Specifies vendor specific information to be exchanged between clients and servers. For the list of supported code types, see <a href="#">DHCP Server Option 43 vendor specific information</a> on page 88.
option-60 <WORD>	Specifies the vendor class identifier.
option-120 <ipv4AddrList>   <DNSName>	Specifies the list of SIP servers as a list of IPv4 addresses, or the DNS name.
option-150 <ipv4AddrList>	Specifies the list of TFTP servers as a list of IPv4 addresses.
option-176 (IP Phone 4600 Series)	Configures IP Phones 4600 Series parameters: <ul style="list-style-type: none"> <li>• mcipadd – enter an IP Phone IPv4 address or list of addresses</li> <li>• mcport—enter a value from 1 to 65535 to specify the UDP port the IP Phone uses for registration. The default is 1719.</li> <li>• tftp-servers—enter one IPv4 address, or multiple IPv4 addresses, of TFTP servers where IP Phones can collect configuration information</li> <li>• l2qvlan—enter a value from 0 to 4096 to specify the 802.1Q VLAN ID. The default is 0.</li> <li>• vlantest—enter a value from 0 to 180 to specify the number of seconds a phone will attempt to return to the previously known voice VLAN.</li> <li>• l2qaud—enter a value from 0 to 7 to specify the layer 2 audio priority value</li> </ul>

*Table continues...*

Variable	Value
	<ul style="list-style-type: none"> <li>l2qsig—enter a value from 0 to 7 to specify the layer 2 signaling priority value</li> </ul>
option-241 (IP Phones 1100, 1200, and 2000 Series)	<p>Configures parameters for IP Phones 1100, 1200 and 2000 Series. For the list of supported parameters, see <a href="#">DHCP Server Option 241 parameters</a> on page 91. If the parameter is not included, the parameter will retain its default value, or the value that was previously provisioned for the specific parameter. Parameter value is between the equals sign and semicolon. Format and example of the parameter list: IP Phone, s1ip=47.11.62.20;p1=4100;a1=1;r1=255;s2ip=47.11.62.21;p2=4100;a2=1;r2=2;</p>
option-242 (IP Phones 4600, 960x)	<p>Configures parameters for IP Phones 4600, 960x. The following parameters are supported:</p> <ul style="list-style-type: none"> <li>httpport – enter a value from 0 to 65535 to specify the HTTP port. The default is 80.</li> <li>httpsrvr – enter an IP Phone IPv4 address or list of addresses. You can enter up to eight (8) IP addresses.</li> <li>mcipadd – enter an IP Phone IPv4 address or list of addresses. You can enter up to eight (8) Call Server IP Addresses. This parameter is used as a backup for the IP phone in case the HTTP Server is unavailable, in which case the IP phone can reach the Call Server.</li> </ul>
range <A.B.C.D> <A.B.C.D>	Specifies the start and end of the IP address allocation list.

## DHCP Server Option 43 vendor specific information

The following table lists the code types supported with the DHCP Server Option-43 vendor specific info command.

Name	Code	Type	Description
snmk	1	ip	<p>Subnet mask of the IP address to be allocated.</p> <p>Default: natural mask corresponding to the IP address.</p> <p>The server does not issue IP addresses to clients on different subnets.</p>
tmof	2	long	Time offset from UTC, in seconds.

*Table continues...*



Name	Code	Type	Description
rou	3	iplist	List of routers on the same subnet as the client.
tmsv	4	iplist	A list of time servers (RFC 868).
nmsv	5	iplist	A list of name servers (IEN 116).
dnsv	6	iplist	A list of DNS servers (RFC 1035).
lgsv	7	iplist	A list of MIT-LCS UDP log servers.
chsv	8	iplist	A list of Cookie servers (RFC 865).
lpsv	9	iplist	A list of LPR servers (RFC 1179).
imsv	10	iplist	A list of Imagen Impress servers.
rlsv	11	iplist	A list of Resource Location servers (RFC 887).
hstn	12	str	Host name of the client.
btsz	13	short	Size of the boot image.
mdmp	14	str	Path name to which client dumps core.
dnsd	15	str	Domain name for DNS.
sww	16	ip	IP address of swap server.
rpth	17	str	Path name of root disk of the client.
epth	18	str	Extensions Path (RFC 1533).
plcy	21	ippairs	Policy filter for non-local source routing. A list of pairs of: Destination IP, Subnet mask.
mdgs	22	short	Maximum size of IP datagram that the client should be able to reassemble.
ditl	23	octet	Default IP TTL.
mtat	24	long	Aging timeout, in seconds, to be used with Path MTU discovery (RFC 1191).
mtpt	25	mtpt	A table of MTU sizes to be used with Path MTU Discovery.
ifmt	26	short	MTU to be used on an interface.
brda	28	ip	Broadcast address in use on the client subnet. The system calculates the default from the subnet mask and the IP address.
rtsl	32	ip	Destination IP address to which the client sends router solicitation request.
strt	33	ippairs	A table of static routes for the client consisting of pairs (Destination, Router). You cannot specify the default route as a destination.
arpt	35	long	Timeout, in seconds, for ARP cache.
dttl	37	octet	Default TTL of TCP.
kain	38	long	Client TCP keepalive interval, in seconds.
nisd	40	str	Domain name for NIS.

*Table continues...*

Name	Code	Type	Description
nisv	41	iplist	A list of NIS servers
ntsv	42	iplist	A list of NTP servers.
vend	43	str	<p>Vendor Specific Options—must be specified in the following format:</p> <pre>vend=&lt;code&gt;:&lt;type&gt;:&lt;date&gt;:&lt;code&gt;:&lt;type&gt;:&lt;date&gt;</pre> <ul style="list-style-type: none"> <li>&lt;code&gt; is an int 1 &lt; &lt;code&gt; &lt;255 Do not use 0 and 255, they are reserved.</li> <li>&lt;type&gt; can be str, octet, short, long, ip, ip list, ippairs, mtpt, or raw. All types have the same format described above, except raw, which is a list of type values separated by white space. Example for raw: 0x4 0xAC 0x11 0x41</li> <li>&lt;data&gt; is the actual data. Data cannot contain single quotes.</li> </ul> <p>Syntax:</p> <p>You can specify more than one code, type, or data triplets, but you must separate each by a colon (:). You must enclose the entire vendor options within single quotes (').</p>
nnsv	44	iplist	A list of NetBIOS name servers (RFC 1001, 1002).
ndsv	45	iplist	A list of NetBIOS datagram distribution servers (RFC 1001, 1002).
nbnt	46	octet	NetBIOS node type (RFC 1001, 1002).
nbsc	47	str	NetBIOS scopt (RFC 1001, 1002).
xsfv	48	iplist	A list of font servers of X Window system.
xdmn	49	iplist	A list of display managers of X Window system.
dht1	58	short	<p>Specifies when the client should start RENEWING.</p> <p>DEFAULT: 500</p> <p>The default indicates that the client starts RENEWING after 50% of the lease duration passes.</p>
dht2	59	short	<p>Specifies when the client should start REBINDING.</p> <p>DEFAULT: 875</p> <p>The default indicates that the client starts REBINDING after 87.5% of the lease duration passes.</p>
nspd	64	str	The name of the client NIS+ domain.

*Table continues...*

Name	Code	Type	Description
nsps	65	iplist	A list of NIS+ servers.
miph	68	iplist	A list of mobile IP home agents.
smtp	69	iplist	A list of SMTP servers
pops	70	iplist	A list of POP3 servers.
nntp	71	iplist	A list of NNTP servers.
wwws	72	iplist	A list of WWW servers.
fngs	73	iplist	A list of Finger servers.
ircs	74	iplist	A list of IRC servers.
stsv	75	iplist	A list of StreetTalk servers.
stda	76	iplist	A list of STDA servers.
<p><b>* Note:</b>            For any code number not in this list you must use a default of <code>str</code> (string). For example:  <code>200:str:information</code>. Option numbers 0 and 255 are reserved.</p>			

## DHCP Server Option 241 parameters

To configure the DHCP Server Option 241 parameters, see [Configuring DHCP Server IP address pool options using CLI](#) on page 86.

The following table lists the parameters supported with the DHCP Server Option 241 command.

Parameter	Value	Description
s1ip	Value from 0.0.0.0 to 255.255.255.255	Primary server IP address
p1	Value from 1 to 65535	Primary server port number
a1	Value from 0 to 255	Primary server action code
r1	Value from 0 to 255	Primary server retry count
s2ip	Value from 0.0.0.0 to 255.255.255.255	Secondary server IP address
p2	Value from 1 to 65535	Secondary server port number
a2	Value from 0 to 255	Secondary server action code
r2	Value from 0 to 255	Secondary server retry count
dhcp	'y' yes 'n' no	Enable DHCP
xip	Value from 0.0.0.0 to 255.255.255.255	XAS server IP address

*Table continues...*

Parameter	Value	Description
xp	Value from 0 to 65535	XAS server port number
xa	Character string made up of the following character 'g' graphical XAS mode 'f' full screen XAS mode 's' secure XAS mode 'h' hidden Phone mode 'r' reduced Phone mode	XAS server action code (XAS Mode and Phone Mode)  Note that there is no explicit character to select text-mode. Instead, the lack of specifying graphical 'g' implies the XAS mode is text.  Also note that there is no explicit character to select Full phone mode. Instead, the lack of specifying either hidden 'h' or reduced 'r' implies the phone is to be provisioned for Full phone mode. Please be careful not to confuse Full Screen XAS mode 'f' with Full phone mode.  Note that hidden Phone mode and reduced Phone mode are supported on the IP Phone 2007 only.
unid	Character string up to 32 characters	Unique network identification
menulock	'f' full lock 'p' partial lock 'u' unlock	Menu lock mode
vq	'y' yes 'n' no	Enable 802.1Q for voice [1]
vcp	Value from 0 to 8	802.1Q control p bit for voice stream. Provisioning this value to 8 tells the phone to use the value it receives from the LLDP Network Policy TLV or from the call server
vmp	Value from 0 to 8	802.1Q media p bit for voice stream. Provisioning this value to 8 tells the phone to use the value it receives from the LLDP Network Policy TLV or from the call server
vlanf	'y' yes 'n' no	Enable VLAN filter on voice stream
nis	'a' auto negotiation '10' 10 Mbps '100' 100 Mbps	Network port speed [1]
nid	'a' auto negotiation 'f' full duplex 'h' half duplex	Network port duplex [1]
pc	'y' yes	Enable PC port

*Table continues...*

Parameter	Value	Description
	'n' no	
pcs	'a' auto negotiation '10' 10 Mbps '100' 100 Mbps	PC port speed
pcd	'a' auto negotiation 'f' full duplex 'h' half duplex	PC port duplex
dq	'y' yes 'n' no	Enable 802.1Q for PC port
dv	'y' yes 'n' no	Enable VLAN for data
dvid	Value from 1 to 4094	VLAN ID for data VLAN
dp	Value from 0 to 8	802.1Q p bit for data stream. Provisioning this value to 8 tells the phone to use the value it receives from the LLDP Network Policy TLV or from the call server
pcuntag	'y' yes 'n' no	Enable stripping of tags on packets forwarded to PC port
lldp	'y' yes 'n' no	Enable 802.1ab LLDP [1]
pk1	Character string of 16 characters representing 16 hexadecimal digits	S1 PK [2]
pk2	Character string of 16 characters representing 16 hexadecimal digits	S2 PK [2]
stickiness	'y' yes 'n' no	Enable stickiness (provisioning is persistent in the event a new info block is not received)
cachedip	'y' yes 'n' no	Enable cached IP
igarp	'y' yes 'n' no	Ignore GARP
srtp	'y' yes 'n' no	Enable SRTP-PSK
eap	'dis' disable 'md5' EAP-MD5 'peap' PEAP/MD5	Disable or choose an EAP authentication method [1] [2]

*Table continues...*

Parameter	Value	Description
	'tls' EAP-TLS	
eapid1	Character string up to 32 characters	802.1x (EAP) device ID1 [1] [2]
eapid2	Character string up to 32 characters	802.1x (EAP) device ID2 [1] [2]
eappwd	Character string up to 32 characters	802.1x (EAP) password [1] [2]
ca	Character string up to 80 characters	Certificate Authority (CA) server
cahost	Character string up to 32 characters	Certificate Authority (CA) host name
cadomain	Character string up to 50 characters	Certificate Authority (CA) domain name
cdiff	Value from 0 to 255	Diffserv code points for control messages
mdiff	Value from 0 to 255	Diffserv code points for media messages
prov	Character string up to 50 characters	Provisioning server address or URL (if the string is prefixed with "http://" the phone will connect to a HTTP server, otherwise the phone will connect to a TFTP server)
dns	Character string up to 50 characters	Primary DNS server URL
dns2	Character string up to 50 characters	Secondary DNS server URL
ct	Value from 0 to 15 for IP Phone 1100 series Value from 7 to 39 for IP Phone 2007	Contrast value
br	Value from 0 to 15	Brightness value
blt	'0' 5 seconds '1' 1 minute '2' 5 minutes '3' 10 minutes '4' 15 minutes '5' 30 minutes '6' 1 hour '7' 2 hours '8' always on	Backlight timer
dim	'y' yes 'n' no	As of UNISlim software release 3.4, the previously supported "dim" parameter is no longer supported since its functionality is superseded by the dimt parameter. The phone will still accept the dim parameter to prevent errors when reading existing provisioning files but the parameter will be ignored in favor of the new dimt parameter.
dimt	'0' Off	Phone inactivity timer to dim the screen (IP Phone 2007 only)

*Table continues...*

Parameter	Value	Description
	'1' 5 seconds '2' 1 minute '3' 5 minutes '4' 15 minutes '5' 30 minutes '6' 1 hour '7' 2 hours	
bt	'y' yes 'n' no	Enable Bluetooth (IP Phone 1140E and 1150E only)
zone	Character string up to 8 characters	Zone ID
file	Character string up of the following character 'z' read zone file 't' read type file 'd' read device file	For system specific provisioning file specifies what other provisioning files to read
hd	Character string up of the following character 'w' wired 'b' Bluetooth 'n' none	Headset type
ar	'y' yes 'n' no	Enable Auto-recovery
arl	'cr' critical 'ma' major 'mi' minor	Auto-recovery level
ll	'cr' critical 'ma' major 'mi' minor	Log level
ssh	'y' yes 'n' no	Enable SSH
sshid	Character string between 4 and 12 characters	SSH user ID [2]
sshpwd	Character string between 4 and 12 characters	SSH password [2]
bold	'y' yes	Enable bold on font display

*Table continues...*

Parameter	Value	Description
	'n' no	
menupwd	String between and 21 characters containing only numeric digits, asterisk (*) and hash (#) – i.e. only the dialpad symbols	Administrator password [2]
vvsources	'n' no VLAN 'a' auto VLAN via DHCP 'lv' auto VLAN via VLAN Name TLV 'lm' auto VLAN via Network Policy TLV	Source of VLAN information
srtpid	96 115 120	Payload type ID
ntqos	'y' yes 'n' no	Enable Automatic QoS
dscpovr	'y' yes 'n' no	DSCP Precedence Override
vpn	'y' yes 'n' no	Enable the UNISTim VPN Client (UVC) within the phone
vpntype	'1' Nortel VPN	Only Nortel VPN devices are supported at this time
vpnmode	'aggressive' 'main'	Authentication mode
vpnauth	'psk' preshared key 'certificate' X.509 certificate	Authentication credential When 'certificate' is provisioned, both a CA root certificate and a device certificates must be installed in the phone.
vpnauth	'0' none '1' password	X Authentication type
vpnpskuser	Character string up to 64 characters	PreShared Key (PSK) User ID
vpnpskpwd	Character string up to 64 characters	PreShared Key (PSK) password
vpnauthuser	Character string up to 64 characters	X Authentication User ID
vpnauthpwd	Character string up to 64 characters	X Authentication password
vpns1	Character string up to 64 characters	IP address or FQDN of the primary VPN server If a FQDN is entered, the remote user's local network must have access to DNS to resolve the entered name. Typically in a home

*Table continues...*



Parameter	Value	Description
		environment, this would be the service provider's DNS.
vpns2	Character string up to 64 characters	IP address or FQDN of the secondary VPN server
vpndiffcpy	'y' copy DSCP from inner packet 'n' use vpndiff value	Source of DSCP value for the tunnel traffic. Determines if DSCP value is copied from inner packet to outer packet or if vpndiff is used.
vpndiff	0–255	If vpndiffcpy=n, then this value is used for the DSCP value for the tunnel traffic
vpnmotd	0-999	Message of the Day (MOTD) timer
dcpsource1	'scep' 'pkcs12'	Method used to install device certificates
dcpactive1	'n' Inactive 'y' Active	Profile is active or not
dcppurpose1	Character string made up of the following character 'a' All applications 'v' VPN 'd' DTLS 's' SCR 'g' GXAS 'e' EAP-TLS 'l' Licensing	Specifies which phone applications can use this device certificate  Multiple values can be cascaded (e.g. 'dsg') but 'a' can only be used by itself
dcprenew1	Integer value, but also supports the following special values '-1' Never '0' Immediately	Number of days prior to certificate expiry that a certificate renewal is requested
dcpdelete1	'n' No action 'y' Delete	If set to 'y' forces the device certificate to be deleted
dcpautocn1	'0' Manual '1' Automatic	Automatically construct the Certificate Name using cadomain and cahost
dcpcaname1	Character string of 128 characters	CA name included in the SCEP request to identify requested CA (note that not all CA require the CA name)
dcphostnameoverride1	Character string of 128 characters	Override hostname (cahost) for this DCP only

*Table continues...*

Parameter	Value	Description
dcpattrcn1	Character string of 128 characters	If “Auto CN” is disabled, this value is used instead of combining cadomain and cahost
dcpattrextkeyusage1	Character string made up of one of the following characters ‘a’ anyExtendedKeyUsage ‘c’ clientAuth ‘i’ ipsecIKE (RFC 4945) ‘m’ iKEIntermediate ‘ ’ no Extended Key Usage	Define the Extended Key Usage attributes to be requested for the device certificate.  The default is clientAuth.
<p><b>* Note:</b></p> <p>[1]: Warning - changing this parameter could impact the network connectivity and may require manual correction</p> <p>[2]: Warning – provisioning this parameter via TFTP, HTTP, or DHCP means that secure information is transferred in clear text</p>		

## Deleting Option 241 parameters for DHCP server pool

Use this procedure to remove parameters or reset parameters to default values for DHCP Server Option 241 for IP Phones 1100, 1200, and 2000.

### Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. To set parameters to default, enter the following command:

```
{no | default } ip dhcp-server pool <poolName> option-241
<parameterList>
```

## Variable definitions

The following table describes the parameters for the { **no|default** } **ip dhcp-server pool** command.

Variable	Value
<poolName>	Specifies the name of the pool.

*Table continues...*

Variable	Value
<i>&lt;parameter list&gt;</i>	<p>Specifies the individual parameters to be removed.</p> <p>The format for <i>&lt;parameterList&gt;</i> is: Nortel-i2004–B,param1, param2, param3,...</p> <p>Note: The use of <b>Nortel-i2004–B</b> specific option at the beginning of the string is optional.</p> <p>See <a href="#">DHCP Server Option 241 parameters</a> on page 91 for the list of supported parameters.</p>

---

## Deleting Option 242 parameters for DHCP server pool

To configure Option 242 parameters, see [Configuring DHCP Server IP address pool options CLI](#) on page 86.

Use this procedure to remove parameters or reset parameters to default values for DHCP Server Option 242 for IP Phones 1600 and 9600 Series.

### Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. To set parameters to default, enter the following command:

```
{no | default} ip dhcp-server pool <poolName> option-242 [httpport]
[httpsrvr][mcipadd <ipv4AddrList>]
```

---

## Variable definitions

The following table describes the parameters for the { **no|default** } **ip dhcp-server pool** command.

Variable	Value
<i>&lt;poolName&gt;</i>	Specifies the name of the pool.
<i>mcipadd &lt;ipv4AddrList&gt;</i>	Specifies an IP Phone IPv4 address or list of addresses to be removed.

---

## Disabling DHCP Server IP address pools

Use this procedure to disable DHCP Server IP address pools.

### Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. At the prompt, enter the following command:

```
[no | default] ip dhcp-server pool <poolName>
```

---

## Variable definitions

The following table describes the parameters for the { `no|default` } `ip dhcp-server pool` command.

Variable	Value
<code>&lt;poolName&gt;</code>	Specifies the name of the pool.
<code>no</code>	Clears the specified DHCP Server IP address pool.
<code>default</code>	Returns the list to DHCP Server IP address pool to default, which is disabled.

---

## Configuring static IP addresses

Use this procedure to configure the entry of reserved IP addresses for static devices (such as printers).

### Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. At the prompt, enter the following command:

```
ip dhcp-server pool <poolName> host <A.B.C.D> <MACAddr>
```

---

## Variable definitions

The following table describes the parameters for the `ip dhcp-server pool <poolName> host` command.

Variable	Value
<poolName>	Specifies the name of the pool.
host <A.B.C.D> <MACAddr>	Specifies the static IP allocation, the host IP address. The format for <MACAddr> is H.H.H or XX:XX:XX:XX:XX:XX or XX.XX.XX.XX.XX.XX or XX-XX-XX-XX-XX-XX.

---

## Creating the IP DHCP Server Pool for a Vendor Class Identifier

Use this procedure to create the IP DHCP Server Pool for a Vendor Class Identifier.

### Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. At the prompt, enter the following command:

```
ip dhcp-server pool <poolName> option-60 <WORD> option-43 <WORD>
```

---

## Variable definitions

The following table describes the parameters for the `ip dhcp-server pool <poolName> option-60` command.

Variable	Value
option-60 <WORD>	Specifies the vendor class identifier.
option-43 <WORD>	Specifies the vendor specific information to be exchanged between clients and servers. Format is <option number>:<type (IP/ASCII string/hex)>:<value>.

# Chapter 10: UDP broadcast forwarding configuration using CLI

This chapter describes the procedures you can use to configure UDP broadcast forwarding using CLI. UDP broadcast forwarding is a general mechanism for selectively forwarding limited UDP broadcasts received on an IP interface to a configured IP address.

You cannot enable or disable the UDP broadcast forwarding feature on a global level. When you attach the first UDP forwarding list to a VLAN interface, the feature is enabled. When you remove the last UDP forwarding list from a VLAN, the feature is disabled.

---

## Prerequisites to UDP broadcast forwarding

- Enable IP routing globally.
- Enable IP routing and configure an IP address on the VLAN to be configured as a UDP forwarding interface.
- Ensure that a route (local or static) to the destination address is available on the switch.

### Important:

If you configure EAPOL on the switch, enable EAPOL prior to enabling UDP Forwarding, otherwise the UDP broadcast traffic matching UDP forward lists is forwarded regardless of the EAPOL port state (authorized, force unauthorized, or auto).

---

## UDP broadcast forwarding configuration procedures

To configure UDP broadcast forwarding, perform the following steps:

1. Create UDP protocol entries that specify the protocol associated with each UDP port that you want to forward.
2. Create a UDP forwarding list that specifies the destination IP addresses for each forwarding UDP port. (You can create up to 128 UDP forwarding lists.)
3. Apply UDP forwarding lists to local VLAN interfaces.

---

## Configuring UDP protocol table entries

Use the following procedure to create UDP protocol table entries that identify the protocols associated with specific UDP ports to forward.

### Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. At the command prompt, enter the following command:

```
ip forward-protocol udp [<forwarding_port> <protocol_name>]
```

---

## Variable definitions

The following table describes the parameters for the `ip forward-protocol udp` command.

Variable	Value
<forwarding_port>	Specifies the UDP port number. RANGE: 1–65535
<protocol_name>	Specifies the UDP protocol name.

---

## Displaying the UDP protocol table

Use the following procedure to display the configured UDP protocol table entries.

### Procedure

1. Log on to CLI to enter User EXEC mode.
2. At the command prompt, enter the following command:

```
show ip forward-protocol udp
```

The following information is displayed:

- UDP\_Port — Indicates the UDP ports.
- PROTOCOL\_NAME — Indicates the name of the associated protocol.

---

## Configuring a UDP forwarding list

Use the following procedure to configure a UDP forwarding list, which associates UDP forwarding ports with destination IP addresses. Each forwarding list can contain multiple port/destination entries.

A maximum of 16 port/destination entries per forwarding list and up to 128 forwarding lists can be configured.

### Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. At the command prompt, enter the following command:

```
ip forward-protocol udp portfwdlist <forward_list> <udp_port>
<dest_ip> [name <list_name>]
```

---

## Variable definitions

The following table describes the parameters for the `ip forward-protocol udp portfwdlist` command.

Variable	Value
<forward_list>	Specifies the ID of the UDP forwarding list. RANGE: 1–128
<udp_port>	Specifies the port on which the UDP forwarding originates.
<dest_ip>	Specifies the destination IP address for the UDP port.
<list_name>	Specifies the name of the UDP forwarding list being created (maximum 15 characters).

---

## Applying a UDP forwarding list to a VLAN

Use the following procedure to associate a UDP forwarding list with a VLAN interface. One list can be associated at a time.

The same UDP forwarding list can be associated to a maximum of 16 different VLANs.



**\* Note:**

Due to hardware limitations, a forwarding list cannot be applied unless a QoS filter is free. To obtain a free QoS filter, you can disable DHCP Relay (if not used) or use the following CLI commands:

```
Switch(config)#qos if-group name <name of the interface group> class unrestricted
Switch(config)#qos if-assign port all name <name of the interface group>
```

## Procedure

1. Enter VLAN Interface Configuration mode:

```
enable
configure terminal
interface vlan <vlan ID>
```

2. At the command prompt, enter the following command:

```
ip forward-protocol udp [vlan <vid>] [portfwddlist <forward_list>]
[broadcastmask <bcast_mask>] [maxttl <max_ttl>]
```

## Variable definitions

The following table describes the parameters for the `ip forward-protocol udp` command.

Variable	Value
<vid>	Specifies the VLAN ID on which to attach the UDP forwarding list. This parameter is optional, and if not specified, the UDP forwarding list is applied to the interface specified in the <code>interface vlan</code> command.
<forward_list>	Specifies the ID of the UDP forwarding list to attach to the selected VLAN interface.
<bcast_mask>	Specifies the 32-bit mask used by the selected VLAN interface to make forwarding decisions based on the destination IP address of the incoming UDP broadcast traffic. If you do not specify a broadcast mask value, the switch uses the mask of the interface to which the forwarding list is attached
<max_ttl>	Specifies the time-to-live (TTL) value inserted in the IP headers of the forwarded UDP packets coming out of the selected VLAN interface.  DEFAULT: 4

**\* Note:**

If you specify `maxttl` and/or `broadcastmask` values with no `portfwdlist` specified, the switch saves the settings for this interface. If you subsequently attach `portfwdlist` to this interface without defining the `maxttl` and/or `broadcastmask` values, the saved parameters are automatically attached to the list. But, if when specifying the `portfwdlist`, you also specify the `maxttl` and/or `broadcastmask`, your specified properties are used, regardless of any previous configurations.

---

## Displaying the UDP broadcast forwarding configuration

Use the following procedure to display the UDP broadcast forwarding configuration.

### Procedure

1. Log on to CLI to enter User EXEC mode.
2. At the command prompt, enter the following command:

```
show ip forward-protocol udp [interface [vlan <1-4094>]]
[portfwdlist [<portlist>]]
```

The following information is displayed:

- `UDP_PORT` — Indicates the UDP ports.
- `PROTOCOL_NAME` — Indicates the name of the protocol.

The following information is displayed for the UDP interfaces command:

- `INTF_ADDR` — Indicates the IP address of the interface.
- `FWD LISTID` — Identifies the UDP forwarding policy.
- `MAXTTL` — Indicates the maximum TTL.
- `RXPKTS` — Indicates the number of received packets.
- `FWDOKTS` — Indicates the number of forwarded packets.
- `DRPDEST UNREACH` — Indicates the number of dropped packets that cannot reach the destination.
- `DRP_UNKNOWN PROTOCOL` — Indicates the number of packets dropped with an unknown protocol.
- `BDCASTMASK` — Indicates the value of the broadcast mask.

The following information is displayed for the UDP `portfwdlist` command:

- `LIST_ID` — Specifies the UDP forwarding policy number.
- `NAME` — Specifies the name of the UDP forwarding policy.

---

## Variable definitions

The following table describes the parameters for the `show ip forward-protocol udp` command.

Variable	Value
[interface [vlan <1–4094>]]	Displays the configuration and statistics for a VLAN interface. If no VLAN is specified, the configuration for all UDP forwarding-enabled VLANs is displayed.
[portfwldlist [<forward_list>]]	Displays the specified UDP forwarding list. If no list is specified, a summary of all forwarding lists is displayed.

---

## Clearing UDP broadcast counters on an interface

Use the following procedure to clear the UDP broadcast counters on an interface.

### Procedure

1. Enter Privileged EXEC mode:  

```
enable
```
2. At the command prompt, enter the following command:  

```
clear ip forward-protocol udp counters <1-4094>
```

---

## Variable definitions

The following table describes the parameters for the `clear ip forward-protocol udp counters` command.

Variable	Value
<1–4094>	Specifies the VLAN ID.

# Chapter 11: Directed broadcasts configuration using CLI

This chapter describes the procedures you can use to configure and display the status of directed broadcasts.

---

## Configuring directed broadcasts

Use the following procedure to enable directed broadcasts on the switch.

 **Note:**

By default, directed broadcasts are disabled.

### Before you begin

- Enable IP routing globally.
- Enable IP routing and configure an IP address on the VLAN to be configured as a broadcast interface.
- Ensure that a route (local or static) to the destination address is available on the switch.

### Procedure

1. Enter Global Configuration mode:

```
enable
```

```
configure terminal
```

2. At the command prompt, enter the following command:

```
ip directed-broadcast enable
```

---

## Displaying the directed broadcast configuration

Use the following procedure to display the status of directed broadcasts on the switch.

**\* Note:**

By default, directed broadcasts are disabled.

**Procedure**

1. Log on to CLI to enter User EXEC mode.
2. At the command prompt, enter the following command:

```
show ip directed-broadcast
```

# Chapter 12: Static ARP and Proxy ARP configuration

This chapter describes the procedures you can use to configure Static ARP, Proxy ARP, and display ARP entries using the CLI.

---

## Configuring a static ARP entry

Use this procedure to configure a static ARP entry.

### Before you begin

- Enable IP routing globally.
- Enable IP routing and configure an IP address on the target VLAN.

### Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. At the command prompt, enter the following command:

```
[no] arp <A.B.C.D> <aa:bb:cc:dd:ee:ff> <unit/port> [vid <1-4094>]
```

---

## Variable definitions

The following table describes the parameters for the **arp** command.

Variable	Value
[no]	Removes the specified ARP entry.
<A.B.C.D>	Specifies the IP address of the device being set as a static ARP entry.
<aa:bb:cc:dd:ee:ff>	Specifies the MAC address of the device being set as a static ARP entry.

*Table continues...*

Variable	Value
<unit/port>	Specifies the unit and port number to which the static ARP entry is being added.
vid <1–4094>	Specifies the VLAN ID to which the static ARP entry is being added.

## Displaying ARP entries

Use the following procedure to display ARP entries.

### Procedure

1. Log on to CLI to enter User EXEC mode.
2. At the command prompt, enter the following command:

```
show arp-table
```

OR

```
show arp [<ip-addr>] [-s <subnet> <mask>] [static <ip-addr> [-s <subnet> <mask>]] [<mac-addr>] [dynamic <ip-addr> [-s <subnet> <mask>]] [<mac-addr>] {<mac_addr>} {summary} [vlan <1-4096>]
```

### \* Note:

The `show arp` command is invalid if the switch is not in Layer 3 mode.

The following information is displayed:

- IP Address — Specifies the IP address of the ARP entry.
- Age (min) — Displays the ARP age time.
- MAC Address — Specifies the MAC address of the ARP entry.
- VLAN-Unit/Port/Trunk — Specifies the VLAN/port of the ARP entry.
- Flags — Specifies the type of ARP entry: S=Static, D=Dynamic, L=Local, B=Broadcast.

## Variable definitions

The following table describes the parameters for the `show arp` command.

Variable	Value
dynamic <ip-addr> [-s <subnet> <mask>]	Displays dynamic entries for the specified subnet. If you do not specify a subnet, all dynamic entries are displayed.

*Table continues...*

Variable	Value
<ip-addr>	Specifies the IP address of the ARP entry to be displayed.
<mac-addr>	Specifies the MAC address of the ARP entry to be displayed. The format can be H.H.H, xx:xx:xx:xx:xx:xx, xx.xx.xx.xx.xx.xx, or xx-xx-xx-xx-xx-xx.
—s <subnet> <mask>	Displays ARP entries for the specified subnet only.
static <ip-addr> [-s <subnet> <mask>]	Displays static entries for the specified subnet. If you do not specify a subnet, all configured static entries are displayed, including those without a valid route.
summary	Displays a summary of ARP entries.
vlan <1–4096>	Displays ARP entries for a specific VLAN.

---

## Configuring a global timeout for ARP entries

Use the following procedure to configure an aging time for the ARP entries.

### Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. At the command prompt, enter the following command:

```
arp timeout <timeout>
```

---

## Variable definitions

The following table describes the parameters for the `ip arp timeout` command.

Variable	Value
timeout	Specifies the amount of time in minutes before an ARP entry ages out.  DEFAULT: 360 minutes.  RANGE: 5–360.



---

## Clearing the ARP cache

Use the following procedure to clear the cache of ARP entries.

### Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. At the command prompt, enter the following command:

```
clear arp-cache
```

---

## Configuring proxy ARP status

Use this procedure to enable proxy ARP functionality on a VLAN.

### \* Note:

By default, proxy ARP is disabled.

### Before you begin

- Enable IP routing globally.
- Enable IP routing and configure an IP address on the VLAN to be configured as a Proxy ARP interface.

### Procedure

1. Enter VLAN Interface Configuration mode:

```
enable
configure terminal
interface vlan <vlan ID>
```

2. At the command prompt, enter the following command:

```
[default] [no] ip arp-proxy enable
```

---

## Variable definitions

The following table describes the parameters for the **ip arp-proxy enable** command.

Variable	Value
[default]	Disables proxy ARP functionality on the VLAN.
[no]	Disables proxy ARP functionality on the VLAN.

---

## Displaying proxy ARP status on a VLAN

Use the following procedure to display the status of proxy ARP on a VLAN.

### Procedure

1. Log on to CLI to enter User EXEC mode.
2. At the command prompt, enter the following command:

```
show ip arp-proxy interface [vlan <vid>]
```

The following information is displayed:

- Vlan — Identifies a VLAN.
- Proxy ARP status — Specifies the status of Proxy ARP on the VLAN.

---

## Variable definitions

The following table describes the parameters for the `show ip arp-proxy interface` command.

Variable	Value
<vid>	Specifies the ID of the VLAN to display. RANGE: 1–4094.

# Chapter 13: IP blocking configuration using CLI

This chapter describes the procedures you can use to configure and display the status of IP blocking in a stack using CLI.

---

## Configuring IP blocking for a stack

Use this procedure to set the IP blocking mode in a stack.

### Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. At the command prompt, enter the following command:

```
ip blocking-mode {full | none}
```

---

## Variable Definitions

The following table describes the parameters for the `ip blocking-mode` command.

Variable	Value
full	Select this parameter to set IP blocking to full, which never allows a duplicate IP address in a stack.
none	Select this parameter to set IP blocking to none, which allows duplicate IP addresses unconditionally.

---

## Configuring IP blocking mode to default value

Use this procedure to set the IP blocking mode to its default value of none.

### Procedure

1. Enter Global Configuration mode:

```
enable
```

```
configure terminal
```

2. At the command prompt, enter the following command:

```
default ip blocking-mode
```

---

## Displaying IP blocking mode

Use this procedure to display the IP blocking mode on the switch.

### Procedure

1. Enter Global Configuration mode:

```
enable
```

```
configure terminal
```

2. At the command prompt, enter the following command:

```
show ip blocking-mode
```

---

## Displaying IP blocking state

Use this procedure to display the IP blocking state on the switch.

### Procedure

1. Enter Global Configuration mode:

```
enable
```

```
configure terminal
```

2. At the command prompt, enter the following command:

```
show ip blocking
```

---

## Clearing the IP blocking mode state

Use this procedure to clear the current IP blocking-mode state.

## Procedure

1. Enter Global Configuration mode:

```
enable
```

```
configure terminal
```

2. At the command prompt, enter the following command:

```
clear ip-blocking
```

# Chapter 14: IGMP snooping configuration using CLI

This chapter describes the procedures you can use to configure and display IGMP snooping parameters using CLI.

---

## Configuring IGMP snooping on a VLAN

Enable IGMP snooping on a VLAN to forward the multicast data to only those ports that are members of the multicast group.

**\* Note:**

IGMP snooping is disabled by default.

### Procedure

1. Enter VLAN Interface Configuration mode:

```
enable
configure terminal
interface vlan <vlan ID>
```

2. At the command prompt, enter the following command:

```
[default] [no] ip igmp snooping
```

### OR

In Global Configuration command mode, enter the following at the command prompt:

```
vlan igmp {1-4094} snooping {enable | disable}
```

---

## Variable definitions

The following table describes the parameters for the `ip igmp snooping` command.

Variable	Value
default	Restores IGMP snooping for the VLAN to default. DEFAULT: Disabled
no	Disables IGMP snooping for the selected VLAN.

---

## Configuring IGMP proxy on a VLAN

Use the following procedure to enable IGMP proxy on a snoop-enabled VLAN. With IGMP proxy enabled, the switch consolidates incoming report messages into one proxy report for that group.

**\* Note:**

IGMP proxy is disabled by default.

### Before you begin

Enable snoop on the VLAN.

### Procedure

1. Enter VLAN Interface Configuration mode:

```
enable
configure terminal
interface vlan <vlan ID>
```

2. At the command prompt, enter the following command:

```
[default] [no] ip igmp proxy
```

### OR

In Global Configuration command mode, enter the following at the command prompt:

```
vlan igmp {1-4094} proxy {enable | disable}
```

---

## Variable definitions

The following table describes the parameters for the `ip igmp proxy` command.

Variable	Value
default	Restores IGMP proxy on the selected VLAN to default. DEFAULT: Disabled
no	Disables IGMP proxy on the selected VLAN.

## Configuring static mrouter ports on a VLAN

IGMP snoop considers the port on which the IGMP query is received as the active IGMP multicast router (mrouter) port.

To forward the IGMP reports to additional ports, you can configure the additional ports as static mrouter ports.

**\* Note:**

By default, the switch forwards incoming IGMP Membership Reports only to the active mrouter port.

### Procedure

1. Enter VLAN Interface Configuration mode:

```
enable
configure terminal
interface vlan <vlan ID>
```

2. At the command prompt, enter the following command:

```
[default] [no] ip igmp mrouter <portlist>
```

### OR

To configure IGMPv1 or IGMPv2 static mrouter ports, in Global Configuration command mode, enter the following at the command prompt:

```
vlan igmp {1-4094} [v1-members | v2-members] {add | remove}
<portlist>
```

## Variable definitions

The following table describes the parameters for the `[default] [no] ip igmp mrouter` command.

Variable	Value
default	Removes all static mrouter ports.
no	Removes the specified static mrouter ports. If no ports are specified, all static mrouter ports are removed.



## Configuring IGMP parameters on a VLAN

Use the following procedure to configure the IGMP parameters on a VLAN.

### ! Important:

The query interval and robustness values must be the same as those configured on the interface (VLAN) of the IGMP querier router.

### Procedure

1. Enter VLAN Interface Configuration mode:

```
enable
configure terminal
interface vlan <vlan ID>
```

2. At the command prompt, enter the following command:

```
[default] ip igmp [last-member-query-interval <last-mbr-query-int>]
[query-interval <query-int>] [query-max-response <query-max-resp>]
{robust-value <robust-val>} [version <1-3>]
```

### OR

3. Enter Global Configuration mode:

```
enable
configure terminal
```

4. `vlan igmp {1-4094} [query-interval <query-int>] [robust-value <robust-val>]`

## Variable definitions

The following table describes the parameters for the `ip igmp [query-interval] [robust-value]` command.

Variable	Value
default	Sets the selected parameter to the default value. If no parameters are specified, snoop is disabled and all IGMP parameters are set to their defaults.
<last-mbr-query-int>	Sets the maximum response time (in 1/10 seconds) that is inserted into group-specific queries sent in response to leave group messages. This parameter is also the time between group-specific query messages. This value is not configurable for IGMPv1.

*Table continues...*

Variable	Value
	<p>Decreasing the value reduces the time to detect the loss of the last member of a group.</p> <p>RANGE: 0–255</p> <p>DEFAULT: 10 (1 second)</p> <p><b>* Note:</b> It is recommended to configure this parameter to values higher than 3. If a fast leave process is not required, it is recommended to have a value above 10. (The value 3 is equal to 0.3 of a second, and 10 is equal to 1.0 second.)</p>
<query-int>	<p>Sets the frequency (in seconds) at which host query packets are transmitted on the VLAN.</p> <p>RANGE: 1–65535</p> <p>DEFAULT: 125 seconds</p>
<query-max-resp>	<p>Specifies the maximum response time (in 1/10 seconds) advertised in IGMPv2 general queries on this interface.</p> <p>RANGE: 0–255</p> <p>DEFAULT: 100 (10 seconds)</p>
<robust-val>	<p>Specifies tuning for the expected packet loss of a network. This value is equal to the number of expected query packet losses for each serial query interval, plus 1.</p> <p><b>* Note:</b> If a network is expected to lose query packets, increase the robustness value and ensure that the robustness value is equal to the configured value on the multicast router (IGMP querier).</p> <p>RANGE: 0–255</p> <p>DEFAULT:</p>

*Table continues...*

Variable	Value
	2 (meaning that one query for each query interval can be dropped without aging out).

## Displaying IGMP interface information

Use the following procedure to display IGMP interface information.

### Procedure

1. Enter Privileged EXEC mode:

```
enable
```

2. At the command prompt, enter the following command:

```
show ip igmp interface [vlan <vid>] OR show vlan igmp <vid>
```

The following information is displayed with the `show ip igmp interface` command:

- VLAN — Indicates the VLAN on which IGMP is configured.
- Query Intvl — Specifies the frequency (in seconds) at which host query packets are transmitted on the interface.
- Vers — Specifies the version of IGMP configured on the interface.
- Oper Vers — Specifies the version of IGMP running on this interface.
- Querier — Specifies the address of the IGMP querier on the IP subnet.
- Query MaxRspT — Indicates the maximum query response time (in tenths of a second) advertised in IGMPv2 queries on this interface.
- Wrong Query — Indicates the number of queries received whose IGMP version does not match the interface version. You must configure all routers on a LAN to run the same version of IGMP. Thus, if queries are received with the wrong version, a configuration error occurs.
- Joins — Indicates the number of times a group membership was added on this interface.
- Robust — Specifies the robust value configured for expected packet loss on the interface.
- LastMbrQuery — Indicates the maximum response time (in tenths of a second) inserted into group-specific queries sent in response to leave group messages, and is also the amount of time between group-specific query messages. Use this value to modify the leave latency of the network. A reduced value results in reduced time to detect the loss of the last member of a group. This does not apply if the interface is configured for IGMPv1.
- Send Query — Indicates whether the `ip igmp send-query` feature is enabled or disabled. Values are YES or NO. Default is disabled.

The following information is displayed with the `show vlan igmp` command.

- Snooping — Indicates whether snooping is enabled or disabled.
- Proxy — Indicates whether proxy snoop is enabled or disabled.
- Robust Value — Indicates the robustness value configured for expected packet loss on the interface.
- Query Time — Indicates the frequency (in seconds) at which host query packets are transmitted on the interface.
- IGMPv1 Static Router Ports — Indicates the IGMPv1 static mrouter ports.
- IGMPv2 Static Router Ports — Indicates the IGMPv2 static mrouter ports.
- Send Query — Indicates whether the `ip igmp send-query` feature is enabled or disabled. Values are YES or NO. Default is disabled.

---

## Variable definitions

The following table describes the parameters for the `show ip igmp` command.

Variable	Value
[vlan <vid>]	Specifies the VLAN ID for which to display IGMP information.  RANGE: 1–4094

---

## Displaying IGMP group membership information

Use the following procedure to display IGMP group membership information and to show the learned multicast groups and attached ports.

### Procedure

1. Enter Privileged EXEC mode:

```
enable
```

2. At the command prompt, enter the following command:

```
show ip igmp group [count] [group <A.B.C.D>] [member-subnet  
<A.B.C.D>/<0-32>]
```

```
show vlan multicast membership <vid>
```

The following information is displayed after the `show ip igmp group` command:

- Group Address — Indicates the multicast group address.

- VLAN — Indicates the VLAN interface on which the group exists.
- Member Address — Indicates the IP address of the IGMP receiver (host or IGMP reporter). The IP address is 0.0.0.0 if the type is static.
- Expiration — Indicates the time left before the group report expires. This variable is updated upon receiving a group report.
- Type — Specifies the type of membership : static or dynamic
- In Port — Identifies the member port for the group. This is the port on which group traffic is forwarded, and in those cases where the type is dynamic, it is the port on which the IGMP join was received.

The following information is displayed after the `show vlan multicast membership` command:

- Multicast Group Address — Indicates the multicast group address
- In Port — Indicates the physical interface or the logical interface (VLAN) that received group reports from various sources.

---

## Variable definitions

The following table describes the parameters for the `show ip igmp group` command.

Variable	Value
Group Address	Indicates the multicast group address.
VLAN	Indicates the VLAN interface on which the group exists.
Member Address	Indicates the IP address of the IGMP receiver (host or IGMP reporter). The IP address is 0.0.0.0 if the type is static.
Expiration	Indicates the time left before the group report expires. This variable is updated upon receiving a group report.
Type	Specifies the type of membership: static or dynamic
In Port	Identifies the member port for the group. This is the port on which group traffic is forwarded, and in those cases where the type is dynamic, it is the port on which the IGMP join was received

---

## Displaying IGMP cache Information

Use the following procedure to show the learned multicast groups in the cache and the IGMPv1 version timers.

**\* Note:**

Using the `show ip igmp cache` command may not display the expected results in some configurations. If the expected results are not displayed, use the `show ip igmp group` command to view the information.

**Procedure**

1. Enter Privileged EXEC mode:

```
enable
```

2. At the command prompt, enter the following command:

```
show ip igmp cache
```

The following information is displayed:

- Group Address — Indicates the multicast group address.
- VLAN ID — Indicates the VLAN interface on which the group exists.
- Last Reporter — Indicates the last IGMP host to join the group.
- Expiration — Indicates the group expiration time (in seconds).
- V1 Host Timer — Indicates the time remaining until the local router assumes that no IGMP version 1 members exist on the IP subnet attached to the interface. Upon hearing an IGMPv1 membership report, this value is reset to the group membership timer. When the time remaining is nonzero, the local interface ignores any IGMPv2 Leave messages that it receives for this group.
- Type — Indicates whether the entry is learned dynamically or is added statically.

---

## Flushing the IGMP router table

Use the following procedure to flush the IGMP router table.

**Procedure**

1. Enter Global Configuration mode:

```
enable
```

```
configure terminal
```

2. At the command prompt, enter the following command:

```
ip igmp flush vlan <vid> {grp-member|mrouter}
```

---

## Variable definitions

The following table describes the parameters for the `ip igmp flush vlan` command.

Variable	Value
{grp-member mrouter}	Flushes the table specified by type.

## Configuring IGMP router alert on a VLAN

Use the following procedure to enable the router alert feature.

This feature instructs the router to drop control packets that do not have the router-alert flag in the IP header.

### \* Note:

To maximize your network performance, it is recommended that you set the router alert option according to the version of IGMP currently in use:

- IGMPv1 — Disable
- IGMPv2 — Enable
- IGMPv3 — Enable

### Procedure

1. Enter VLAN Interface Configuration mode:

```
enable
configure terminal
interface vlan <vlan ID>
```

2. At the command prompt, enter the following command:

```
[default] [no] ip igmp router-alert
```

## Variable definitions

The following table describes the parameters for the `ip igmp router-alert` command.

Variable	Value
default	Disables the router alert option.
no	Disables the router alert option.

# Chapter 15: IP routing configuration using Enterprise Device Manager

The ERS 3500 Series are Layer 3 switches. This means that a regular Layer 2 VLAN becomes a routable Layer 3 VLAN if an IP address is attached to the VLAN. When routing is enabled in Layer 3 mode, every Layer 3 VLAN is capable of routing and carrying the management traffic. You can use any Layer 3 VLAN instead of the Management VLAN to manage the switch.

---

## Configuring global IP routing status and ARP lifetime using EDM

Use this procedure to enable and disable global routing at the switch level and to configure the ARP lifetime.

By default, routing is disabled.

### Procedure

1. From the navigation tree, double-click **IP**.
2. In the IP tree, click **IP**.
3. In the IP work area, click the **Globals** tab.
4. In the Globals section, configure Forwarding and ARPLife Time as required.
5. On the toolbar, click **Apply**.
6. On the toolbar, you can click **Refresh** verify the configuration.

---

## Variable definitions

The following table describes the variables associated with configuring global routing and ARP lifetime.



Variable	Value
<b>Forwarding</b>	Indicates whether routing is enabled (forwarding) or disabled (nonforwarding) on the switch.
<b>DefaultTTL</b>	Indicates the default time-to-live (TTL) value for a routed packet. TTL is the maximum number of seconds elapsed before a packet is discarded. The value is inserted in the TTL field of the IP header of datagrams when one is not supplied by the transport layer protocol. The TTL field is also reduced by one each time the packet passes through a router.  RANGE: 1–255  DEFAULT: 64 seconds
<b>ReasmTimeout</b>	Indicates the maximum number of seconds that received fragments are held while they await reassembly at this entity.  DEFAULT: 60 seconds
<b>ARPLifeTime</b>	Specifies the lifetime in minutes of an ARP entry within the system.  RANGE: 5–360  DEFAULT: 360 minutes
<b>DirectedBroadcast</b>	Enables and disables IP directed broadcast.

---

## Configuring an IP address and enabling routing for a VLAN

Use the following procedure to configure an IP address and enable routing for a VLAN.

### Procedure

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, click **VLANs**.
3. In the VLAN work area, select a VLAN by clicking the applicable row.
4. On the toolbar, click **IP**

5. On the toolbar, click **Insert**.
6. In the Insert IP Address section, configure as required.
7. Click **Insert**.

---

## Variable definitions

The following table describes the variables associated with the Insert IP Address field.

Variable	Value
<b>IpAddress</b>	Specifies the IP address to associate with the selected VLAN.
<b>NetMask</b>	Specifies the subnet mask.
<b>MacOffset</b>	Specifies the value used to calculate the VLAN MAC address, which is offset from the switch MAC address.  RANGE: 1–256  Specify the value 1 for the Management VLAN only. If no MAC offset is specified, the switch applies one automatically.

---

## Displaying configured IP Addresses using EDM

Use the following procedure to display configured IP addresses on the switch.

### Procedure

1. From the navigation tree, double-click **IP**.
2. In the IP tree, click **IP**.
3. In the IP work area, click the **Addresses** tab.

---

## Variable definitions

The following table describes the variables associated with displaying IP addresses.

Variable	Value
<b>IfIndex</b>	Specifies the VLAN ID.

*Table continues...*

Variable	Value
<b>IpAddress</b>	Specifies the associated IP address.
<b>NetMask</b>	Specifies the subnet mask.
<b>BcastAddrFormat</b>	Specifies the format of the IP broadcast address.
<b>ReasmMaxSize</b>	Specifies the size of the largest IP datagram that this entity can reassemble from fragmented datagrams received on this interface.
<b>VlanId</b>	Specifies the VLAN ID number. A value of -1 indicates that the VLAN ID is ignored.
<b>MacOffset</b>	Specifies the value used to calculate the VLAN MAC address, which is offset from the switch MAC address.

# Chapter 16: Static route configuration using Enterprise Device Manager

This chapter describes the procedures you can use to configure static routes using Enterprise Device Manager.

---

## IP route management using EDM

Use the following procedures to display and filter IP route information.

---

### Displaying IP routes using EDM

Use the following procedure to display the different routes known to the switch.

Routes are not be displayed until at least one port in the VLAN has link.

#### Procedure

1. From the navigation tree, double-click **IP**.
2. In the IP tree, click **IP**.
3. In the IP work area, click the **Routes** tab.

### Variable definitions

The following table describes the variables associated with displaying IP route information.

Variable	Value
<b>Dest</b>	Specifies the destination address of the route.
<b>Mask</b>	Specifies the subnet mask for the route.
<b>NextHop</b>	Specifies the next hop for the route.
<b>HopOrMetric</b>	Specifies the metric associated with the route.

*Table continues...*

Variable	Value
<b>Interface</b>	Specifies the interface associated with the route.
<b>Proto</b>	Specifies the protocol associated with the route. Options are local or static.
<b>PathType</b>	Specifies the route path type: <ul style="list-style-type: none"> <li>• i — indirect</li> <li>• d — direct</li> <li>• B — best</li> <li>• U — unresolved</li> </ul>
<b>Pref</b>	Specifies the preference value associated with the route.

## Filtering route information using EDM

Use the following procedure to filter the routes displayed in the Routes tab to display only the desired switch routes.

### Procedure

1. From the navigation tree, double-click **IP**.
2. In the IP tree, click **IP**.
3. In the IP work area, click the **Routes** tab.
4. On the toolbar, click **Filter**.
5. In the Filter route section, configure as required.
6. Click **Filter**.

## Variable definitions

The following table describes the variables associated with filtering route information.

Variable	Value
<b>Condition</b>	When using multiple filter expressions on the tab, this is the condition that is used to join them together.
<b>Ignore Case</b>	Indicates whether filters are case sensitive or insensitive.
<b>Column</b>	Indicates the type of criteria to apply to values used for filtering.
<b>All Records</b>	Select this check box to clear any filters and display all rows.

*Table continues...*

Variable	Value
<b>Dest</b>	Select this check box and enter a value to filter on the route destination value.
<b>Mask</b>	Select this check box and enter a value to filter on the route destination subnet mask value.
<b>NextHop</b>	Select this check box and enter a value to filter on the route next hop value.
<b>HopOrMetric</b>	Select this check box and enter a value to filter on the hop count or metric of the route.
<b>Interface</b>	Select this check box and enter a value to filter on the interface associated with the route.
<b>Proto</b>	Select this check box and enter a value to filter on the route protocol.
<b>PathType</b>	Select this check box and enter a value to filter on the route path type.
<b>Pref</b>	Select this check box and enter a value to filter on the route preference value.

---

## Configuring static routes using EDM

Use the following procedure to configure static routes for the switch.

### Before you begin

- Enable IP routing globally.
- Enable IP routing and configure an IP address on the VLANs to be routed.

### Procedure

1. From the navigation tree, double-click **IP**.
2. In the IP tree, click **IP**.
3. In the IP work area, click the **Static Routes** tab.
4. On the toolbar, click **Insert**.
5. In the Insert Static routes section, configure as required.
6. Click **Insert**.

---

## Variable definitions

The following table describes the variables associated with configuring static routes.

Variable	Value
<b>Dest</b>	Specifies the destination IP address of the route. DEFAULT: 0.0.0.0
<b>Mask</b>	Specifies the destination mask of the route.
<b>NextHop</b>	Specifies the IP address of the next hop of this route.
<b>Metric</b>	Represents the cost of the static route. It is used to choose the best route (the one with the smallest cost) to a certain destination. If this metric is not used, the value is set to -1. RANGE: 1–65535
<b>IfIndex</b>	Specifies the interface on which the static route is configured.
<b>Enable</b>	Specifies whether the route is administratively enabled (true) or disabled (false).
<b>Status</b>	Specifies the operational status of the route.

---

## Displaying TCP information for the switch using EDM

Use the following procedure to display Transmission Control Protocol (TCP) information for the switch.

### Procedure

1. From the navigation tree, double-click **IP**.
2. In the IP tree, click **TCP/UDP**.
3. In the TCP/UDP work area, click the **TCP Globals** tab.

---

## Variable definitions

The following table describes the variables associated with displaying TCP information for the switch.

Variable	Value
<b>RtoAlgorithm</b>	Specifies the algorithm used to determine the timeout value used for retransmitting unacknowledged octets.

*Table continues...*

Variable	Value
<b>RtoMin</b>	Specifies the minimum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds.
<b>RtoMax</b>	Specifies the maximum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds.
<b>MaxConn</b>	Specifies the limit on the total number of TCP connections that the entity can support. In entities where the maximum number of connections is dynamic, this object contains the value -1.

## Displaying TCP Connections using EDM

Use the following procedure to display information about the current TCP connections.

### Procedure

1. From the navigation tree, double-click **IP**.
2. In the IP tree, click **TCP/UDP**.
3. In the TCP/UDP work area, click the **TCP Connections** tab.

## Variable definitions

The following table describes the variables associated with TCP connections.

Variable	Value
<b>LocalAddressType</b>	Specifies the local IP address type for this TCP connection.
<b>LocalAddress</b>	Specifies the local IP address for this TCP connection. In the case of a connection in the listen state, which is willing to accept connections for any IP interface associated with the node, the value 0.0.0.0 is used.
<b>LocalPort</b>	Specifies the local port number for this TCP connection.
<b>RemAddressType</b>	Specifies the remote IP address type for this TCP connection.
<b>RemAddress</b>	Specifies the remote IP address for this TCP connection.

*Table continues...*



Variable	Value
<b>RemPort</b>	Specifies the remote port number for this TCP connection.
<b>State</b>	Specifies the state of this TCP connection.

---

## Displaying TCP Listeners using EDM

Use the following procedure to display information about the current TCP listeners on the switch.

### Procedure

1. From the navigation tree, double-click **IP**.
2. In the IP tree, click **TCP/UDP**.
3. In the TCP/UDP work area, click the **TCP Listeners** tab.

---

## Variable definitions

The following table describes the variables associated with TCP listeners.

Variable	Value
<b>LocalAddressType</b>	Specifies the IP address type of the local TCP listener.
<b>LocalAddress</b>	<p>Specifies the local IP address of the TCP listener. The value of this field can be represented in three possible ways, depending on the characteristics of the listening application:</p> <ul style="list-style-type: none"> <li>• For an application willing to accept both IPv4 and IPv6 datagrams, the value of this object is a zero-length octet string, and the value of the corresponding LocalAddressType field is unknown.</li> <li>• For an application willing to accept either IPv4 or IPv6 datagrams, the value of this object must be 0.0.0.0 or ::, with the LocalAddressType identifying the supported address type.</li> <li>• For an application that is listening for data destined only to a specific IP address, the value of this object is the specific local address, with LocalAddressType identifying the supported address type.</li> </ul>
<b>LocalPort</b>	Specifies the local port number for this TCP connection.

## Displaying UDP endpoints using EDM

Use the following procedure to display information about the UDP endpoints.

### Procedure

1. From the navigation tree, double-click **IP**.
2. In the IP tree, click **TCP/UDP**.
3. In the TCP/UDP work area, click the **UDP Endpoints** tab.
4. On the toolbar, you can click **Refresh** to refresh the information displayed.

## Variable definitions

The following table describes the variables associated with UDP endpoints.

Variable	Value
<b>LocalAddressType</b>	Specifies the local address type (IPv6 or IPv4).
<b>LocalAddress</b>	<p>Specifies the local IP address for this UDP listener. In the case of a UDP listener that accepts datagrams for any IP interface associated with the node, the value 0.0.0.0 is used. The value of this field can be represented in three possible ways:</p> <ul style="list-style-type: none"> <li>• For an application willing to accept both IPv4 and IPv6 datagrams, the value of this object is a zero-length octet string, and the value of the corresponding LocalAddressType field is unknown.</li> <li>• For an application willing to accept either IPv4 or IPv6 datagrams, the value of this object must be 0.0.0.0 or ::, with the LocalAddressType identifying the supported address type.</li> <li>• For an application that is listening for data destined only to a specific IP address, the value of this object is the address for which this node is receiving packets, with LocalAddressType identifying the supported address type.</li> </ul>
<b>LocalPort</b>	Specifies the local port number for this UDP listener.
<b>RemoteAddressType</b>	Displays the remote address type (IPv6 or IPv4).
<b>RemoteAddress</b>	Displays the remote IP address for this UDP endpoint. If datagrams from all remote systems are to be accepted, this value is a zero-length octet string. Otherwise, the address of the remote system from which datagrams are to be accepted (or to which all datagrams are to be sent) is displayed with

*Table continues...*

Variable	Value
	the RemoteAddressType identifying the supported address type.
<b>RemotePort</b>	Displays the remote port number. If datagrams from all remote systems are to be accepted, this value is zero.
<b>Instance</b>	Distinguishes between multiple processes connected to the same UDP endpoint.
<b>Process</b>	Displays the ID for the UDP process.

# Chapter 17: DHCP relay configuration using Enterprise Device Manager

This chapter describes the procedures you can use to configure DHCP relay using Enterprise Device Manager.

---

## DHCP relay configuration procedures

To configure DHCP using Enterprise Device Manager, perform the following steps:

1. Specify DHCP relay configuration.
2. Specify the remote DHCP server as the destination.
3. Enable DHCP relay on the VLAN.

---

## Configuring DHCP Forwarding

Use these procedures to configure DHCP forwarding.

---

## Enabling or disabling DHCP Forwarding

Use the following procedure to enable or disable DHCP forwarding.

### Procedure

1. From the navigation tree, double-click **IP**.
2. In the IP tree, click **DHCP Relay**.
3. In the DHCP Relay work area, click the **DHCP Globals** tab.
4. In the DhcpForwardingEnabled section, check box to enable or uncheck box to disable.
5. On the toolbar, click **Apply**.

---

## Configuring DHCP Forwarding maximum frame size globally

Use the following procedure to specify the maximum frame size the DHCP relay agent can forward to the DHCP server.

### Procedure

1. From the navigation tree, double-click **IP**.
2. In the IP tree, click **DHCP Relay**.
3. In the DHCP Relay work area, click the **DHCP Globals** tab.
4. In the DhcpForwardingMaxFrameLength section, enter the frame length between 576 and 1536 bytes.

 **Note:**

The default value is 576 bytes.

5. On the toolbar, click **Apply**.

---

## Configuring DHCP Relay using EDM

Use this procedure to configure DHCP Relay.

### Procedure

1. From the navigation tree, double-click **IP**.
2. In the IP tree, click **DHCP Relay**.
3. In the DHCP Relay work area, click the **DHCP Relay** tab.
4. Click **Insert**.
5. In the Insert section, configure as required.
6. Click **Insert**.
7. On the toolbar, you can click **Refresh** to verify the configuration.

---

## Variable definitions

The following table describes the variables associated with configuring the DHCP relay.

Variable	Value
<b>AgentAddr</b>	The IP address of the local VLAN serving as the DHCP relay agent.
<b>ServerAddr</b>	The IP address of the remote DHCP server.
<b>Enable</b>	Enables (selected) or disables (cleared) DHCP relay.
<b>Mode</b>	Indicates whether the relay instance applies for BOOTP packets, DHCP packets, or both.

---

## Configuring DHCP Relay with Option 82 globally using EDM

Use this procedure to enable DHCP Relay Option 82 globally.

### Procedure

1. From the navigation tree, double-click **IP**.
2. In the IP tree, click **DHCP Relay**.
3. In the DHCP Relay work area, click the **DHCP Globals** tab.
4. In the DhcpForwardingOption82Enabled section, check the box to enable.
5. On the toolbar, click **Apply**.

---

## Configuring DHCP Relay with Option 82 for a VLAN using EDM

Use this procedure to configure DHCP Relay with Option 82 for a VLAN.

### Before you begin

- Enable IP routing globally.
- On the VLAN: enable IP Routing and configure an IP address to be set as the DHCP Relay agent.
- Ensure that a route, either local or static, is available on the switch to the destination DHCP server.

### Procedure

1. From the navigation tree, double-click **IP**.
2. In the IP tree, click **DHCP Relay**.
3. In the DHCP Relay work area, click the **DHCP Relay-VLAN** tab.

4. In the table, double click the **Option82Enabled** cell to edit.
  - **true** enables DHCP Relay with Option 82 for the VLAN
  - **false** disables DHCP Relay with Option 82 for the VLAN
5. On the toolbar, click **Apply**.

---

## Configuring DHCP parameters on a VLAN using EDM

Use the following procedure to configure the DHCP relay parameters on a VLAN.

### Procedure

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, click **VLANs**.
3. In the VLANs work area, click the **Basic** tab.
4. In the Basic section, select the VLAN for which the DHCP relay is to be configured.
5. On the toolbar, click **IP**.
6. Select the **DHCP** tab.
7. In the DHCP section, configure as required.
8. Click **Apply**.

---

## Variable definitions

The following table describes the variables associated with DHCP parameters on VLANs.

Variable	Value
<b>Enable</b>	Specifies whether DHCP relay is enabled or disabled.
<b>MinSec</b>	Indicates the min-sec value. The switch immediately forwards a BootP/DHCP packet if the secs field in the BootP/DHCP packet header is greater than the configured min-sec value; otherwise, the packet is dropped.
<b>Mode</b>	Specifies the type of packets this VLAN interface forwards: BootP, DHCP, or both.
<b>AlwaysBroadcast</b>	Specifies whether DHCP Reply packets are broadcast to the DHCP clients on this VLAN interface.

*Table continues...*

Variable	Value
<b>ClearCounters</b>	Specifies to clear the DHCP relay counters for the VLAN.
<b>CounterClearTime</b>	Specifies the last time the counter values in this entry were reset to 0.

---

## Displaying and graphing DHCP counters on a VLAN using EDM

Use the following procedure to display and graph the current DHCP counters on a VLAN.

### Procedure

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, click **VLANS**.
3. In the VLANs work area, click the **Basic** tab.
4. In the Basic section, select a VLAN.
5. On the toolbar, click **IP**.
6. In the **IP** work area, click the **DHCP** tab.
7. Click **Graph**.
8. On the toolbar, select a **Poll interval** from the drop down menu.
9. Select **Line**, **Area**, **Bar** or **Pie** chart.

The following information is displayed:

- NumRequests — indicates the number of DHCP requests.
- NumReplies — indicates the number of DHCP replies.

---

## Assigning a DHCP Relay Option 82 subscriber ID to a port using EDM

Use the following procedure to assign a DHCP Relay Option 82 subscriber ID to a port.

### Before you begin

- Enable IP Routing globally.
- On the VLAN: enable IP Routing and configure an IP address to be set as the DHCP Relay agent.



- Ensure the a route, either local or static, is available on the switch to the destination DHCP server.

**Procedure**

1. From the navigation tree, double-click **IP**.
2. In the IP tree, click **DHCP Relay**.
3. In the DHCP Relay work area, click the **DHCP Relay-port** tab.
4. In the Multiple Port Configuration section, click the ellipsis and highlight required port(s), click **OK**.
5. In the PortDhcpOption82SubscriberId section, double click cell and enter **subscriber ID** for the port.
6. On the toolbar, click **Apply**.

**Variable definitions**

The following table describes the variables associated with Option 82 subscriber ID.

Variable	Value
<b>rcPortIndex</b>	Indicates the slot and port number.
<b>PortDhcpOption82SubscriberId</b>	Specifies the DHCP Option 82 subscriber ID for the port.  The value is a character string between 1 and 64.

**Displaying DHCP Relay counters information using EDM**

Use the following procedure to display the current DHCP relay counters information. This includes the number of requests and the number of replies.

**Procedure**

1. From the navigation tree, double-click **IP**.
2. In the IP tree, click **DHCP Relay**.
3. In the DHCP Relay work area, click the **DHCP Relay Counters** tab.

**Variable definitions**

The following table describes the fields for the **DHCP Relay Counters** tab.

## DHCP relay configuration using Enterprise Device Manager

<b>Variable</b>	<b>Value</b>
<b>IfIndex</b>	Indicates the VLAN interface index.
<b>NumRequests</b>	Indicates the count of DHCP requests.
<b>NumReplies</b>	Indicates the count of DHCP replies.

# Chapter 18: DHCP Server configuration using Enterprise Device Manager

If you have no separate DHCP server or other device available to provide the service to local hosts, you can use the procedures in this chapter to configure the DHCP Server feature to provide and manage client IPv4 addresses in your network and eliminate manual TCP/IP configuration.

Please note that the procedures in this chapter assume a single VLAN configuration. For configurations in which there is only one VLAN (VLAN 1) on the switch, and where the Switch IP Address is in the same VLAN as the new IP Address Pool that is being configured, routing (IP Forwarding) does not need to be enabled.

---

## Enabling DHCP Server

Use the following procedure to enable DHCP Server and specify the global DHCP Server lease expiry time.

### Before you begin

For a single VLAN configuration:

- Configure or change the IPv4 address configuration according to your setup on the switch or stack (Management VLAN) so the DHCP server can offer an address to the client in that VLAN
- Define at least one IP address pool range or host with a valid network mask
- Enable DHCP

### Note:

When IP routing is disabled, the DHCP Server IP is bound to the Management VLAN IP. When IP routing is enabled, the DHCP Server is bound on all the VLAN IPs from the switch or stack..

When adding a second or subsequent VLAN to which you want to assign DHCP Server pools:

- Enable IP routing/forwarding on the switch or stack

In order for the DHCP Server to function on a VLAN IP or Management VLAN, the configured subnet mask must be identical to the subnet class of the VLAN IP (Management or other VLAN subnet mask configured) and the subnet mask from the DHCP Server IP pool (range or host).

**\* Note:**

When you enable the DHCP Server, DHCP Snooping functionality is disabled, even if the configuration indicates that DHCP Snooping is enabled.

**Procedure**

1. From the navigation tree, double-click **IP**.
2. In the IP tree, click **DHCP Server**.
3. In the DHCP Server work area, click the **DHCP Server Globals** tab.
4. Select the **ServerEnable** checkbox.
5. If selecting a lease time, enter a value for the DHCP Server lease expiry time, or accept the default of 1 day.
6. On the toolbar, click **Apply**.

## Variable definitions

The following table describes the variables associated with configuring the DHCP server.

Variable	Value
<b>ServerEnable</b>	Enable or disable DHCP Server. The DHCP Server default is disabled.
<b>Server Lease</b>	Specify either Days/Hours/Minutes or Infinite. The system uses this lease time for addresses assigned from a pool that does not have a lease time setting. Specify a global lease expiry time: <ul style="list-style-type: none"> <li>• <b>Days:</b> 0 to 49710</li> <li>• <b>Hours:</b> 0 to 23.</li> <li>• <b>Minutes:</b> 0 to 59.</li> </ul> The infinite lease expiry time is 4294967295 seconds.

## Configuring DHCP Server global options

Use the following procedure to configure DHCP Server global options.

**Procedure**

1. From the navigation tree, double-click **IP**.

2. In the IP tree, click **DHCP Server**.
3. In the DHCP Server work area, click the **DHCP Server Global Options** tab.
4. Configure optional parameters.
5. On the toolbar, click **Apply**.

---

## Displaying the DHCP Server pool

Use the following procedure to view DHCP Server Pool information.

### Procedure

1. From the navigation tree, double-click **IP**.
2. In the IP tree, click **DHCP Server**.
3. In the DHCP Server work area, click the **DHCP Server Pool** tab.

---

## Variable definitions

The following table describes the variables associated with configuring the DHCP server pool settings.

Variable	Value
<b>Name</b>	Indicates the unique DHCP Server Pool name.
<b>Lease</b>	Displays the lease expiry time in: <ul style="list-style-type: none"> <li>• <b>Days:</b> 0 to 49710</li> <li>• <b>Hours:</b> 0 to 23</li> <li>• <b>Minutes:</b> 0 to 59</li> </ul>
<b>StartAddress</b>	Displays the first IPv4 IP address for the pool range.
<b>EndAddress</b>	Displays the last IPv4 IP address for the pool range.
<b>MACAddress</b>	Displays the MAC Address associated with a device for a statically-assigned DHCP Server host.
<b>SubnetMask</b>	Indicates the subnet mask associated for this pool range.
<b>Routers</b>	Specifies the router(s) associated for this address pool range. If entering multiple routers, separate the entries with commas.
<b>DNS Servers</b>	Specifies the list of DNS servers. If entering multiple servers, separate the entries with commas.

*Table continues...*

Variable	Value
<b>VendorClassId</b>	Indicates the vendor-specific identifier that allows your DHCP Server to receive vendor-specific configuration or identification information for clients.
<b>VendorSpecificInfo</b>	Indicates the vendor class identifier allows DHCP clients and DHCP servers in your network to exchange vendor-specific information.

## Configuring a DHCP Server pool

Use this procedure to configure a DHCP Server address pool.

### About this task

If you require more than one IP address pool, you must first create additional VLANs — a VLAN to associate with each additional IP address pool.

### Procedure

1. From the navigation tree, double-click **IP**.
2. In the IP tree, click **DHCP Server**.
3. In the DHCP Server work area, click the **DHCP Server Pool** tab.
4. On the toolbar, click **Insert**.
5. On the **Insert DHCP Server Pool** pane, enter the values to configure a pool.
6. Click **Insert**.
7. On the DHCP Server Pool toolbar, click **Refresh** to display the new DHCP Server Pool.

## Variable definitions

The following table describes the variables associated with configuring the DHCP server pool settings.

Name	Description
<b>Name</b>	Enter a unique DHCP Server Pool name up to 32 alpha-numeric characters long.  If the value is greater than 0, it is an explicit setting for a specific address pool. Zero is a global value used for all pools that do not have addresses of the specified type configured. Global entry types must be either may DNS or router.

*Table continues...*

Name	Description
<b>Lease</b>	Specify either Days/Hours/Minutes or Infinite. Specify a value for lease expiry time in: <ul style="list-style-type: none"> <li>• <b>Days:</b> 0 to 49710</li> <li>• <b>Hours:</b> 0 to 23</li> <li>• <b>Minutes:</b> 0 to 59</li> </ul>
<b>StartAddress</b>	Enter the first IPv4 IP address for the pool range.  This address must be in the same class as the DHCP Server address and must be less than or equal to the value of EndAddress.
<b>EndAddress</b>	Enter the last IPv4 IP address for the pool range.  This address must be in the same class as the DHCP Server address and must be greater than or equal to the value of StartAddress.  If the value is equal to StartAddress, it describes a static IP DHCP Server host.
<b>MACAddress</b>	Enter the MAC Address associated with a device for a statically-assigned DHCP Server host.  If address pools contain start and end addresses that are not equal, this value is not used and has no effect.
<b>SubnetMask</b>	Specifies the subnet mask associated for this address pool range.
<b>Router(s)</b>	Specifies the router(s) associated for this address pool range.  If entering multiple routers, separate the entries with commas.
<b>DNS Server(s)</b>	Specifies the list of DNS servers.  If entering multiple servers, separate the entries with commas.
<b>TFTP Server(s)</b>	Specifies the list of TFTP servers  If entering multiple servers, separate the entries with commas.
<b>SIP Server(s)</b>	Specifies the list of SIP servers  If entering multiple servers, separate the entries with commas.
<b>VendorClassId</b>	Enter the vendor class identifier so your DHCP server can receive vendor-specific configuration or identification information for clients. If you are using this parameter and VendorSpecificInfo(43), a specific

*Table continues...*

Name	Description
	<p>IP pool must be created using only these parameters, as well as the default values. Separate IP pools should be created with additional variables as required.</p> <p>The minimum length for a vendor class identifier is 1 character. Entries are case-sensitive</p>
<b>VendorSpecificInfo</b>	<p>Enter the vendor class identifier if DHCP clients and DHCP servers in your network need to exchange vendor-specific information. If you are using this parameter and VendorClassID(60), a specific IP pool must be created using only these parameters, as well as the default values. Separate IP pools should be created with additional variables as required.</p> <p>The minimum length for a vendor class identifier is 1 character</p> <p>Vendor specific options must be specified in the following format:</p> <p><code>&lt;code&gt;:&lt;type&gt;:&lt;data&gt;:&lt;code&gt;:&lt;type&gt;:&lt;data&gt;</code></p> <p><code>&lt;code&gt;</code>: 255, 0 and 255 are reserved and cannot be used.</p> <p><code>&lt;type&gt;</code>: available types are str, octet, short, long, ip, iplist, ippairs, mtpt or raw. All the types have the same format as described above, except raw which is a list of byte values separated by white space. For example: 0x4 0xAC 0x11 0X41</p> <p><code>&lt;data&gt;</code>: the actual data to be included. Cannot contain single quotes.</p> <p>More than one code, type, data triplet can be specified, but must be separated by ":" . The entire vendor options must be enclosed within single quotes.</p> <p>Entries are case sensitive.</p>

**\* Note:**

The DHCP Server IP address pool Option-176 feature supports only IP Phones 4600 series for provisioning a number of parameters. When you create a DHCP Server IP Address Pool, Option 176 is automatically enabled with several default parameters, with the exception of the MCIPADD and TFTP Server IP address information.

**\* Note:**

When you create a DHCP Server IP vendorclass pool, configure only Option 43. The StartAddress and EndAddress should be 0.0.0.0 and the remaining parameters must remain blank.



## DHCP Server Option 43 vendor specific information


The following table lists the code types supported with the DHCP Server Option-43 vendor specific info command.

Name	Code	Type	Description
snmk	1	ip	Subnet mask of the IP address to be allocated. Default: natural mask corresponding to the IP address. The server does not issue IP addresses to clients on different subnets.
tmof	2	long	Time offset from UTC, in seconds.
rout	3	iplist	List of routers on the same subnet as the client.
tmsv	4	iplist	A list of time servers (RFC 868).
nmsv	5	iplist	A list of name servers (IEN 116).
dnsv	6	iplist	A list of DNS servers (RFC 1035).
lgsv	7	iplist	A list of MIT-LCS UDP log servers.
chsv	8	iplist	A list of Cookie servers (RFC 865).
lpsv	9	iplist	A list of LPR servers (RFC 1179).
imsv	10	iplist	A list of Imagen Impress servers.
rlsv	11	iplist	A list of Resource Location servers (RFC 887).
hstn	12	str	Host name of the client.
btsz	13	short	Size of the boot image.
mdmp	14	str	Path name to which client dumps core.
dnsd	15	str	Domain name for DNS.
swwsv	16	ip	IP address of swap server.
rpth	17	str	Path name of root disk of the client.
epth	18	str	Extensions Path (RFC 1533).
plcy	21	ippairs	Policy filter for non-local source routing. A list of pairs of: Destination IP, Subnet mask.
mdgs	22	short	Maximum size of IP datagram that the client should be able to reassemble.
ditl	23	octet	Default IP TTL.
mtat	24	long	Aging timeout, in seconds, to be used with Path MTU discovery (RFC 1191).
mtpt	25	mtpt	A table of MTU sizes to be used with Path MTU Discovery.
ifmt	26	short	MTU to be used on an interface.

*Table continues...*

Name	Code	Type	Description
brda	28	ip	Broadcast address in use on the client subnet. The system calculates the default from the subnet mask and the IP address.
rtsl	32	ip	Destination IP address to which the client sends router solicitation request.
strt	33	ippairs	A table of static routes for the client consisting of pairs (Destination, Router). You cannot specify the default route as a destination.
arpt	35	long	Timeout, in seconds, for ARP cache.
dttl	37	octet	Default TTL of TCP.
kain	38	long	Client TCP keepalive interval, in seconds.
nisd	40	str	Domain name for NIS.
nisv	41	iplist	A list of NIS servers
ntsv	42	iplist	A list of NTP servers.
vend	43	str	<p>Vendor Specific Options—must be specified in the following format:</p> <pre>vend=&lt;code&gt;:&lt;type&gt;:&lt;date&gt;:&lt;code&gt;:&lt;type&gt;:&lt;date&gt;</pre> <ul style="list-style-type: none"> <li>&lt;code&gt; is an int 1 &lt; &lt;code&gt; &lt;255 Do not use 0 and 255, they are reserved.</li> <li>&lt;type&gt; can be str, octet, short, long, ip, ip list, ippairs, mtpt, or raw. All types have the same format described above, except raw, which is a list of type values separated by white space. Example for raw: 0x4 0xAC 0x11 0x41</li> <li>&lt;data&gt; is the actual data. Data cannot contain single quotes.</li> </ul> <p>Syntax:</p> <p>You can specify more than one code, type, or data triplets, but you must separate each by a colon (:).</p> <p>You must enclose the entire vendor options within single quotes (').</p>
nnsv	44	iplist	A list of NetBIOS name servers (RFC 1001, 1002).
nds v	45	iplist	A list of NetBIOS datagram distribution servers (RFC 1001, 1002).
nbnt	46	octet	NetBIOS node type (RFC 1001, 1002).
nbsc	47	str	NetBIOS scopt (RFC 1001, 1002).

*Table continues...*

Name	Code	Type	Description
xsfv	48	iplist	A list of font servers of X Window system.
xdmn	49	iplist	A list of display managers of X Window system.
dht1	58	short	Specifies when the client should start RENEWING. DEFAULT: 500  The default indicates that the client starts RENEWING after 50% of the lease duration passes.
dht2	59	short	Specifies when the client should start REBINDING. DEFAULT: 875  The default indicates that the client starts REBINDING after 87.5% of the lease duration passes.
nspd	64	str	The name of the client NIS+ domain.
nsps	65	iplist	A list of NIS+ servers.
miph	68	iplist	A list of mobile IP home agents.
smtp	69	iplist	A list of SMTP servers
pops	70	iplist	A list of POP3 servers.
nntp	71	iplist	A list of NNTP servers.
wwws	72	iplist	A list of WWW servers.
fngs	73	iplist	A list of Finger servers.
ircs	74	iplist	A list of IRC servers.
stsv	75	iplist	A list of StreetTalk servers.
stda	76	iplist	A list of STDA servers.
<p> <b>Note:</b> For any code number not in this list you must use a default of <code>str</code> (string). For example: <code>200:str:information</code>. Option numbers 0 and 255 are reserved.</p>			

## Deleting a DHCP Server pool

Use the following procedure to delete any DHCP Server pool

### Procedure

1. From the navigation tree, double-click **IP**.
2. In the IP tree, click **DHCP Server**.
3. In the DHCP Server work area, click the **DHCP Server Pool** tab.
4. In the **Name** column, click a DHCP Server Pool to delete.
5. On the toolbar, click **Delete**.

## Configuring DHCP Server pool options

Use the following procedure to configure DHCP Server pool options.

### Procedure

1. From the navigation tree, double-click **IP**.
2. In the IP tree, click **DHCP Server**.
3. In the DHCP Server work area, click the **DHCP Server Pool** tab.
4. On the toolbar, click **Options**.
5. Use the fields and buttons on the **DHCP Server Pool Options** pane to configure the DHCP Server Pool Options.
6. On the toolbar, click **Apply** to save your changes.

## Variable definitions

The following table describes the variables associated with configuring the DHCP server pool options.

Variable	Value
Options	
<b>Routers(3)</b>	Specifies up to a maximum of 8 global routers.
<b>DNS Servers(6)</b>	Specifies up to a maximum of 8 DNS servers.
<b>SIP Servers(120)</b>	Specifies up to a maximum of 8 SIP servers.
<b>TFTP Servers(150)</b>	Specifies up to a maximum of 8 TFTP servers.
Option 176 (IP Phone 4600 Series)	
<b>MC IP Addr</b>	Specifies up to a maximum of 8 ipPhoneMCipaddr servers.
<b>TFTP Servers</b>	Specifies up to a maximum of 8 ipPhoneTftpsrvr servers
<b>Mcport</b>	Indicates a value from 1 to 65535 that specifies the UDP port that the IP Phone uses for registration. Default value: 1719.
<b>L2qvlan</b>	Specifies a value from 0 to 4096 that specifies the 802.1Q VLAN ID. Default value: 0.
<b>Vlantest</b>	Specifies a value from 0 to 180 that specifies the number of seconds a phone will attempt to return to the previously known voice VLAN. Default value: 60.
<b>L2qaud</b>	Specifies a value from 0 to 7 that specifies the Layer 2 audio priority value. Default value: 6.

*Table continues...*

<b>L2qsig</b>	Specifies a value from 0 to 7 that specifies the Layer 2 signaling priority value. Default value: 6.
Option 241 (IP Phones 200x, 1100, 1200)	
<b>Parameter String</b>	Specifies the parameters for IP Phones. For the list of supported parameters, see <a href="#">DHCP Server Option 241 parameters</a> on page 91. If the parameter is not included, the parameter retains its default value, or the value that was previously provisioned for the specific parameter. Parameter value is between the equals sign and semicolon. Format and example of the parameter list:  Nortel-i2004–  B,s1ip=47.11.62.21;p1=4100;a1=;r1=255;s2ip=47.11.62.21;p2=4100;a2=1;r2=2
Option 242 (IP Phones 4600, 960x)	
<b>HTTP Port</b>	Specifies the HTTP port, a value from 0 to 65535. Default value: 80.
<b>HTTP Servers</b>	Specifies an IP Phone IPv4 address or list of addresses. You can enter up to eight (8) IP addresses.
<b>MC IP Addr</b>	Specifies an IP Phone IPv4 address or list of addresses. You can enter up to eight (8) Call Server IP Addresses. This parameter is used as a backup for the IP phone in case the HTTP Server is unavailable, in which case the IP phone can reach the Call Server.

---

## Deleting DHCP Server pool options

Use this procedure to delete DHCP Server pool options.

### Procedure

1. From the navigation tree, double-click **IP**.
2. In the IP tree, click **DHCP Server**.
3. In the DHCP Server work area, click the **DHCP Server Pool** tab.
4. On the toolbar, click **Options**.
5. In the **Name** column, select the pool for which you wish to delete the options.
6. On the toolbar, click **Options**,
7. Within the DHCP Server Pool, select an option row to delete.
8. On the toolbar, click **Delete**.

---

## Displaying DHCP Server Client information

Use the following procedure to display DHCP Server Client information.

### Procedure

1. From the navigation tree, double-click **IP**.
2. In the IP tree, click **DHCP Server**.
3. In the DHCP Server work area, click the **DHCP Server Clients** tab.

---

## DHCP Server Clients tab field descriptions

The following table describes the variables associated with the DHCP Server clients.

Name	Description
<b>Client</b>	Specifies the IP address assigned to the client.
<b>ClientHostName</b>	Specifies the hostname sent from the client in the discover and request packet
<b>ClientPhysicalAddress</b>	Specifies the MAC address of the client.
<b>ClientTimeRemaining</b>	Specifies the time remaining until the IP address assigned to the client expires.
<b>ClientSubnetMask</b>	Specifies the subnet mask of the IP address of the client.
<b>ClientLeaseType</b>	Indicates dynamic (if from a range IP pool) or static.

# Chapter 19: UDP broadcast forwarding configuration using Enterprise Device Manager

This chapter describes the procedures you can use to configure and manage UDP broadcast forwarding using Enterprise Device Manager.

UDP broadcast forwarding is a general mechanism for selectively forwarding limited UDP broadcasts received on an IP interface to a configured IP address.

---

## UDP broadcast forwarding configuration procedures

To configure UDP broadcast forwarding using Enterprise Device Manager, perform the following steps:

1. Create UDP protocol entries that specify each UDP port and associated protocol that you want to forward.
2. Create UDP forwarding entries that specify the destination address for each UDP port that you want to forward.
3. Add UDP forwarding entries to a UDP forwarding list (you can create up to 128 UDP forwarding lists.)
4. Apply UDP forwarding lists to local VLAN interfaces.

---

## Configuring UDP protocol table entries using EDM

Use the following procedure to create UDP table entries that identify the protocols associated with specific UDP ports to forward.

### Procedure

1. From the navigation tree, double-click **IP**.
2. In the IP tree, click **UDP Forwarding**.

3. In the UDP Forwarding area, click the **Protocols** tab.
4. In the Protocols section, click **Insert**.
5. In the Insert Protocols section, configure as required.
6. Click **Insert**.

## Variable definitions

The following table describes the variables associated with configuring UDP protocol table entries.

Variable	Value
<b>PortNumber</b>	Specifies the UDP port number.
<b>Name</b>	Specifies the protocol name associated with the UDP port.

## Configuring UDP forwarding entries using EDM

Use the following procedure to configure individual UDP forwarding entries, which associate UDP forwarding ports with destination IP addresses.

### Procedure

1. From the navigation tree, double-click **IP**.
2. In the IP tree, click **UDP Forwarding**.
3. In the UDP Forwarding work area, click the **Forwardings** tab.
4. On the toolbar, click **Insert**.
5. In the Insert Forwardings section, specify a destination address.
6. Click **Insert**.

## Variable definitions

The following table describes the variables associated with UDP forward entries.

Name	Description
<b>DestPort</b>	Specifies the port on which the UDP forwarding originates (configured using the Protocols tab).
<b>DestAddress</b>	Specifies the destination IP address.
<b>Id</b>	The unique identifier assigned to the forwarding list.

*Table continues...*



Name	Description
<b>FwdListIdList</b>	The forwarding entry IDs associated with the port/server IP pairs created using the Forwardings tab.

---

## Configuring a UDP forwarding list using EDM

Use the following procedure to add the UDP port/destination forwarding entries (configured in the Forwardings tab) to UDP forwarding lists.

Each UDP forwarding list can contain multiple port/destination entries.

### Procedure

1. From the navigation tree, double-click **IP**.
2. In the IP tree, click **UDP Forwarding**.
3. In the UDP Forwarding work area, click the **Forwarding Lists** tab.
4. On the toolbar, click **Insert**.
5. In the Insert Forwarding Lists section, configure as required.
6. In the **FwdIdList** section, click the ellipsis and select the desired port/destination pairs.
7. Click **Ok**.
8. Click **Insert**.

---

## Variable definitions

The following table describes the variables associated with UDP forwarding lists.

Variable	Value
<b>Id</b>	The unique identifier assigned to the forwarding list.
<b>Name</b>	The name assigned to the forwarding list.
<b>FwdIdList</b>	The forwarding entry IDs associated with the port/server IP pairs created using the Forwardings tab.

---

## Applying a UDP forwarding list to a VLAN using EDM

Use the following procedure to assign a UDP forwarding list to a VLAN and to configure the related UDP forwarding parameters for the VLAN.

**Procedure**

1. From the navigation tree, double-click **IP**.
2. In the IP tree, click **UDP Forwarding**.
3. In the UDP Forwarding work area, click the **Broadcast Interfaces** tab.
4. Click **Insert**.
5. In the Insert Broadcast Interface section, configure as required.
6. Click **Insert**.

---

**Variable definitions**

The following table describes the variables associated with applying a UDP forwarding list to a VLAN.

Variable	Value
<b>LocalIfAddr</b>	Specifies the IP address of the local VLAN interface.
<b>UdpPortFwdListId</b>	Specifies the port forwarding lists associated with the interface. This ID is defined in the Forwarding Lists tab.
<b>MaxTtl</b>	Indicates the maximum number of hops an IP broadcast packet can take from the source device to the destination device. This is an integer value between 1 and 16.
<b>NumRxPkts</b>	Specifies the total number of UDP broadcast packets received by this local interface.
<b>NumFwdPkts</b>	Specifies the total number of UDP broadcast packets forwarded.
<b>NumDropPktsDestUnreach</b>	Specifies the total number of UDP broadcast packets dropped because the destination is unreachable.
<b>NumDropPktsUnknownPort</b>	Specifies the total number of UDP broadcast packets dropped because the destination port or protocol specified has no matching forwarding policy.
<b>BroadCastMask</b>	Specifies the 32-bit mask used by the selected VLAN interface to take forwarding decisions based on the destination IP address of the incoming UDP broadcast traffic. If you do not specify a broadcast mask value, the switch uses the mask of the interface to which the forwarding list is attached.

# Chapter 20: Static ARP and Proxy ARP configuration using Enterprise Device Manager

This chapter describes the procedures you can use to configure Static ARP, display ARP entries, and configure Proxy ARP using Enterprise Device Manager.

---

## Configuring static ARP entries using EDM

Use this procedure to configure static ARP entries for the switch.

### Before you begin

- Enable IP routing globally.
- Enable IP routing and configure an IP address on the target VLAN interface.

### Procedure

1. From the navigation tree, double-click **IP**.
2. In the IP tree, click **IP**.
3. In the IP work area, click the **ARP** tab.
4. Click **Insert**.
5. Click **Port in Vlan** and select the VLAN to add the static ARP entry.
6. Configure entries as required.
7. Click **Insert**.

---

## Variable definitions

The following table describes the variables associated with configuring static ARP entries.

Variable	Value
<b>Interface</b>	Specifies the VLAN and port to which the static ARP entry is being added.
<b>MacAddress</b>	Specifies the MAC address of the device being set as a static ARP entry.
<b>IpAddress</b>	Specifies the IP address of the device being set as a static ARP entry.
<b>Type</b>	Specifies the type of ARP entry: static, dynamic, or local.

---

## Configuring Proxy ARP using EDM

Use the following procedure to configure proxy ARP on the switch. Proxy ARP allows the switch to respond to an ARP request from a locally attached host (or end station) for a remote destination.

### Procedure

1. From the navigation tree, double-click **IP**.
2. In the IP tree, click **IP**.
3. In the IP work area, click the **ARP Interfaces** tab.

 **Important:**

Device Manager does not display the ARP Interfaces tab if you have not enabled routing on the switch.

4. In the ARP Interfaces section, click the **DoProxy** column on a VLAN.
5. Click **Enable**.
6. Click **Apply**.

---

## Variable definitions

The following table describes the variables associated with the ARP interface tab.

Variable	Value
<b>IfIndex</b>	Specifies a configured switch interface.
<b>DoProxy</b>	Enables or disables proxy ARP on the interface.
<b>DoResp</b>	Specifies whether the sending of ARP responses on the specified interface is enabled or disabled.

# Chapter 21: IGMP snooping configuration using Enterprise Device Manager

This chapter describes the procedures used to configure IGMP snooping using Enterprise Device Manager.

---

## Managing IGMP snoop using EDM

Use the following procedures to configure IGMP snooping and proxy and static mrouter ports.

---

## Configuring IGMP snoop, proxy and static mrouter ports on a VLAN using EDM

Use the following procedure to configure IGMP snooping, proxy, and static mrouter ports on a VLAN.

By default, IGMP snoop and proxy are disabled, and no static mrouter ports are configured.

### Procedure

1. From the navigation tree, double-click **IP**.
2. In the IP tree, click **IGMP**.
3. In the IGMP work area, click the **Snoop** tab.
4. In the Snoop section, configure cells as required.
5. On the toolbar, click **Apply**.
6. On the toolbar, you can click **Refresh** verify the configuration.

### Variable definitions

The following table describes the fields on the IGMP snoop tab.

Variable	Value
<b>IfIndex</b>	Specifies the VLAN ID.
<b>SnoopEnable</b>	Specifies the IGMP snoop status: <ul style="list-style-type: none"> <li>• enabled (true)</li> <li>• disabled (false)</li> </ul>
<b>ProxySnoopEnable</b>	Specifies the IGMP proxy status: <ul style="list-style-type: none"> <li>• enabled (true)</li> <li>• disabled (false)</li> </ul>
<b>SnoopMRouterPorts</b>	Specifies the static mrouter ports. Such ports are directly attached to a multicast router so the multicast data and group reports are forwarded to the router.
<b>SnoopActiveMRouterPorts</b>	Displays all dynamic (querier port) and static mrouter ports that are active on the interface.
<b>SnoopMRouterExpiration</b>	Specifies the time remaining before the multicast router is aged out on this interface. If the switch does not receive queries before this time expires, it flushes out all group memberships known to the VLAN. The Query Max Response Interval (obtained from the queries received) is used as the timer resolution.

## Displaying IGMP groups using EDM

Use this procedure to display the IGMP group information.

### Procedure

1. From the navigation tree, double-click **IP**.
2. In the IP tree, click **IGMP**.
3. In the IGMP work area, click the **Groups** tab.

## Variable definitions

The following table describes the variables associated with IGMP group information.

Variable	Value
<b>IpAddress</b>	Indicates the multicast group IP address.

*Table continues...*

Variable	Value
	An address can be the same for many incoming ports.
<b>IfIndex</b>	Indicates VLAN interface associated with the multicast group address.
<b>Members</b>	Indicates the IP address of the IGMP receiver (host or IGMP reporter).
<b>Expiration</b>	Indicates the time left before the group report expires. This variable is updated when a group report is received.
<b>InPort</b>	Indicates the member port for the group. This is the port on which group traffic is forwarded.

---

## Displaying IGMP group information using EDM

Use the following procedure to display IGMP group information.

### Procedure

1. From the navigation tree, double-click **IP**.
2. In the IP tree, click **IGMP**.
3. In the IGMP work area, click the **Groups-Ext** tab.

---

## Variable definitions

The following table describes the variables associated with IGMP group information.

Variable	Value
<b>IpAddress</b>	Indicates the multicast group address.
<b>SourceAddress</b>	Indicates the source address.
<b>Members</b>	Indicates the IP address of the IGMP receiver (host or IGMP reporter).
<b>Mode</b>	Indicates the mode.
<b>IfIndex</b>	Indicates the VLAN interface from which the multicast group address is heard.
<b>Expiration</b>	Indicates the time left before the group report expires on this port. This variable is updated upon receiving a group report.
<b>InPort</b>	Indicates the member port for the group. This is the port on which group traffic is forwarded.

---

## Displaying IGMP cache information using EDM

Use the following procedure to display IGMP cache information.

### Procedure

1. From the navigation tree, double-click **IP**.
2. In the IP tree, click **IGMP**.
3. In the IGMP work area, click the **Cache** tab.

---

## Variable definitions

The following table describes the variables associated with IGMP cache information.

Name	Description
<b>Address</b>	Indicates the IP multicast group address.
<b>IfIndex</b>	Indicates the VLAN interface from which the group address is heard.
<b>LastReporter</b>	Indicates the last IGMP host to join the group.
<b>ExpiryTime</b>	Indicates the amount of time (in seconds) remaining before this entry is aged out.
<b>Version1Host Timer</b>	Indicates the time remaining until the local router assumes that no IGMP version 1 members exist on the IP subnet attached to the interface. Upon hearing an IGMPv1 membership report, this value is reset to the group membership timer. When the time remaining is nonzero, the local interface ignores IGMPv2 Leave messages that it receives for this group.
<b>Type</b>	Indicates whether the entry is learned dynamically or is added statically.

---

## Managing IP Address multicast filter tables using EDM

Use the following procedures to display IP address multicast filter tables and specify IP address flooding.



## Specifying an IP address to be allowed to flood a VLAN using EDM

Use the following procedure to configure the IP address multicast filter table. This table specifies multicast IP addresses that are allowed to be flooded to all ports on a per-VLAN basis.

### Procedure

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, click **VLANs**.
3. In the VLANs work area, click the **IP address Multicast Filter Table** tab.
4. Click **Insert**.
5. In the Insert section, configure as required.
6. Click **Insert**.

### Variable definitions

The following table describes the variables of the IP Address Multicast Filter Table tab.

Variable	Value
<b>VlanAllowedInetAddressVlanId</b>	Specifies the ID of the VLAN to configure.
<b>VlanAllowedInetAddressType</b>	Specifies the address type: ipv4.
<b>VlanAllowedInetAddress</b>	Specifies a multicast IP address that is allowed to flood all ports. Unicast and broadcast addresses are not allowed.

## Displaying the IP Address Multicast Filter Table using EDM

Use the following procedure to display the IP Multicast Filter Table.

### Procedure

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, click **VLANs**.
3. In the VLANs work area, click the **IP Address Multicast Filter Table** tab.

### Variable definitions

The following table describes the variables associated with the IP Address Multicast Filter Table.

Variable	Value
<b>VlanAllowedInetAddressVlanId</b>	The ID of the VLAN in which the specified multicast IP address is allowed to flood traffic.
<b>VlanAllowedInetAddressVlanType</b>	The address type. The only supported value is ipv4.
<b>VlanAllowedInetAddress</b>	Multicast IP address. Traffic destined to this address will be flooded inside the VLAN.

## Configuring IGMP interface parameters and flushing IGMP tables using EDM

Use the following procedure to make interface specific IGMP settings and/or flush the IGMP tables on a VLAN.

### Procedure

1. From the navigation tree, double-click **IP**.
2. In the IP tree, click **IGMP**.
3. In the IGMP work area, click the **Interface** tab.
4. Double click the cell under the **FlushAction** column and select the desired flush option.
5. On the toolbar, click **Apply**.

## Variable definitions

The following table describes the fields on the IGMP Interface tab.

Name	Description
<b>IfIndex</b>	Indicated the interface on which the IGMP is enabled.
<b>QueryInterval</b>	Indicates the frequency (in seconds) at which IGMP host query packets are transmitted on the interface. Ensure that the robustness value is the same as the configured value on the multicast router (IGMP querier).  RANGE: 1–65535 DEFAULT: 125
<b>Status</b>	Indicates whether or not the interface is active. The interface becomes active if any IGMP forwarding ports exist on the interface. If the VLAN has no port

*Table continues...*

Name	Description
	members or if all of the port members are disabled, the status is notInService.
<b>Version</b>	Indicates the version of IGMP (1, 2, or 3) configured on this interface. For IGMP to function correctly, all routers on a LAN must use the same version.  DEFAULT: 2
<b>OperVersion</b>	Indicates the version of IGMP currently running on this interface.
<b>Querier</b>	Indicates the address of the IGMP querier on the IP subnet to which this interface is attached.
<b>QueryMaxResponseTime</b>	Indicates the maximum response time (in 1/10 seconds) advertised in IGMPv2 general queries on this interface.
<b>WrongVersionQueries</b>	Indicates the number of queries received with an IGMP version that does not match the interface. IGMP requires that all routers on a LAN be configured to run the same version of IGMP. If queries are received with the wrong version, it indicates a version mismatch.
<b>Joins</b>	Indicates the number of times a group membership is added on this interface; that is, the number of times an entry for this interface is added to the cache table. This number gives an indication of the amount of IGMP activity over time.
<b>Robustness</b>	Specifies tuning for the expected packet loss of a network. This value is equal to the number of expected query packet losses for each serial query interval, plus 1. If you expect a network to lose query packets, you must increase the robustness value. Ensure that the robustness value is the same as the configured value on the multicast router (IGMP querier).  RANGE: 2–255  DEFAULT: 2  The default value of 2 means that one query for each query interval can be dropped without the querier aging out.
<b>LastMembQueryIntvl</b>	Sets the maximum response time (in tenths of a second) that is inserted into group-specific queries sent in response to leave group messages. This parameter is also the time between groupspecific query messages. This value is not configurable for

*Table continues...*

Name	Description
	<p>IGMPv1. Decreasing the value reduces the time to detect the loss of the last member of a group.</p> <p>RANGE: 0–255</p> <p>Extreme Networks recommends configuring this parameter to values higher than 3. If a fast leave process is not required, Extreme Networks recommends values above 10. (The value 3 is equal to 0.3 of a second, and 10 is equal to 1.0 second.)</p>
<b>RouterAlertEnable</b>	<p>When enabled, this parameter instructs the router to ignore IGMP packets that do not contain the router alert IP option. When disabled (default setting), the router processes IGMP packets regardless of whether the router alert IP option is set or not.</p> <p>To maximize your network performance, Extreme Networks recommends that you set this parameter according to the version of IGMP currently in use:</p> <ul style="list-style-type: none"> <li>• IGMPv1—Disable</li> <li>• IGMPv2—Enable</li> <li>• IGMPv3—Enable</li> </ul>
<b>SendQuery</b>	<p>Indicates whether to enable the SendQuery feature on this vlan or not. With SendQuery enabled, a multicast snooping capable switch will send out general queries at every query interval, overcoming the absence of an actual mrouter in the LAN.</p>
<b>FlushAction</b>	<p>Flushes the specified table type:</p> <ul style="list-style-type: none"> <li>• none</li> <li>• flushGrpMem — group member table</li> <li>• flushMrouter — mrouter table</li> </ul>

---

## Configuring VLAN snooping using EDM

Use this procedure to configure VLAN snooping.

### Procedure

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, click **VLANs**.
3. In the VLANs work area, click the **Snoop** tab.
4. In the Snoop section, configure as required.

- On the toolbar, click **Apply**.

## Variable definitions

The following table describes the fields on the VLAN snoop tab.

Name	Description
<b>Id</b>	Specifies the VLAN ID.
<b>Name</b>	Specifies the VLAN name.
<b>Enable</b>	Specifies whether snooping is enabled or disabled.
<b>ReportProxyEnable</b>	Specifies whether the proxy is enabled or disabled.
<b>Robustness</b>	<p>Specifies tuning for the expected packet loss of a network. This value is equal to the number of expected query packet losses for each serial query interval, plus 1. If you expect a network to lose query packets, you must increase the robustness value. Ensure that the robustness value is the same as the configured value on the multicast router.</p> <p>RANGE: 0–255</p> <p>DEFAULT: 2</p> <p>The default value of 2 means that one query for each query interval can be dropped without the querier aging out.</p>
<b>QueryInterval</b>	Sets the frequency (in seconds) at which host query packets are transmitted on the VLAN.
<b>MRouterPorts</b>	Specifies ports in the VLAN that provide connectivity to an IP Multicast router.
<b>Ver1MRouterPorts</b>	Specifies ports in this VLAN that provide connectivity to an IP Multicast router using IGMP version 1.
<b>Ver2MRouterPorts</b>	Specifies ports in this VLAN that provide connectivity to an IP Multicast router using IGMP version 2.
<b>ActiveMRouterPorts</b>	Specifies the active mrouter ports (dynamic and static) in this VLAN that provide connectivity to an IP Multicast router.
<b>ActiveQuerier</b>	Specifies the IP address of the multicast querier router.
<b>QuerierPort</b>	Specifies the port on which the multicast querier router is heard.
<b>MRouterExpiration</b>	Specifies the multicast querier router aging timeout.

---

## Displaying the MAC Multicast Filter Table using EDM

Use the following procedure to display the MAC Multicast Filter Table.

### Procedure

1. From the navigation tree, double-click **VLAN**.
2. In the VLAN tree, click **VLANs**.
3. In the VLANs work area, click the **MAC Multicast Filter Table** tab.

---

## Variable definitions

The following table describes the variables associated with the Multicast Filter Table.

Name	Description
<b>AllowedAddressMacAddr</b>	Indicates the MAC addresses for which flooding is allowed.
<b>AllowedAddressVlanId</b>	Indicates the VLAN interface for which the multicast MAC address is allowed.

# Chapter 22: IP Routing capabilities and limitations

The following table lists the capabilities and limitations of IP Routing features and protocols for the switch.

**Table 2: Capabilities and limitations**

Feature	Maximum number supported
IP Interfaces (VLANs or Brouter ports)	64
ARP Entries — local (IP interfaces per switch/stack)	256
Static ARP entries	256
Dynamic ARP entries	480
IPv4 Static routes	32 (including the default route)
IPv4 Local routes	32
Management routes	4
UDP Forwarding entries	128
UDP port/protocol entries	128
VLANs bound to a single UDP forwarding list	16
Ports with IP addresses in single UDP forwarding list	16
DHCP relay entries	256
DHCP relay forward paths	512
RIP routes	510
RIP Layer 3 VLANs	256
<b>Miscellaneous</b>	
When adding a static ARP entry for a VLAN subnet, the IP address associated with the MAC address must be in the subnet for the VLAN. Otherwise the following error message is returned:	
<pre>% Cannot modify settings IP address does not match with VLAN subnet.</pre>	