ArubaOS-Switch Multicast and Routing Guide for YA/YB.16.04

aruba

a Hewlett Packard
Enterprise company

Part Number: 5200-3133a
Published: August 2017
Edition: 2

Notices

The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

Confidential computer software. Valid license from Hewlett Packard Enterprise required for possession, use, or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Links to third-party websites take you outside the Hewlett Packard Enterprise website. Hewlett Packard Enterprise has no control over and is not responsible for information outside the Hewlett Packard Enterprise website.

Acknowledgments

Intel®, Itanium®, Pentium®, Intel Inside®, and the Intel Inside logo are trademarks of Intel Corporation in the United States and other countries.

Microsoft® and Windows® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Adobe® and Acrobat® are trademarks of Adobe Systems Incorporated.

Java® and Oracle® are registered trademarks of Oracle and/or its affiliates.

UNIX® is a registered trademark of The Open Group.

This guide provides information on how to configure IGMP, routing protocols and DHCP configuration.

Applicable products

This guide applies to these products:

Aruba 2530 Switch Series (J9772A, J9773A, J9774A, J9775A, J9776A, J9777A, J9778A, J9779A, J9780A, J9781A, J9782A, J9783A, J9853A, J9854A, J9855A, J9856A, JL070A)

Switch prompts used in this guide

Examples in this guide are representative and may not match your particular switch/environment. The following table explains the types of command prompts that may be used in examples, along with information on what each prompt indicates.

Prompt	Explanation
`switch#`	`#` indicates manager context (authority).
`switch>`	`>` indicates operator context (authority).
`switch(config)#`	`(config)` indicates the config context.
`switch(vlan-`*x*`)#`	`(vlan-`*x*`)` indicates the vlan context of config, where *x* represents the VLAN ID. For example: `switch(vlan-128)#`.
`switch(eth-`*x*`)#`	`(eth-`*x*`)` indicates the interface context of config, where `x` represents the interface. For example: `switch(eth-48)#`.
`switch-Stack#`	`Stack` indicates stacking is enabled.
`switch-Stack(config)#`	`Stack(config)` indicates the config context while stacking is enabled.
`switch-Stack(stacking)#`	`Stack(stacking)` indicates the stacking context of config while stacking is enabled.
`switch-Stack(vlan-`*x*`)#`	`Stack(vlan-`*x*`)` indicates the vlan context of config while stacking is enabled, where *x* represents the VLAN ID. For example: `switch-Stack(vlan-128)#`.
`switch-Stack(eth-`*x*`/`*y*`)#`	`Stack(eth-`*x*`/`*y*`)` indicates the interface context of config, in the form `(eth-`*<member-in-stack>*`/`*<interface>*`)`. For example: `switch(eth-1/48)#`

Overview

This chapter describes multimedia traffic control with IP multicast-Internet Group Management Protocol (IGMP). IGMP reduces unnecessary bandwidth usage on a per-port basis. For general information about IGMP, see **IGMP general operation and features** on page 7.

NOTE

The use of static multicast filters is described in the chapter titled "Traffic/Security Filters" in the Access Security Guide for your HPE switch.

IGMP general operation and features

In a network where IP multicast traffic is transmitted for various multimedia applications, you can use the switch to reduce unnecessary bandwidth usage on a per-port basis by configuring IGMP. In the factory default state (IGMP disabled), the switch simply floods all IP multicast traffic it receives on a given VLAN through all ports on that VLAN (except the port on which it received the traffic.) This can result in significant and unnecessary bandwidth usage in networks where IP multicast traffic is a factor. Enabling IGMP allows the ports to detect IGMP queries and report packets and manage IP multicast traffic through the switch.

IGMP is useful in multimedia applications such as LAN TV, desktop conferencing, and collaborative computing, where there is multipoint communication, that is, communication from one to many hosts, or communication originating from many hosts and destined for many other hosts. In such multipoint applications, IGMP is configured on the hosts, and multicast traffic is generated by one or more servers (inside or outside of the local network.) Switches in the network (that support IGMP) can then be configured to direct the multicast traffic to only the ports where needed. If multiple VLANs are configured, you can configure IGMP on a per-VLAN basis.

Enabling IGMP allows detection of IGMP queries and report packets used to manage IP multicast traffic through the switch. If no other querier is detected, the switch then also functions as the querier. If you need to disable the querier feature, you can do so using the IGMP configuration CLI commands, see **Configuring the querier function** on page 14.

NOTE

IGMP configuration on the switches operates at the VLAN context level.

IGMP operating features

Basic operation

In the factory default configuration, IGMP is disabled. To enable IGMP

- If multiple VLANs are not configured:Configure IGMP on the default VLAN (DEFAULT_VLAN; VID=1.)
- If multiple VLANs are configured:Configure IGMP on a per-VLAN basis for every VLAN where this feature is to be used.

Enhancements

With the CLI, you can configure these additional options:

Auto/blocked/ forward	You can use the console to configure individual ports to any of the following states: **Auto** (Default) Causes the switch to interpret IGMP packets and to filter IP multicast traffic based on the IGMP packet information for ports belonging to a multicast group. This means that IGMP traffic will be forwarded on a specific port only if an IGMP host or multicast router is connected to the port. **Blocked** Causes the switch to drop all IGMP transmissions received from a specific port, and also blocks all outgoing IP Multicast packets for that port, thus preventing IGMP traffic from moving through specific ports. **Forward** Causes the switch to forward all IGMP and multicast transmissions through the port.
Operation with or without IP addressing	This feature helps to conserve IP addresses by enabling IGMP to run on VLANs that do not have an IP address. See **Operation with or without IP addressing** on page 10. This is also referred as IGMP Snooping.
Querier capability	The switch performs querier function for IGMP on VLANs having an IP address when there is no other device in the VLAN acting as querier. See **Using the switch as querier** on page 25.

To configure high priority settings for traffic, see “Quality of Service: managing bandwidth more effectively” in the Advanced Traffic Management Guide.

NOTE

Whenever IGMP is enabled, the switch generates an Event Log message only after the querier election.

IP multicast traffic groups are identified by IP addresses in the range of 224.0.0.0 to 239.255.255.255. Also, incoming IGMP packets intended for reserved, or "well-known" multicast addresses, automatically flood through all ports (except the port on which the packets entered the switch).

For more information about IGMP, see **How IGMP operates** on page 9.

Number of IP multicast addresses allowed

The number of IGMP filters (addresses) and static multicast filters available is 2,038. Additionally, 16 static multicast filters are allowed. If multiple VLANs are configured, then each filter is counted once per VLAN in which it is used.

NOTE

The number of IGMP and static multicast filters available for 2530YA/YB is shown in the following table.

Platform	IPv4	IPv6
2530YA	502	502
2530YB	502	501

How IGMP operates

IGMP is used by IP hosts to report their multicast group memberships with neighboring multicast routers. It is an internal protocol of the IP suite. IGMP messages are encapsulated in IP datagrams, with an IP protocol number of 2. When enabled, IGMP operates in VLAN context. As a result, there is no need of a multicast routing protocol as long as the communication between IP hosts and multicast source is on the same network. If IP hosts and the multicast source are on different network segments, multicast routing is essential.

Multicast routers use IGMP to identify the groups having members on each of their attached physical networks. A multicast router or a switch enabled with IGMP can operate in any of the two roles:

- Querier
- Non Querier

Generally, only one Querier is available per physical network. When you enable IGMP, Querier election takes place and one of the devices perform the role of a Querier. The Querier is responsible for:

- Sending out IGMP group membership queries in a timed interval
- Retrieving IGMP membership reports from an active member
- Allowing to update the group membership table

The multicast group running version 2 of IGMP uses three fundamental types of messages to communicate:

Membership Query (Query)	The message sent always by the Querier to all the devices on the attached network enabled with IGMP. The Membership Query message is of two types: • General Query — Used to learn the groups which have members on the attached network. • Group-specific Query — Used to learn if a particular group has any members on the attached network. The above message types are differentiated by the Group Address. The Membership Query messages are referred as Query messages. To disable the querier feature, use the IGMP configuration CLI commands. For more information about the CLI commands, see **Configuring the querier function** on page 14.
Report (Join)	The message sent by a host to the querier to indicate that the host wants to be or is a member of a given group indicated in the report message.
Leave group	The message sent by a host to all routers 224.0.0.2 is to indicate that the host has ceased to be a member of a specific multicast group.

An IP multicast packet includes the multicast group (address) to which the packet belongs. When an IGMP client connected to a switch port needs to receive multicast traffic from a specific group, it joins the group by sending an IGMP report (join request) to the network. (The multicast group specified in the join request is determined by the requesting application running on the IGMP client.) When a network device with IGMP enabled receives the join request for a specific group, it forwards any IP multicast traffic it receives for that group through the port on which the join request was received. When the client is ready to leave the multicast group, it sends a Leave Group message to the network and ceases to be a group member. When the leave request is detected, the appropriate IGMP device ceases transmitting traffic for the designated multicast group through the port on which the leave request was received (as long as there are no other current members of that group on the affected port.)

Thus, IGMP identifies members of a multicast group (within a subnet) and allows IGMP-configured hosts (and routers) to join or leave multicast groups.

To display IGMP data showing active group addresses, reports, queries, querier access port, and active group address data (port, type, and access), see section "Internet Group Management Protocol (IGMP) Status" in appendix B, "Monitoring and Analyzing Switch Operation" of the Management and Configuration Guide for your switch.

Operation with or without IP addressing

You can configure IGMP on VLANs that do not have IP addressing. The benefit of IGMP without IP addressing is a reduction in the number of IP addresses you have to use and configure. This can be significant in a network with a large number of VLANs. The limitation on IGMP without IP addressing is that the switch cannot become Querier on any VLANs for which it has no IP address—so the network administrator must ensure that another IGMP device will act as Querier. It is also advisable to have an additional IGMP device available as a backup Querier.

Table 1: *Comparison of IGMP operation with and without IP addressing*

IGMP function available with IP addressing configured on the VLAN	Available without IP addressing?	Operating differences without an IP address
Forward multicast group traffic to any port on the VLAN that has received a join request for that multicast group.	Yes	None
Forward join requests (reports) to the Querier.	Yes	None
Configure individual ports in the VLAN to `Auto` (the default)/`Blocked`, or `Forward`.	Yes	None
Configure IGMP traffic forwarding to normal or high-priority forwarding.	Yes	None
Age-out IGMP group addresses when the last IGMP client on a port in the VLAN leaves the group.	Yes	Requires that another IGMP device in the VLAN has an IP address and can operate as Querier. This can be a multicast router or another switch configured for IGMP operation. (Hewlett Packard Enterprise recommends that the VLAN also include a device operating as a backup Querier in case the device operating as the primary Querier fails for any reason.)
Support Fast-Leave IGMP and Forced Fast-Leave IGMP (below.)	Yes	
Support automatic Querier election.	No	Querier operation not available.
Operate as the Querier.	No	Querier operation not available.
Available as a backup Querier.	No	Querier operation not available.

Automatic fast-leave IGMP

IGMP fast-leave is configured for ports on a per-VLAN basis. By default, the switches send IGMP Group-Specific Query message out of the interface, upon which the Leave Group message is received to ensure that no other receivers are connected to the interface. If receivers are directly attached to the switch, there is no point in sending the membership query as the receiver wanting to leave is the only connected host.

Fast-leave processing eliminates the IGMP Group-Specific Query message. Thus, it allows the switch to immediately remove an interface from the bridge table upon receiving the Leave Group message. This processing speeds up the overall leave process and also eliminates the CPU overhead of having to generate an IGMP Group-Specific Query message.

Depending on the switch model, fast-leave is enabled or disabled in the default configuration.

With fast-leave enabled and an IGMP Group Leave being received on a noncascaded port, the following events take place:

- The switch stops forwarding multicast traffic for that group to that port.
- Does not apply to cascaded ports.

When disabled or when the port is cascaded, the regular IGMP leave time is used (up to 10 seconds when the switch is not the IGMP Querier).

On switches that do not support data-driven IGMP, unregistered multicast groups are flooded to the VLAN rather than pruned. In this scenario, fast-leave IGMP can actually increase the problem of multicast flooding by removing the IGMP group filter before the Querier has recognized the IGMP leave. The Querier will continue to transmit the multicast group during this short time, and because the group is no longer registered, the switch will then flood the multicast group to all ports.

On HPE switches that do support data-driven IGMP ("Smart" IGMP), when unregistered multicasts are received the switch automatically filters (drops) them. Thus, the sooner the IGMP leave is processed, the sooner this multicast traffic stops flowing.

Because of the multicast flooding problem mentioned above, the IGMP fast-leave feature is disabled by default on all switches that do not support data-driven IGMP (see **Operation with or without IP addressing** on page 10). The feature can be enabled on these switches via an SNMP set of this object:

```
hpSwitchIgmpPortForceLeaveState.<vid>.<port number>
```

However, Hewlett Packard Enterprise does not recommend this because it will increase the amount of multicast flooding during the period between the client's IGMP leave and the Querier's processing of that leave. For more information on this topic, see **Forced fast-leave IGMP** on page 12.

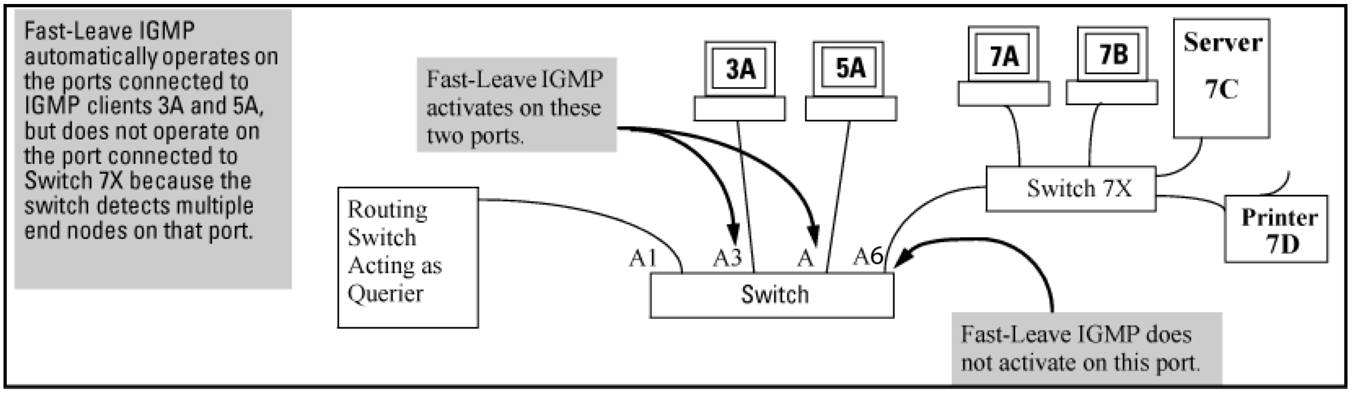
If a switch port has the following characteristics, the fast-leave operation will apply:

- Connected to only one end node.
- The end node currently belongs to a multicast group, that is, is an IGMP client.
- The end node subsequently leaves the multicast group.

Then the switch does not need to wait for the Querier status update interval, but instead immediately removes the IGMP client from its IGMP table and ceases transmitting IGMP traffic to the client. (If the switch detects multiple end nodes on the port, automatic fast-leave does not activate—regardless of whether one or more of these end nodes are IGMP clients.)

In the following figure, automatic fast-leave operates on the switch ports for IGMP clients "3A" and "5A," but not on the switch port for IGMP clients "7A" and "7B," server "7C," and printer "7D."

Figure 1: *Example of automatic fast-leave IGMP criteria*


Fast-Leave IGMP automatically operates on the ports connected to IGMP clients 3A and 5A, but does not operate on the port connected to Switch 7X because the switch detects multiple end nodes on that port.
Fast-Leave IGMP activates on these two ports.
3A
5A
7A
7B
Server 7C
Switch 7X
Printer 7D
Routing Switch Acting as Querier
A1
A3
A
A6
Switch
Fast-Leave IGMP does not activate on this port.

When client "3A" running IGMP is ready to leave the multicast group, it transmits a Leave Group message. Because the switch knows that there is only one end node on port A3, it removes the client from its IGMP table and halts multicast traffic (for that group) to port A3. If the switch is not the Querier, it does not wait for the actual

Querier to verify that there are no other group members on port A3. If the switch itself is the Querier, it does not query port A3 for the presence of other group members.

Fast-leave operation does not distinguish between end nodes on the same port that belong to different VLANs. Thus, for example, even if all the devices on port A6 shown in figure 1 belong to different VLANs, fast-leave does not operate on port A6.

Default (enabled) IGMP operation solves the "delayed leave" problem

Fast-leave IGMP is enabled by default. When fast-leave is disabled and multiple IGMP clients are connected to the same port on an IGMP device (switch or router), if only one IGMP client joins a given multicast group, then later sends a Leave Group message and ceases to belong to that group, the switch automatically retains that IGMP client in its IGMP table and continues forwarding IGMP traffic to the IGMP client until the Querier triggers confirmation that no other group members exist on the same port. This delayed leave operation means that the switch continues to transmit unnecessary multicast traffic through the port until the Querier renews multicast group status.

Configuring fast-leave IGMP

For information about fast-leave IGMP, see **Automatic fast-leave IGMP** on page 10.

Syntax:

```
ip igmp fastleave <port-list>
no ip igmp fastleave <port-list>
```

Enables IGMP fast-leaves on the specified ports in the selected VLAN.

The `no` form of the command disables IGMP fast-leave on the specified ports in the selected VLAN.

Use `show running` to display the ports per-VLAN on which fast-leave is disabled.

Default: Enabled

Forced fast-leave IGMP

When enabled, forced fast-leave IGMP speeds up the process of blocking unnecessary IGMP traffic to a switch port that is connected to multiple end nodes. (This feature does not activate on ports where the switch detects only one end node.) For example, in **Figure 1: Example of automatic fast-leave IGMP criteria** on page 11, even if you configured forced fast-leave on all ports in the switch, the feature would activate only on port A6 (which has multiple end nodes) when a Leave Group request arrived on that port.

When a port having multiple end node receives a Leave Group request from one end node for a given multicast group "X," forced fast-leave activates and waits a small amount of time to receive a join request from any other group "X" member on that port. If the port does not receive a join request for that group within the forced-leave interval, the switch then blocks any further group "X" traffic to the port.

Configuring forced fast-leave IGMP

For information about forced fast-leave, see **Forced fast-leave IGMP** on page 12.

Syntax:

```
vlan <vid> ip igmp forcedfastleave <port-list>
no vlan <vid> ip igmp forcedfastleave <port-list>
```

Enables IGMP forced fast-leave on the specified ports in the selected VLAN, even if they are cascaded.

The `no` form of the command disables forced fast-leave on the specified ports in the selected VLAN.

Use `show running` to display the ports per-VLAN on which forced fast-leave is enabled.

Default: Disabled

`show running-config`	Displays a nondefault IGMP forced fast-leave configuration on a VLAN. If configured, the `show running-config` output does not include forced fast-leave.
`forcedfastleave`	Can be used when there are multiple devices attached to a port.

Configuring delayed group flush

When enabled, this feature continues to filter IGMP groups for a specified additional period after IGMP leaves have been sent. The delay in flushing the group filter prevents unregistered traffic from being forwarded by the server during the delay period. In practice, this is rarely necessary on the switches, which support data-driven IGMP. (Data-driven IGMP, which is enabled by default, prunes off any unregistered IGMP streams detected on the switch.)

Syntax:

```
igmp delayed-flush <0-255>
```

Where leaves have been sent for IGMP groups, enables the switch to continue to flush the groups for a specified period. This command is applied globally to all IGMP-configured VLANs on the switch.

Range: 0 - 255; Default: Disabled (0)

Syntax:

```
show igmp delayed-flush
```

Displays the current `igmp delayed-flush` setting.

Configuring and displaying IGMP (CLI)

Configuring per-port IGMP traffic filters

Syntax:

```
vlan <vid> ip igmp [auto < port-list > | blocked < port-list > | forward < port-
list >]
```

Used in the VLAN context, specifies how each port handles IGMP traffic.

Default: auto.

NOTE

Where a static multicast filter is configured on a port, and an IGMP filter created by this command applies to the same port, the IGMP filter overrides the static multicast filter for any inbound multicast traffic carrying the same multicast address as is configured in the static filter. See section "Filter Types and Operation" in the "Port Traffic Controls" chapter of the Management and Configuration Guide for your switch.

Example:

Suppose that you want to configure IGMP as follows for VLAN 1 on the 100/1000T ports on a module in slot 1:

Ports 1-2	auto	Filter multicast traffic. Forward IGMP traffic to hosts on these ports that belong to the multicast group for which the traffic is intended. (Also forward any multicast traffic through any of these ports that is connected to a multicast router.)
Ports 3-4	forward	Forward all multicast traffic through this port.
Ports 5-6	blocked	Drop all multicast traffic received from devices on these ports.

The different states of IGMP control traffic are auto, forward and blocked.

auto	(Default) Causes the switch to interpret IGMP packets and to filter IP multicast traffic based on the IGMP packet information for ports belonging to a multicast group. This means that IGMP traffic will be forwarded on a specific port only if an IGMP host or multicast router is connected to the port.
forward	Causes the switch to forward all IGMP and multicast transmissions through the port.
blocked	Causes the switch to drop all IGMP transmissions received from a specific port, and also blocks all outgoing IP Multicast packets for that port, thus preventing IGMP traffic from moving through specific ports.

For a description of the default behavior of data-driven switches, see **Automatic fast-leave IGMP** on page 10.

Depending on the privilege level, you could use one of the following commands to configure IGMP on VLAN 1 with the above settings:

```
switch(config)# vlan 1 ip igmp auto 1,2
switch(config)# vlan 1 ip igmp forward 3,4
switch(config)# vlan 1 ip igmp blocked 5,6
```

```
switch(vlan-1)# ip igmp auto 1,2
switch(vlan-1)# vlan 1 ip igmpforward 3,4
switch(vlan-1)# blocked 5,6
```

The following command displays the VLAN and per-port configuration resulting from the above commands.

```
switch> show igmp vlan 1 config
```

Configuring the querier function

Syntax:

```
vlan <vid> ip igmp querier
no vlan <vid> ip igmp querier
```

This command disables or re-enables the ability for the switch to become querier if necessary.

The `no` version of the command disables the querier function on the switch. The `show ip igmp config` command displays the current querier command.

Default querier capability: Enabled

NOTE

It is necessary to have IP address for a switch to perform in a Querier role.

Configuring static multicast groups

Use this command to configure a group on the switch so that multicast traffic for that group can be forwarded with a receiver host. Traffic will be flooded to all the ports in the VLAN for this group.

Syntax:

```
ip igmp static-group <group-address>
no ip igmp static-group <group-address>
```

This command must be issued in a VLAN context.

Creates the IGMP static group with the specified <*group address*> on the selected VLAN. The no form of the command deletes the static group on the selected VLAN.

Viewing IGMP configuration for VLANs

Syntax:

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

Displays IGMP configuration for a specified VLAN or for all VLANs on the switch.

Displaying IGMP status for a VLAN

```
switch(vlan-22)# show ip igmp vlan 22

 IGMP Service Protocol Info

  Total VLANs with IGMP enabled                : 2
  Current count of multicast groups joined     : 2

  IGMP Filter Unknown Multicast: Disabled
  IGMP Filter Unknown Multicast Status: Disabled

  VLAN ID : 22
  VLAN Name : VLAN22
  IGMP version : 2
  Querier Address [this switch] : 10.255.128.2
  Querier Port :
  Querier UpTime : 1h 23m 55s
  Querier Expiration Time : 0h 1m 49s

  Active Group Addresses Type       Expires          Ports      Reports Queries
  ---------------------- ---------- ---------------- ---------- ------- -------
  226.0.6.7              Filter     0h 4m 6s         1          2       0
  226.0.6.8              Filter     0h 4m 5s         2          2       0
```

Viewing the current IGMP configuration

Syntax:

```
show ip igmp config
```

Displays IGMP configuration for all VLANs on the switch.

Syntax:

```
show ip igmp vlan <vid> config
```

Displays IGMP configuration for a specific VLAN on the switch, including per-port data.

For IGMP operating status, see the section "Internet Group Management Protocol (IGMP) status" in the chapter "Monitoring and Analyzing Switch Operation" of the Management and Configuration Guide for your switch.

Example:

Suppose that you have the following VLAN and IGMP configurations on the switch:

VLAN ID	VLAN name	IGMP enabled	Querier
1	DEFAULT_VLAN	Yes	No
22	VLAN-2	Yes	Yes
33	VLAN-3	No	Yes

You could use the CLI to display this data as follows:

Listing of IGMP configuration for all VLANs in the switch

```
switch(vlan-33)# show ip igmp config

 IGMP Service Config

  Control unknown multicast  [Yes] : Yes
  Forced fast leave timeout [0] : 4
  Delayed flush timeout [0] : 0
  Look-up Mode [mac] : mac

  VLAN ID VLAN Name    IGMP Enabled Querier Allowed IGMP Version Querier Interval
  ------- ------------ ------------ --------------- ------------ ----------------
  1       DEFAULT_VLAN Yes          No              2            125
  22      VLAN22       Yes          Yes             2            125
  33      VLAN33       No           Yes             2            125

switch(vlan-33)# show run

Running configuration:

; JL253A Configuration Editor; Created on release #WC.16.02.0000x
; Ver #0d:13.ef.7c.5f.fc.6b.fb.9f.fc.f3.ff.37.ef:09

hostname "Aruba-2930F-24G-4SFPP"
module 1 type jl253a
snmp-server community "public" unrestricted
vlan 1
   name "DEFAULT_VLAN"
   untagged 1-28
   ip address dhcp-bootp
   ip igmp
   no ip igmp querier
   exit
vlan 22
   name "VLAN22"
   no ip address
   ip igmp
   exit
vlan 33
   name "VLAN33"
   no ip address
   exit
```

The following version of the `show ip igmp` command includes the VLAN ID (*vid*) designation, and combines the above data with the IGMP per-port configuration:

Listing of IGMP configuration for a specific VLAN

```
switch(vlan-22)# show ip igmp vlan 22 config

IGMP Service VLAN Config

  VLAN ID : 22
  VLAN NAME : VLAN22
  IGMP Enabled [No] : Yes
  Querier Allowed [Yes] : Yes
  IGMP Version [2] : 2
  Strict Mode                         : No
  Last Member Query Interval (Seconds) [1] : 1
  Querier Interval [125] : 125
  Query Max. Response Time (Seconds) [10] : 10
  Robustness Count [2] : 2

  Port    Type        | Port Mode Forced Fast Leave Fast Leave
  ------- ---------- + --------- ----------------- ----------
  1       1000T       | Auto      No                Yes
  2       1000T       | Auto      No                Yes
  3       1000T       | Blocked   No                Yes
  4       1000T       | Forward   No                Yes
```

1 IGMP configuration for the selected VLAN.

2 IGMP configuration on the individual ports in the VLAN.

Viewing IGMP high-level statistics for all VLANs on the switch

Syntax:

```
show ip igmp statistics
```

Displaying statistics for IGMP joined groups

```
switch(vlan-22)#show ip igmp statistics

 IGMP Service Statistics

  Total VLANs with IGMP enabled                : 2
  Current count of multicast groups joined     : 2


 IGMP Joined Groups Statistics

  VLAN ID VLAN Name                        Total   Filtered Standard Static
EXCLUDE   INCLUDE
  ------- -------------------------------- ------ -------- -------- ------
```

```
--------- ---------
  1       DEFAULT_VLAN                     52     50       0        2
NA        NA
  22      VLAN22                           80     75       5        0
NA        NA
  33      VLAN33                           1100   1000     99       1
NA        NA
```

Viewing IGMP historical counters for a VLAN

Syntax:

```
show ip igmp vlan <vid> counters
```

Display of IGMP historical counters for a VLAN

```
switch(config)# show ip igmp vlan 1 counters

 IGMP service Vlan counters

  VLAN ID : 1
  VLAN Name : DEFAULT_VLAN

    General Query Rx                  : 58
    General Query Tx                  : 58
    Group Specific Query Rx           : 3
    Group Specific Query Tx           : 3
    V1 Member Report Rx               : 0
    V2 Member Report Rx               : 2
    V3 Member Report Rx               : 0
    Leave Rx                          : 0
    Unknown IGMP Type Rx              : 0
    Unknown Pkt Rx                    : 0
    Forward to Routers Tx Counter     : 0
    Forward to Vlan Tx Counter        : 0
    Port Fast Leave Counter           : 0
    Port Forced Fast Leave Counter    : 0
    Port Membership Timeout Counter   : 0
```

Viewing IGMP group address information

Syntax:

```
show ip igmp groups
```

Displaying IGMP groups address information

```
switch(vlan-22)# show ip igmp groups

 IGMP Group Address Information

  VLAN ID Group Address   Expires       UpTime        Last Reporter   | Type
  ------- --------------- ------------- ------------- --------------- + ------
  22      226.0.6.7       0h 3m 26s     0h 14m 22s    10.255.128.1    | Filter
  22      226.0.6.8       0h 3m 19s     0h 13m 20s    10.255.128.3    | Filter
  22      239.20.255.9    0h 0m 0s      0h 0m 0s                      | Static

Sample configuration is as shown:
```

```
switch(vlan-22)# show run

Running configuration:

; JL253A Configuration Editor; Created on release #WC.16.02.0000x
; Ver #0d:13.ef.7c.5f.fc.6b.fb.9f.fc.f3.ff.37.ef:09

hostname "Aruba-2930F-24G-4SFPP"
module 1 type jl253a
snmp-server community "public" unrestricted
vlan 1
   name "DEFAULT_VLAN"
   no untagged 1-4
   untagged 5-28
   no ip address
   ip igmp
   no ip igmp querier
   exit
vlan 22
   name "VLAN22"
   untagged 1-4
   ip address 10.255.128.2 255.255.255.0
   ip igmp
   ip igmp blocked 3
   ip igmp forward 4
   ip igmp static-group 239.20.255.9
   exit
vlan 33
   name "VLAN33"
   no ip address
   exit
```

Viewing IGMP group information for a VLAN with a filtered address

Syntax:

```
show ip igmp vlan <vid> group <ip-addr>
```

Group information for a VLAN with a filtered address group

```
switch(vlan-22)# show ip igmp vlan 22 group 226.0.6.7

 IGMP ports and group information for group 226.0.6.7

 VLAN ID: 22
 Uptime: 0h 15m 32s
 Last Reporter: 10.255.128.1
 Type: Filter

  Port  Port Type Port Mode Expires Access
  ----- --------- --------- ------- -----------
  1     1000T     Auto      253     host
```

Enabling or disabling IGMP on a VLAN

You can enable IGMP on a VLAN, along with the last-saved or default IGMP configuration (whichever was most recently set), or you can disable IGMP on a selected VLAN.

Syntax:

```
 ip igmp
no ip igmp
```

Enables IGMP on a VLAN. This command must be executed in a VLAN context.

Enabling IGMP on VLAN 1

```
switch(vlan-1)# vlan 1 ip igmp
```

– or –

```
switch(vlan-1)# ip igmp
```

Disabling IGMP on VLAN 1

```
switch(config)# no vlan 1 ip igmp
```

```
switch(vlan-1)# no ip igmp
```

NOTE

If you disable IGMP on a VLAN and then later re-enable IGMP on that VLAN, the switch restores the last-saved IGMP configuration for that VLAN. For more information on how switch memory operates, see the chapter "Switch Memory and Configuration" in the Management and Configuration Guide for your switch.

You can also combine the `ip igmp` command with other IGMP-related commands, as described in the following sections.

IGMP proxy forwarding

When a network has a border router connecting a PIM-SM domain to a PIM-DM domain, the routers that are completely within the PIM-DM domain have no way to discover multicast flows in the PIM-SM domain. When an IGMP join occurs on a router entirely within the PIM-DM domain for a flow that originates within the PIM-SM domain, it is never forwarded to the PIM-SM domain.

The IGMP proxy is a way to propagate IGMP joins across router boundaries. The proxy triggers the boundary router connected to a PIM-SM domain to query for multicast flows and forward them to the PIM-DM domain. IGMP needs to be configured on all VLAN interfaces on which the proxy is to be forwarded or received, and PIM-DM must be running for the traffic to be forwarded.

You can configure an IGMP proxy on a selected VLAN that will forward IP joins (reports) and IGMP leaves to the upstream border router between the two multicast domains. You must specify the VLANs on which the proxy is enabled as well as the address of the border router to which the joins are forwarded.

How IGMP proxy forwarding works

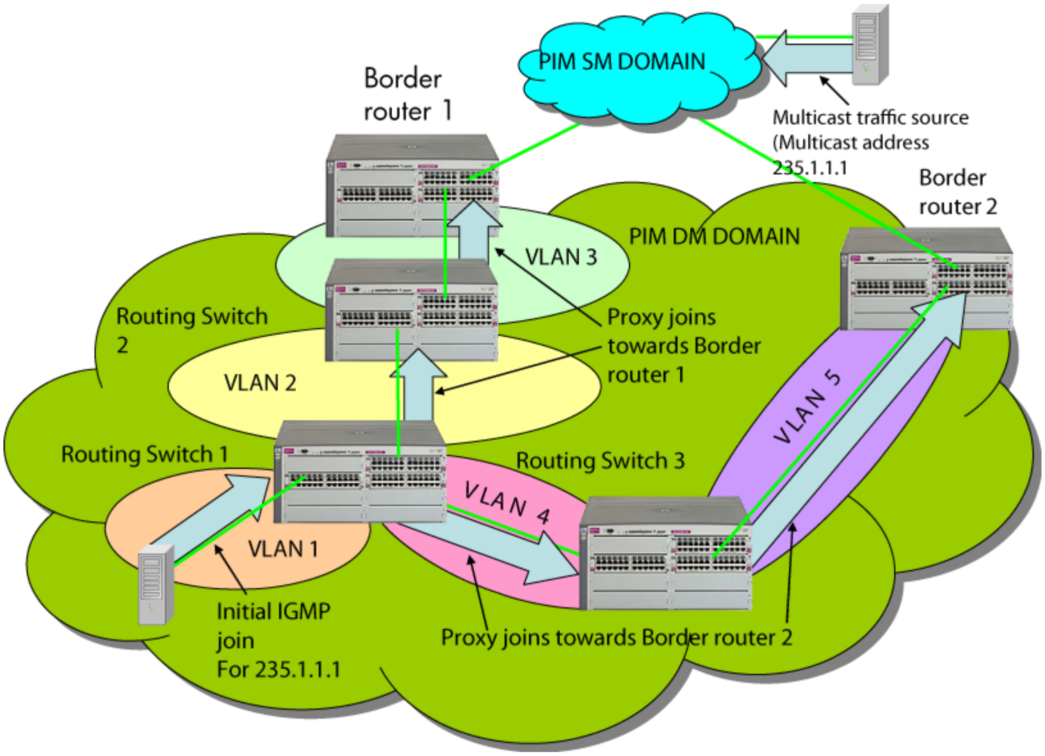
The following steps illustrate how to flood a flow from the PIM-SM domain into the PIM-DM domain when an IGMP join for that flow occurs in the PIM-DM domain. See **Figure 2: IGMP proxy example** on page 21.

Procedure

1. Configure Routing Switch 1 with the IGMP proxy forwarding function to forward joins toward Border Router 1; in addition, configure Routing Switch 1 to forward joins from VLAN 1 toward Border Router 2, as is VLAN 4 on Routing Switch 3.
2. Configure VLAN 2 on Routing Switch 2 to forward joins toward Border Router 1.

3. When the host connected in VLAN 1 issues an IGMP join for multicast address 235.1.1.1, the join is proxied by Routing Switch 1 onto VLAN 2 and onto VLAN 4. The routing information table in Routing Switch 1 indicates that the packet to Border Router 1 and Border Router 2 is on VLAN 2 and VLAN 4, respectively.

Figure 2: *IGMP proxy example*


PIM SM DOMAIN
Border router 1
Multicast traffic source (Multicast address 235.1.1.1
Border router 2
PIM DM DOMAIN
VLAN 3
Routing Switch 2
Proxy joins towards Border router 1
VLAN 2
VLAN 5
Routing Switch 1
Routing Switch 3
VLAN 4
VLAN 1
Initial IGMP join For 235.1.1.1
Proxy joins towards Border router 2

4. Routing Switch 2 then proxies the IGMP join into VLAN 3, which is connected to Border Router 1.
5. Border Router 1 uses PIM-SM to find and connect to the multicast traffic for the requested traffic. The traffic is flooded into the PIM-DM network where it is routed to the original joining host.
6. Additionally, the join was proxied from Routing Switch 3 to Border Router 2. At first, both border routers will flood the traffic into the PIM-DM domain. However, PIM-DM only forwards multicasts based on the shortest reverse path back to the source of the traffic as determined by the unicast routing tables (routing FIB.) Only one multicast stream is sent to the joining host. This configuration provides a redundant in case the first fails.

Configuring IGMP proxy (CLI)

For more information on IGMP proxy, see **IGMP general operation and features** on page 7.

Adding or leaving a multicast domain

Syntax:

```
igmp-proxy-domain <domain-name> [< border-router-ip-address > | <mcast-range |
all>]
no igmp-proxy-domain <domain-name> [< border-router-ip-address > | <mcast-range |
all>]
```

The `no` form of the command is used to remove a multicast domain.

All VLANs associated with the domain must first be removed for this command to work. See the `no` form of `igmp-proxy` in the VLAN context command.

<domain-name>	User-defined name to associate with the PIM border router and multicast range that is being sent toward the border router.
<border-router-ip-addr>	The IP address of the border router toward which IGMP proxy packets are sent. Not required for the `no` form of the command. NOTE The current routing FIB determines the best path toward the border router and therefore the VLAN that a proxy is sent out on
<low-bound-ip-address| all>	The low boundary (inclusive) of the multicast address range to associate with this domain (for example, 234.0.0.1.) If `all` is selected, the multicast addresses in the range of 224.0.1.0 to 239.255.255.255 are included in this domain. NOTE Addresses 224.0.0.0 to 224.0.0.255 are never used, because these addresses are reserved for protocols.
<high-bound-ip-address>	The high boundary (inclusive) of the multicast address range to associate with this domain (for example, 236.1.1.1.)

The following example shows the IGMP proxy border IP address (111.11.111.111) being configured.

IGMP proxy border IP address command

```
switch(config)# igmp-proxy-domain Bob 111.11.111.111
```

The following example shows the lower and upper boundaries of the multicast address range associated with the domain named Bob.

Setting the lower and upper bounds for multicasting

```
switch(config)# igmp-proxy-domain Bob 111.11.111.111 234.0.0.1
switch(config)# igmp-proxy-domain Bob 111.11.111.111 236.1.1.1
```

VLAN context command

This command is performed when in VLAN context mode. When a query occurs on the upstream interface, an IGMP join is sent for all multicast addresses that are currently joined on the downstream interface.

Syntax:

```
igmp-proxy <domain-name>
no igmp-proxy <domain-name>
```

Tells the VLAN which IGMP proxy domains to use with joins on the VLAN.

The `no` version of the command with no domain name specified removes all domains associated with this VLAN.

Multiple different domains may be configured in the same VLAN context where the VLAN is considered the downstream interface. The domain name must exist prior to using this command to add the domain. If the unicast routing path to the specified IP address was through the specified VLAN, no proxy IGMP would occur, that is, a proxy is not sent back out on the VLAN that the IGMP join came in on.

If no unicast route exists to the border router, no proxy IGMP packets are sent.

IGMP proxy show command

Syntax:

```
show igmp-proxy {<entries | domains | vlans>}
```

Shows the currently active IGMP proxy entries, domains, or VLANs.

Showing active IGMP proxy entries

```
switch(config)# show igmp-proxy entries

 Total number of multicast routes: 2

 Multicast Address Border Address   VID   Multicast Domain
 ----------------- --------------   ----- ------
 234.43.209.12     192.168.1.1      1     George
 235.22.22.12      15.43.209.1      1     SAM
 226.44.3.3        192.168.1.1      2     George
```

Showing IGMP proxy domains

```
switch(config)# show igmp-proxy domains

  Total number of multicast domains: 5

 Multicast Domain  Multicast Range         Border Address Active entries
 ----------------  ----------------------- -------------- --------------
 George            225.1.1.1/234.43.209.12 192.168.1.1    2
 SAM               235.0.0.0/239.1.1.1     15.43.209.1    1
 Jane              236.234.1.1/236.235.1.1 192.160.1.2    0
 Bill              ALL                     15.43.209.1    0
```

Showing active IGMP proxy VLANs

```
switch(config)# show igmp-proxy vlans

 IGMP PROXY VLANs

 VID     Multicast Domain   Active entries
 ------  ----------------   --------------
 1            George            1
 1            Sam               1
 1            Jane              0
 2            George            1
 4            George            0
 4            Bill              0
```

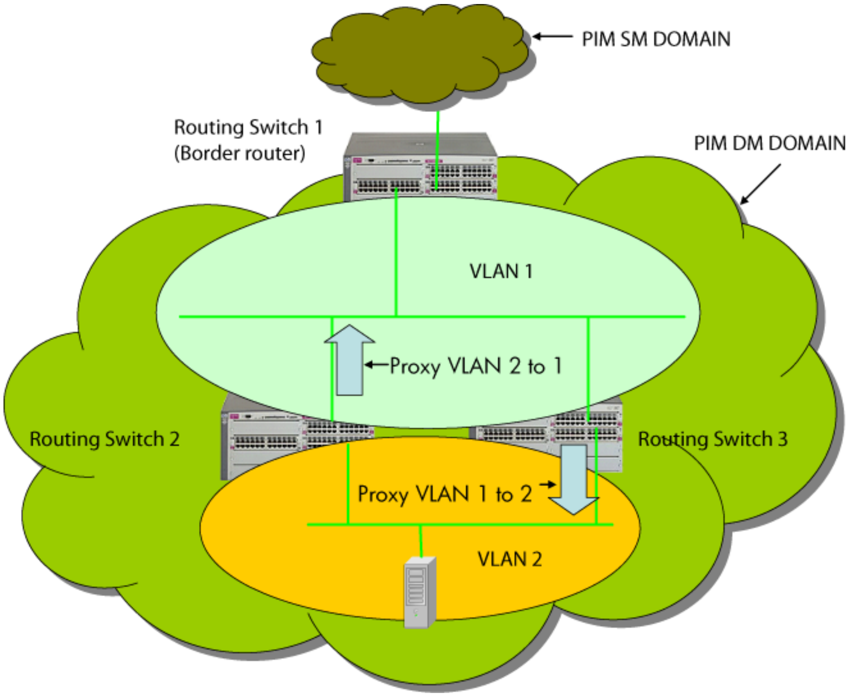
Operating notes for IGMP proxy forwarding

- You can configure up to 12 multicast domains, which indicate a range of multicast addresses and the IP address of the PIM-SM/PIM-DM border router.
- You must give each domain a unique name, up to 20 characters.
- The domains may have overlapping multicast ranges.
- The IP address of the border router may be the same or different in each configured domain.
- Duplicate IGMP joins are automatically prevented, or leaves that would remove a flow currently joined by multiple hosts.
- Range overlap allows for redundant connectivity and the ability for multicasts to arrive from different border routers based on the shortest path back to the source of the traffic.
- The configured domain names must be associated with one or more VLANs for which the proxy joins are to be done.
- All routers in the path between the edge router receiving the initial IGMP packets and the border router have to be configured to forward IGMP using IGMP proxy.
- All upstream and downstream interfaces using IGMP proxy forwarding require IGMP and PIM to be enabled.
- You must remove all VLAN associations with the domain name before that domain name can be removed.
- The appropriate border routers must be used for each VLAN, or PIM-DM will not forward the traffic. This could occur when multiple border routers exist. It may be necessary to configure multiple overlapping domains if the multicast source address can generate the same multicast address and have different best paths to the PIM-DM domain.

CAUTION

Be careful to avoid configuring an IGMP forward loop, because this would leave the VLANs in a joined state forever once an initial join is sent from a host. For example, a join is issued from the host in VLAN 2 and Routing Switch 2 will proxy the join onto VLAN 1. Routing Switch 3 will then proxy the join back onto VLAN 2 and increment its internal count of the number of joins on VLAN 2. Even after the host on VLAN 2 issues a leave, the proxy join will remain and refresh itself each time a query occurs on VLAN 2. This type of loop could be created with multiple routers if an IGMP proxy is allowed to get back to the VLAN of the router that initially received the IGMP join from a host as shown.

Figure 3: *Proxy loop scenario*



Using the switch as querier

The function of the IGMP Querier is to poll other IGMP-enabled devices in an IGMP-enabled VLAN to elicit group membership information. The switch performs this function if there is no other device in the VLAN, such as a multicastrouter, to act as Querier. Although the switch automatically ceases Querier operation in an IGMP-enabled VLAN if it detects another Querier on the VLAN, you can also use the switch's CLI to disable the Querier capability for that VLAN.

NOTE

A Querier is required for proper IGMP operation. For this reason, if you disable the Querier function on a switch, ensure that there is an IGMP Querier (and, preferably, a backup Querier) available on the same VLAN.

If the switch becomes the Querier for a particular VLAN (for example, the DEFAULT_VLAN), then subsequently detects queries transmitted from another device on the same VLAN, the switch ceases to operate as the Querier for that VLAN. If this occurs, the switch Event Log lists a pair of messages similar to these:

```
I 01/15/12 09:01:13 igmp:
DEFAULT_VLAN: Other Querier detected
I 01/15/12 09:01:13 igmp:
DEFAULT_VLAN: This switch is no longer Querier
```

In the above scenario, if the other device ceases to operate as a Querier on the default VLAN, the switch detects this change and can become the Querier as long as it is not pre-empted by some other IGMP Querier on the VLAN. In this case, the switch Event Log lists messages similar to the following to indicate that the switch has become the Querier on the VLAN:

```
I 01/15/12 09:21:55 igmp: DEFAULT_VLAN:
Querier Election in process
I 01/15/12 09:22:00 igmp: DEFAULT_VLAN:
This switch has been elected as Querier
```

IP multicast filters

IP multicast addresses occur in the range from 224.0.0.0 through 239.255.255.255 (which corresponds to the Ethernet multicast address range of 01005e-000000 through 01005e-7fffff.) When a switch has a static traffic/ security filter configured with a "multicast" filter type and a "multicast address" in this range, the switch will use the static filter unless IGMP learns of a multicast group destination in this range. In this case, IGMP dynamically takes over the filtering function for the multicast destination addresses, as long as the IGMP group is active. If the IGMP group subsequently deactivates, the switch returns filtering control to the static filter.

Reserved addresses excluded from IP multicast filtering

Traffic to IP multicast groups in the IP address range of 224.0.0.0 to 224.0.0.255 will always be flooded because addresses in this range are "well known" or "reserved" addresses. Thus, if IP multicast is enabled, and there is an IP multicast group within the reserved address range, traffic to that group will be flooded instead of filtered by the switch.

NOTE

In IP mode, nonreserved multicast IP addresses are not displayed as "reserved" addresses.

Well-known or reserved multicast addresses excluded from IP multicast filtering

Each multicast host group is identified by a single IP address in the range of 224.0.0.0 through 239.255.255.255. Specific groups of consecutive addresses in this range are termed "well-known" addresses and are reserved for predefined host groups. IGMP does not filter these addresses, so any packets the switch receives for such addresses are flooded out all ports assigned to the VLAN on which they were received (except the port on which the packets entered the VLAN.)

The following table lists the 32 well-known address groups (8192 total addresses) that IGMP does not filter on.

NOTE

“**X**” is any value from 0 to 255.

Table 2: *IP multicast address groups excluded from IGMP filtering*

Groups of consecutive addresses in the range of 224.0.0.*X* to 239.0.0.*X*		Groups of consecutive addresses in the range of 224.128.0.*X* to 239.128.0.*X*	
224.0.0.*x*	232.0.0.*x*	224.128.0.*x*	232.128.0.*x*
225.0.0.*x*	233.0.0.*x*	225.128.0.*x*	233.128.0.*x*
226.0.0.*x*	234.0.0.*x*	226.128.0.*x*	234.128.0.*x*
227.0.0.*x*	235.0.0.*x*	227.128.0.*x*	235.128.0.*x*
228.0.0.*x*	236.0.0.*x*	228.128.0.*x*	236.128.0.*x*
229.0.0.*x*	237.0.0.*x*	229.128.0.*x*	237.128.0.*x*
230.0.0.*x*	238.0.0.*x*	230.128.0.*x*	238.128.0.*x*
231.0.0.*x*	239.0.0.*x*	231.128.0.*x*	239.128.0.*x*

NOTE

With aliasing limitation associated with MAC mode, certain non reserved multicast IP addresses are displayed as "reserved" addresses.

For example: 225.0.0.x Multicast IP address is aliased to 224.0.0.x to be displayed as "reserved".

IGMPv3

The Internet Group Management Protocol (IGMP) is used by IPv4 systems (hosts and routers) to report their IP multicast group membership to any neighboring multicast routers. This chapter is to describe version 3 of IGMP. Version 1, specified in [RFC-1112], was the first widely deployed version. Version 2, specified in [RFC-2236], added support for “low leave latency”, that is, a reduction in the time it takes for a multicast router to learn that there are no longer any members of a particular group present on an attached network. Version 3 adds support for “source filtering”, that is, the ability for a system to report interest in receiving packets *only* from specified source addresses, or from *all but* specified source addresses, sent to a particular multicast address. Version 3 is designed to be interoperable with Versions 1 and 2.

In the following figure, DUT-1 becomes the igmpv3 querier. Client-1 start receiving multicast traffic for group 235.6.6.6 from source 60.0.0.100 and client-2 start receiving multicast traffic for group 235.6.6.6 from source 60.0.0.200.

If multiple igmp version devices are available in the network, the igmp querier device must have the lower version of IGMP. This can be achieved by executing the `no ip igmp querier` command under the **vlan** context on other devices.

Figure 4: *Basic topology and configuration for IGMPv3*

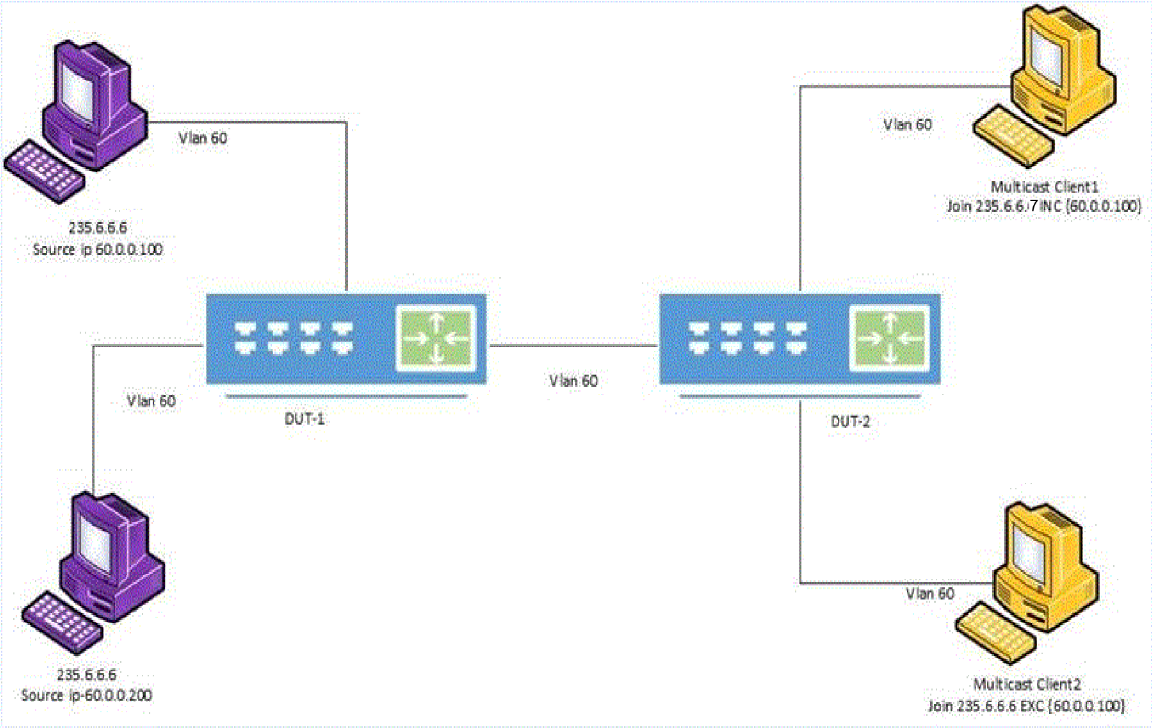


Table 3: *IGMPv3 configuration for Basic topology and configuration for IGMPv3*

DUT-1 configurations	DUT-2 configurations
DUT-1(config)#igmp lookup-mode ip	DUT-2(config)#igmp lookup-mode ip
DUT-1(config)#vlan 60 ip address 60.0.0.1/24	DUT-2(config)#vlan 60 ip address 60.0.0.2/24
DUT-1(config)#vlan 60 ip igmp version 3	DUT-2(config)#vlan 60 ip igmp version 3
	DUT-2(config)#no vlan 60 ip igmp querier

IGMPv3 commands

igmp lookup-mode

To first configure IGMPv3, the igmp lookup-mode must be changed from the default mac mode to ip mode. Use the `ip igmp lookup-mode` command to set the IGMP snooping lookup mode.

IGMPv2 works both in ip mode and mac mode. Lookup-mode is applicable with IGMP disabled on all VLANs.

Syntax

```
ip igmp lookup-mode
```

Options

`mac`: Uses MAC look-up. (Default value)

`ip`: Uses IP look-up.

igmp reload

This command is used to reset the IGMP state on all interfaces.

Syntax

```
igmp reload
```

Example output

```
IGMP application is in Error State as System Resources are exhausted. Traffic will
flood.
Please disable IGMP on all VLANs or Issue the Command "igmp reload" to take it out
of Error.
Refer to your product manual for information on IGMP resource consumption.
this is the output for igmp reload
```

ip igmp

Use the **vlan** context to configure IGMPv3 on the switch.

Syntax

```
ip igmp
```

Options

`last-member-query-interval`: Sets the time interval that the querier waits to receive a response from members to a group-specific query message. It also specifies the amount of time between successive group-specific query messages; the default value is 1 second.

`query-max-response-time`: Sets the time interval to wait for a response to a query; the default value is 10 seconds.

`robustness`: Sets the number of times to retry a query; the default value is 2.

`version`: Sets the IGMP version to use; the default value is 2.

ip igmp version

This command sets the IGMP version and completes igmpv3 configuration, enabling igmpv3 on the switch. Note that the default value is 2.

Syntax

```
ip igmp version
```

```
no ip igmp version
```

Parameters

`<2-3>`: The protocol version to use; the default is 2.

`no`: resets the version to 2.

ip igmp last-member-query-interval

Syntax

```
ip igmp last-member-query-interval
```

```
no ip igmp last-member-query-interval
```

Parameters

`<1-2>`: The number of seconds between successive group-specific query messages; the default is 1.

The `no` version resets the value to its default value of 1 second.

ip igmp querier

By default, IGMP querier is enabled. To disable querier functionality, use the following command:

```
switch (vlan 1)#no ip igmp querier
```

Syntax

```
ip igmp querier
```

Parameters

`interval`: Sets the interval in seconds between IGMP queries; the default is 125.

ip igmp query-max-response-time

Syntax

```
ip igmp query-max-response-time

no ip igmp query-max-response-time
```

Parameters

`<10-128>`: The number of seconds to wait for a response to a query; the default value is 10.

The `no` version resets the value to its default value of 10 seconds.

ip igmp robustness

Syntax

```
ip igmp robustness

no ip igmp robustness
```

Parameters

`<1-8>`: The number of times to retry a query; the default is 2.

The `no` version resets the value to its default value of 2.

show ip igmp

This command is used to show IGMP information for all VLANs

Syntax

```
show ip igmp
```

Example output

Below is the output when version is set to 3.

```
switch(vlan-60)# show ip igmp

 IGMP Service Protocol Info

  Total VLANs with IGMP enabled                : 1
  Current count of multicast groups joined     : 2
  IGMP Filter Unknown Multicast: Disabled
  IGMP Filter Unknown Multicast Status: Disabled

  VLAN ID : 1
  VLAN Name : DEFAULT_VLAN
  IGMP version : 2
  IGMP is not enabled

  VLAN ID : 60
  VLAN Name : VLAN60
  IGMP version : 3
  Querier Address : 60.0.0.1
  Querier Port : 23
  Querier UpTime : 0h 10m 9s
  Querier Expiration Time : 0h 3m 34s

  Active Group Addresses Tracking Vers Mode Uptime   Expires
  ---------------------- -------- ---- ---- -------- --------
  235.6.6.6              Filter   3    INC  0m 3s    4m 17s
  235.6.6.7              Filter   3    EXC  0m 3s    4m 16s

Sample configuration is as shown:

switch(vlan-60)# show run

Running configuration:

; JL253A Configuration Editor; Created on release #WC.16.02.0000x
; Ver #0d:13.ef.7c.5f.fc.6b.fb.9f.fc.f3.ff.37.ef:09

hostname "Aruba-2930F-24G-4SFPP"
module 1 type jl253a
igmp lookup-mode ip
snmp-server community "public" unrestricted
vlan 1
   name "DEFAULT_VLAN"
   no untagged 1-2,23
   untagged 3-22,24-28
   ip address dhcp-bootp
   exit
vlan 60
   name "VLAN60"
   untagged 1-2,23
   ip address 60.0.0.2 255.255.255.0
   ip igmp
   no ip igmp querier
   ip igmp version 3
   exit
```

show ip igmp vlan 1

This command is used to show IGMP information for a VLAN.

Syntax

```
show ip igmp vlan 1
```

Example output

Below is the output when version is set to 3.

```
switch(vlan-60)#  show ip igmp vlan 60

 IGMP Service Protocol Info

  Total VLANs with IGMP enabled                : 1
  Current count of multicast groups joined     : 2

  IGMP Filter Unknown Multicast: Disabled
  IGMP Filter Unknown Multicast Status: Disabled

  VLAN ID : 60
  VLAN Name : VLAN60
  IGMP version : 3
  Querier Address : 60.0.0.1
  Querier Port : 23
  Querier UpTime : 0h 11m 44s
  Querier Expiration Time : 0h 4m 5s

  Active Group Addresses Tracking Vers Mode Uptime   Expires
  ---------------------- -------- ---- ---- -------- --------
  235.6.6.6              Filter   3    INC  1m 38s   4m 13s
  235.6.6.7              Filter   3    EXC  1m 38s   4m 19s
```

show ip igmp vlan group

This command is used to show IGMP group information for a VLAN.

Syntax

```
show ip igmp vlan <vid> group
```

Example output

Below is the output when version is set to 3.

Port and source ipv4 address options are introduced under `group`. The following output captures the details of these options.

```
switch(config)# show ip igmp vlan <vid> group
    IPV4-ADDR      Show IGMP VLAN group address information.
    PORT           Show a list of all the IGMP groups on the specified port.

switch(config)# show ip igmp vlan <vid> group <ip4-addr>
    source         Show IGMP VLAN source address information.


switch(config)# show ip igmp vlan <vid> group <ip4-addr> source
    IPV4-ADDR      Specify the source IPv4 address.

switch(config)# show ipv4 igmp vlan <vid> group <ip4-addr> source <ip4-addr>


switch(vlan-60)# show ip igmp vlan 60 group 235.6.6.6

 IGMP ports and group information for group 235.6.6.6
```

```
  VLAN ID : 60   VLAN Name : VLAN60

  Group Address : 235.6.6.6
  Last Reporter : 10.255.128.1
  Group Type    : Filter

                                   V1       V2       Filter   Sources   Sources
  Port Vers Mode Uptime   Expires  Timer    Timer    Timer    Forwarded Blocked
  ---- ---- ---- -------- -------- -------- -------- -------- --------- --------
  1    3    INC  2m 38s   3m 13s   -        0m 0s    -        1         0


  Group Address   : 235.6.6.6
  Source Address  : 60.0.0.100
  Source Type     : Filter

  Port Mode Uptime   Expires  Configured Mode
  ---- ---- -------- -------- ---------------
  1    INC  2m 38s   3m 13s   auto
```

Usage errors

Error condition	Error message
Attempt to pass a nonexistent group	`ipv4 address Group address is not found.`

show ip igmp vlan group source

This command is used to show IGMP group/source information for a VLAN.

Syntax

```
show ip igmp vlan <vid> group <ip4-addr> source <ip4-addr>
```

Example output

Below is the output when version is set to 3.

```
switch(vlan-60)# show ip igmp vlan 60 group 235.6.6.6 source 60.0.0.100
  VLAN ID : 60     VLAN Name : VLAN60

  Group Address   : 235.6.6.6
  Source Address  : 60.0.0.100
  Source Type     : Filter

  Port Mode Uptime   Expires  Configured Mode
  ---- ---- -------- -------- ---------------
  1    INC  3m 31s   2m 20s   auto
```

Usage errors

Error condition	Error message
Attempt to pass a nonexistent group	`ipv4 address Group address is not found.`

show ip igmp vlan group port

This command is used to show IGMP group/source information for a VLAN port.

Syntax

```
show ip igmp vlan <vid> group <ip4-addr> port <port>
```

Example output

Below is the output when version is set to 3.

```
switch(vlan-60)# show ip igmp vlan 60 group port 1

  VLAN ID : 60     Name : VLAN60

  Group Address : 235.6.6.6
  Last Reporter : 10.255.128.1
  Group Type    : Filter

 Port Vers Mode Uptime   Expires  Timer    Timer    Timer    Forwarded Blocked
 ---- ---- ---- -------- -------- -------- -------- -------- --------- --------
 1    3    INC  8m 53s   3m 24s   -        0m 0s    -        1         0

  Group Address   : 235.6.6.6
  Source Address  : 60.0.0.100
  Source Type     : Filter

 Port Mode Uptime   Expires  Configured Mode
 ---- ---- -------- -------- ---------------
 1    INC  8m 54s   3m 23s   auto
```

show ip igmp vlan counters

This command is used to show IGMP counters for a VLAN.

Syntax

```
show ip igmp vlan <vid> counters
```

Example output

Below is the output when version is set to 3.

```
switch(vlan-60)# show ip igmp vlan 60 counters

IGMP service Vlan counters

VLAN ID : 60   NAME : VLAN60

                                            Rx           Tx
                                            ------------ ------------
 V1 All Hosts Query                         0            0
 V2 All Hosts Query                         0            0
 V3 All Hosts Query                         12           0
 V1 Group Specific Query                    0            0
 V2 Group Specific Query                    0            0
 V3 Group Specific Query                    8            0
 Group and Source Specific Query            12           0
 V3 Member Report                           22           22
 V2 Member Report                           8            0
 V1 Member Report                           0            0
 V2 Member Leave                            0            0
 Forward to Routers                         0            32
 Forward to VLAN                            0            26

 Errors:
```

```
 Unknown IGMP Type                          0
 Unknown Packet                             0
 Malformed Packet                           0
 Bad Checksum                               0
 Martian Source                             0
 Packet received on IGMP-disabled Interface 0
 Interface Wrong Version Query              0

 Port Counters:

 Fast Leave          : 4
 Forced Fast Leave   : 0
 Membership Timeout  : 0
```

show ip igmp vlan statistics

This command is used to show IGMP statistics for a VLAN.

Syntax

```
show ip igmp vlan <vid> statistics
```

Example output

Below is the output when version is set to 3.

```
switch(vlan-60)# show ip igmp vlan 60 statistics

 IGMP Statistics

  VLAN ID : 60
  VLAN Name : VLAN60

  Number of Filtered Groups     : 2
  Number of Standard Groups     : 0
  Number of Static Groups       : 0
  Total Multicast Groups Joined : 2


 Mode         EXCLUDE      INCLUDE
 ------------ ------------ ------------
 Filtered     1            1
 Standard     0            0
 Total        1            1
```

show ip igmp statistics

This command is used to show global IGMP statistics.

Syntax

```
show ip igmp statistics
```

Example output

NOTE

The `show ip igmp statistics` is common for both IGMPv2 and IGMPv3. Output for the "EXCLUDE" and "INCLUDE" columns is displayed as "NA" if the version configured is IGMPv2 (as shown in the following example).

```
switch# show ip igmp statistics

IGMP Service Statistics

Total VLANs with IGMP enabled                : 1
Current count of multicast groups joined     : 2

IGMP Joined Groups Statistics

  VLAN ID VLAN Name                        Total  Filtered Standard Static
EXCLUDE   INCLUDE
  ------- -------------------------------- ------ -------- -------- ------
--------- ---------
  1       DEFAULT_VLAN                     2      2        0        0
1         1
```

show ip igmp vlan config

This command is used to show the IGMP configuration for a VLAN.

Syntax

```
show ip igmp vlan (vid) config
```

Example output

Below is the output when version is set to 3.

```
switch(vlan-60)# show ip igmp vlan 60 config

 IGMP Service VLAN Config

  VLAN ID : 60
  VLAN NAME : VLAN60
  IGMP Enabled [No] : Yes
  Querier Allowed [Yes] : No
  IGMP Version [2] : 3
  Strict Mode                         : No
  Last Member Query Interval (Seconds) [1] : 1
  Querier Interval [125] : 125
  Query Max. Response Time (Seconds) [10] : 10
  Robustness Count [2] : 2

  Port    Type       | Port Mode Forced Fast Leave Fast Leave
  ------- ---------- + --------- ----------------- ----------
  1       1000T      | Auto      No                Yes
  2       1000T      | Auto      No                Yes
  23      1000T      | Auto      No                Yes
```

show ip igmp config

This command is used to show the global IGMP configuration.

Syntax

```
show ip igmp config
```

Example output

Below is the output when version is set to 3.

```
switch(vlan-60)# show ip igmp config

 IGMP Service Config

  Control unknown multicast  [Yes] : Yes
  Forced fast leave timeout [0] : 4
  Delayed flush timeout [0] : 0
  Look-up Mode [mac] : ip

  VLAN ID VLAN Name    IGMP Enabled Querier Allowed IGMP Version Querier Interval
  ------- ------------ ------------ --------------- ------------ ----------------
  1       DEFAULT_VLAN No           Yes             2            125
  60      VLAN60       Yes          No              3            125
```

show ip igmp vlan group

This command is used to show IGMP group information for a VLAN.

Syntax

```
show ip igmp vlan <vid> group
```

Example output

```
switch# show ip igmp vlan 60 group

 IGMP ports and group information for group 235.6.6.6

  VLAN ID : 60   VLAN Name : VLAN60

  Group Address : 235.6.6.6
  Last Reporter : 10.255.128.1
  Group Type    : Filter

                                   V1       V2       Filter   Sources   Sources
  Port Vers Mode Uptime   Expires  Timer    Timer    Timer    Forwarded Blocked
  ---- ---- ---- -------- --------- --------- --------- --------- ---------- --------
  1    3    INC  15m 47s  2m 44s   -        0m 0s    -        1         0

  Group Address   : 235.6.6.6
  Source Address  : 60.0.0.100
  Source Type     : Filter

  Port Mode Uptime   Expires  Configured Mode
  ---- ---- -------- -------- ---------------
  1    INC  15m 47s  2m 44s   auto

 IGMP ports and group information for group 235.6.6.7

  VLAN ID : 60   VLAN Name : VLAN60

  Group Address : 235.6.6.7
  Last Reporter : 10.255.128.3
  Group Type    : Filter

                                   V1       V2       Filter   Sources   Sources
  Port Vers Mode Uptime   Expires  Timer    Timer    Timer    Forwarded Blocked
  ---- ---- ---- -------- -------- -------- -------- -------- --------- --------
  2    3    EXC  15m 48s  2m 39s   -        0m 0s    2m 39s   0         1

  Group Address   : 235.6.6.7
  Source Address  : 60.0.0.100
  Source Type     : Filter

  Port Mode Uptime   Expires  Configured Mode
  ---- ---- -------- -------- ---------------
  2    EXC  15m 48s  2m 39s   auto
```

igmp reload

This command is used to reset IGMP on all interfaces when error state is displayed.

Syntax

```
igmp reload
```

Example output

```
IGMP application is in Error State as System Resources are exhausted. Traffic will
flood.
Please disable IGMP on all VLANs or Issue the Command "igmp reload" to take it out
of Error.
Refer to your product manual for information on IGMP resource consumption.
this is the ouput for igmp reload
```

Enabling forwarding of IP directed broadcasts (CLI)

To enable forwarding of IP directed broadcasts, enter the following CLI command:

Syntax:

```
no ip directed-broadcast
```

```
switch(config)# ip directed-broadcast
```

HPE software makes the forwarding decision based on the routing switch's knowledge of the destination network prefix. Routers cannot determine that a message is unicast or directed broadcast apart from the destination network prefix. The decision to forward or not forward the message is by definition only possible in the last-hop router.

Introduction to feature

Wake-on-LAN (WOL) is an Ethernet computer networking standard that allows a computer to be turned on or awakened by a network message. The message is sent by a program executed on the same local area network. Messages can also be initiated from another network by using subnet directed broadcasts or a WOL gateway service. WOL is implemented using specially designed packet called magic packet. WOL is enabled on the switch by using a `ip directed-broadcast` command with an IPv4 configuration, which can be used to specify an access list name, thus avoiding unnecessary administrative overhead.

IP directed-broadcasts would only be forwarded if permitted by the associated access-list. An `implicit deny` at the end of an access list drops all IP directed-broadcasts that are not authorized according to the access-list entries.

> NOTE
>
> IP routing must be enabled on the switch for this feature to work.

CLI commands

The optional association of access-list with IP directed-broadcast allows user to filter directed broadcast traffic alone based on access-list entry rule. The feature's CLI includes an optional parameter to specify access-list name along with the already existing `ip directed-broadcast`command. The access-list rule specified is applied globally on the switch and is not specific to any vlan's alone. There is an Implicit Deny at the end of an access list that will drop all IP Directed Broadcasts that do not match any of the access list entries.

Configuration commands

Enable IP directed broadcast forwarding for Wake-on-LAN support. An optional ACL can also be applied to control what packets are forwarded.

Syntax

```
Switch(config)# ip directed-broadcast [access-group <ACL-ID>]
```

access-group

Apply the specified access control list.

access-list-name-str

ASCII string specifying an ACL

Example configuration

```
Switch(config)# ip directed-broadcast [access-group] <wol-acl>
```

<wol-acl> entries

```
ip access-list extended <wol-acl>
10 permit ip 192.168.1.1 255.255.255.0 182.168.1.1 55.255.255.0
20 deny ip 172.168.1.1 255.255.255.0 162.168.1.1 255.255.255.0
Exit
```

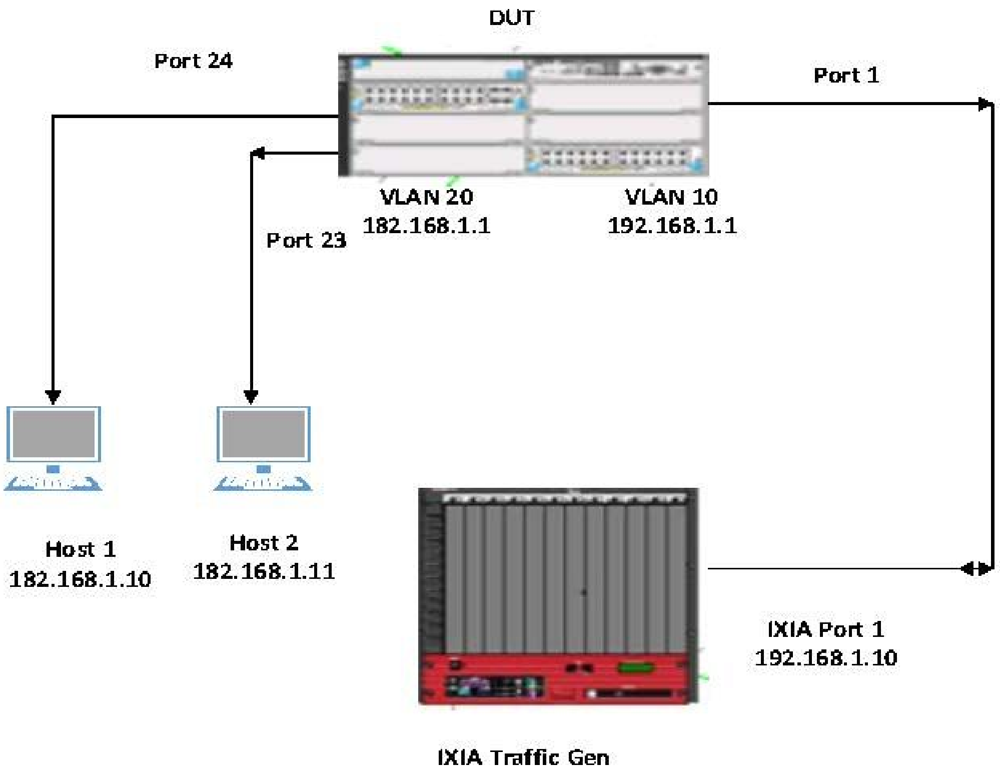
Example running configuration

```
; J9573A Configuration Editor; Created on release #xx.15.18.0000x
; Ver #06:7c.fd.ff.ff.3f.ef:57
hostname "switch"
module 1 type j9573x
ip access-list extended "wol-acl"
....10 permit ip 192.168.1.10 0.0.0.0 182.168.1.1 0.0.0.255
....exit

ip directed-broadcast access-group "wol-acl"
ip routing
snmp-server community "public" unrestricted
oobm
....ip address dhcp-bootp
    exit
vlan 1
....name "DEFAULT_VLAN"
....no untagged 1,23-24
....untagged 2-22,25-26
....ip address dhcp-bootp
....exit
vlan 10
....name "VLAN10"
....untagged 1
....ip address 192.168.1.1 255.255.255.0
....exit
vlan 20
....name "VLAN20"
....untagged 23-24
```

```
....ip address 182.168.1.1 255.255.255.0
....exit
```

Figure 5: *Configuration diagram*



NOTE

- If specified ACL ID is nonexisting, it is not possible to associate with IP Directed Broadcast. An error will be shown to the user.
- It is not allowed to delete an ACL which is associated with IP Directed Broadcast and on attempt, an error message will be shown to user.
- The same ACL *wol-acl* can be applied to any other interface like VLAN, port, and tunnel.

Show commands

IP directed broadcast hit counts for the associated access-list with can be displayed using the `show` command.

Show statistics

Show IPV4 ACL Statistics.

Syntax

```
show statistics aclv4 <acl-id>
```

Options

`port <port>`

`vlan` <*vlan-id*> vlan

`ip-directed-broadcast`

NOTE

Please note that the existing help text of all other parameters listed other than newly added `ip-directed-broadcast` will remain the same.

Syntax

```
show statistics aclv4 <acl-name-str>
```

ip-directed-broadcast

Show Statistics for the IP Directed Broadcast ACL.

```
switch # show statistics aclv4 wol-acl ip-directed-broadcast
HitCounts for ip-directed-broadcast ACL wol-acl
Total
(       0 )    10 permit ip 192.168.1.1 255.255.255.0 182.168.1.1 55.255.255.0
(       0 )    20 deny ip 172.168.1.1 255.255.255.0 162.168.1.1 255.255.255.0
```

`Clear` command

The hit count statistics for ACL on IP directed broadcast can be cleared using clear command.

Syntax

```
clear statistics aclv4 <acl-id>
```

Options

port <`port`>
vlan <`vlan-id`> vlan
<`ip-directed-broadcast`>

Reset IPV4 Statistics.

NOTE

Please note that the existing help text of all other parameters listed other than newly added `ip-directed-broadcast` will remain the same.

Syntax

```
clear statistics aclv4 <acl-name-str>
```

ip-directed-broadcast Clear Statistics for the IP Directed Broadcast ACL.

`show access-list` command

The existing “show access-list” command will have the following modification to support ip- directed-broadcast.

Syntax

```
show access-list
```

Options

<`ACL-ID`> [*config*]

<`config`>

<`ip-directed-broadcast`>

ports <<`PORT-LIST`>>

```
  <radius>
  <resources>
```

Show Access Control List Information.

NOTE

Please note that the existing help of all other parameters listed other than newly added ip-directed-broadcast will remain the same.

Show ACL's applied to IP Directed Broadcast traffic

```
show access-list <ip-directed-broadcast>
```

```
Switch # show access-list ip-directed-broadcast

Access Lists for IP Directed Broadcast
IPv4                   : wol-acl   Type: Extended
```

If user uses already existing `show access-list <ACL_NAME-STR>` command, the status of ACL on IP Directed Broadcast will be shown `applied` as in this example below.

```
switch # sh access-list wol-acl
Access Control Lists
.......Name: wol-acl
 ......Type: Extended
.......Applied: Yes
.......SEQ  Entry
-----------------------------------------------------------------------------
10  .Action: permit
 ......Src IP: 192.168.1.1       Mask: 255.255.255.0     Port(s):
.......Dst IP: 182.168.1.1       Mask: 55.255.255.0      Port(s):
.......Proto : IP
 ......TOS   : -                 Precedence: -
20  Action: deny
.......Src IP: 172.168.1.1       Mask: 255.255.255.0     Port(s):
.......Dst IP: 162.168.1.1       Mask: 255.255.255.0     Port(s):
 ......Proto : IP
 ......TOS   : -                 Precedence: -
```

Disabling the directed broadcasts

```
switch(config)# no ip directed-broadcast
```

Chapter 4
Dynamic Host Configuration Protocol

The Dynamic Host Configuration Protocol (DHCP) is used for configuring hosts with IP address and other configuration parameters without user intervention. The protocol is composed of three components:

- DHCP client
- DHCP server
- DHCP relay agent

For more information, see **Overview of DHCP** on page 51.

Enabling DHCP relay

The DHCP relay function is enabled by default on an HPE routing switch. However, if DHCP has been disabled, you can re-enable it by entering the following command at the global configuration level:

```
switch(config)# dhcp-relay
```

To disable the DHCP relay function, enter the `no` form of the command:

```
switch(config)# no dhcp-relay
```

Using DHCP Option 12 to send a hostname

This feature allows you to include the hostname in the DHCP packet sent to the DHCP server. This is disabled by default. The command must be executed from the global configuration level.

Syntax:

```
dhcp host-name-option
no dhcp host-name-option
```

Sends the hostname option with DHCP packets. Use the `no` form of the command to not include the hostname in the packet.

The maximum size of the hostname is 32 characters.

Default: disabled

DHCP Option 12 command

```
switch(config)# dhcp host-name-option
```

SNMP support

A MIB object supports enabling and disabling the DHCP Option 12 feature. It is added in the `hpicfDhcpclient.mib`. The hostname is retrieved from the MIB variable SYSNAME. Validity checks on the name include:

- The name starts with a letter, ends with a letter or a digit, and can have letters, hyphens, or digits in between the first and last characters.
- The maximum size supported for a hostname is 30 characters. If SYSNAME is more than 30 characters, then DHCP Option 12 will not be included in the packet.
- The minimum number of characters supported for a hostname is one character. If the SYSNAME in the MIB is null, then DHCP Option 12 will not be included in the packet.

Configuring a BOOTP/DHCP relay gateway

The DHCP relay agent selects the lowest-numbered IP address on the interface to use for DHCP messages. The DHCP server then uses this IP address when it assigns client addresses. However, this IP address may not be the same subnet as the one on which the client needs the DHCP service.

This feature provides a way to configure a gateway address for the DHCP relay agent to use for DHCP requests, rather than the DHCP relay agent automatically assigning the lowest-numbered IP address.

You must be in VLAN context to use this command, for example:

```
switch# config
switch(config)# vlan 1
switch(vlan-1)#
```

Syntax:

```
ip bootp-gateway ip-addr
```

Allows you to configure an IP address for the DHCP relay agent to use for DHCP requests. The IP address must have been configured on the interface.

Default: Lowest-numbered IP address

If the IP address has not already been configured on the interface (VLAN), you will see the message shown in the following example.

Example of trying to configure an IP address that is not on this interface (VLAN)

```
switch# config
switch(config)# vlan 1
switch(vlan-1)# ip bootp-gateway 10.10.10.1
The IP address 10.10.10.1 is not configured on this VLAN.
```

Viewing the BOOTP gateway

To display the configured BOOTP gateway for an interface (VLAN) or all interfaces, enter this command. You do not need to be in VLAN context mode.

Syntax:

```
show dhcp-relay bootp-gateway [vlan vid]
```

Displays the configured BOOTP gateway for a specified VLAN (interface.) If a specific VLAN ID is not entered, all VLANs and their configured BOOTP gateways display.

The following example shows an IP address being assigned to a gateway for VLAN 22, and then displayed using the `show dhcp-relay bootp-gateway` command.

Assigning a gateway to an interface and then displaying the information

```
switch(vlan-22)ip bootp-gateway 12.16.18.33
switch(vlan-22)# exit
switch(config)# show dhcp-relay bootp-gateway vlan 22


 BOOTP Gateway Entries


 VLAN                    BOOTP Gateway
 --------------------- ----------------
 VLAN 22                 12.16.18.33
```

Operating notes

- If the configured BOOTP gateway address becomes invalid, the DHCP relay agent returns to the default behavior (assigning the lowest-numbered IP address.)
- If you try to configure an IP address that is not assigned to that interface, the configuration fails and the previously configured address (if there is one) or the default address is used.

Configuring an IP helper address

To add the IP address of a DHCP server for a specified VLAN on a routing switch, enter the `ip helper-address` command at the VLAN configuration level as in the following example:

```
switch(config)# vlan 1
switch(vlan-1)# ip helper-address ip-addr
```

To remove the DHCP server helper address, enter the `no` form of the command:

```
switch(vlan-1)# no ip helper-address ip-addr
```

Operating notes

- You can configure up to 4000 IP helper addresses on a routing switch. The helper addresses are shared between the DHCP relay agent and UDP forwarder feature.
- A maximum of sixteen IP helper addresses is supported in each VLAN.

Disabling the hop count in DHCP requests

For more information, see **Hop count in DHCP requests** on page 51.

To disable the default behavior of a DHCP relay agent so that the hop count in a DHCP client request is not increased by one at each hop when it is forwarded to a DHCP server, enter the `no dhcp-relay hop-count-increment` command at the global configuration level:

```
switch(config)# no dhcp-relay hop-count-increment
```

To reset the default function, which increases the hop count in each DHCP request forwarded to a DHCP server, enter the following command:

```
switch(config)# dhcp-relay hop-count-increment
```

Operating notes

- By default, the DHCP relay agent increases the hop count in each DHCP request by one. You must enter the `no dhcp-relay hop-count-increment` command to disable this function.
- You enter the `no dhcp-relay hop-count-increment` command at the global configuration level. The command is applied to all interfaces on the routing switch that are configured to forward DHCP requests.
- This DHCP relay enhancement applies only to DHCP requests forwarded to a DHCP server. The server does not change the hop count included in the DHCP response sent to DHCP clients.
- When you disable or re-enable the DHCP hop count function, no other behavior of the relay agent is affected.
- You can configure the DHCP relay hop count function only from the CLI; you cannot configure this software feature from the drop-down menus.
- A new MIB variable, hpDhcpRelayHopCount, is introduced to support SNMP management of the hop count increment by the DHCP relay agent in a switch.

Verifying the DHCP relay configuration

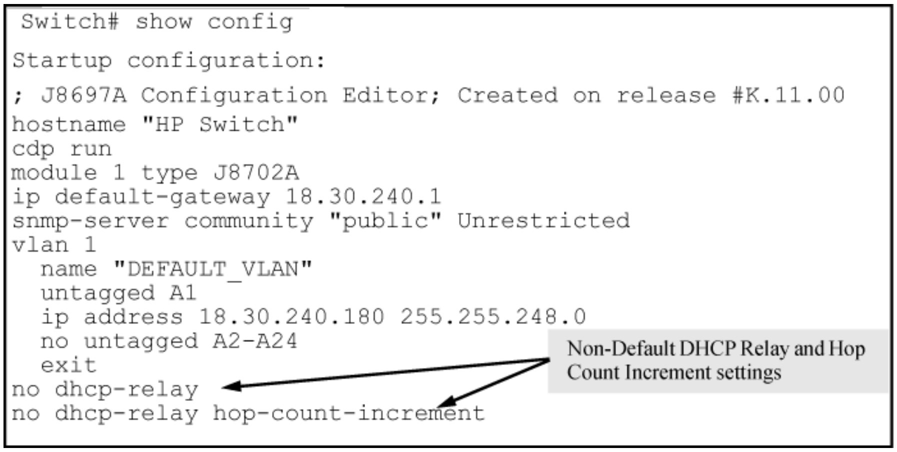
Viewing the DHCP relay setting

Use the `show config` command (or `show running` for the running-config file) to display the current DHCP relay setting.

NOTE

The DHCP relay and hop count increment settings appear in the `show config` command output only if the non-default values are configured. For more information about the DHCP hop count increment, see **Hop count in DHCP requests** on page 51.

Displaying startup configuration with DHCP relay and hop count increment disabled



```
 Switch# show config

Startup configuration:

; J8697A Configuration Editor; Created on release #K.11.00
hostname "HP Switch"
cdp run
module 1 type J8702A
ip default-gateway 18.30.240.1
snmp-server community "public" Unrestricted
vlan 1
   name "DEFAULT_VLAN"
   untagged A1
   ip address 18.30.240.180 255.255.248.0
   no untagged A2-A24
   exit
no dhcp-relay
no dhcp-relay hop-count-increment
```

Non-Default DHCP Relay and Hop Count Increment settings

Viewing DHCP helper addresses

This command displays the list of currently configured IP Helper addresses for a specified VLAN on the switch.

Syntax:

```
show ip helper-address [vlan vlan-id]
```

Displays the IP helper addresses of DHCP servers configured for all static VLANS in the switch or on a specified VLAN, regardless of whether the DHCP relay feature is enabled. The `vlan vlan-id` parameter specifies a VLAN ID number.

Example

The following command lists the currently configured IP Helper addresses for VLAN 1.

Displaying IP helper addresses

```
switch(config)# show ip helper-address vlan 1

 IP Helper Addresses

  IP Helper Address
  -----------------
  10.28.227.97
  10.29.227.53
```

Viewing the hop count setting

To verify the current setting for increasing the hop count in DHCP requests, enter the `show dhcp-relay` command. The current setting is displayed next to DHCP Request Hop Count Increment.

Displaying hop count status

```
switch# show dhcp-relay
Status and Counters - DHCP Relay Agent
DHCP Relay Agent Enabled        : Yes
DHCP Request Hop Count Increment: Disabled
Option 82 Handle Policy         : Replace
Remote ID                       : MAC Address

Client Requests       Server Responses
Valid     Dropped      Valid    Dropped
--------- ----------   --------- ----------
1425          2          1425      0
```

Viewing the MAC address for a routing switch

To view the MAC address for a given routing switch, execute the `show system-information` command in the CLI.

Using the CLI to view the switch MAC address

```
switch(config)# show system information

Status and Counters - General System Information
System Name       : switch
System Contact    :
System Location   :

MAC Age Time (sec) : 300

Time Zone          : 0
Daylight Time Rule : None


Software revision : K.15.06.0000x       Base MAC Addr     : 00110a-a50c20
ROM Version       : K.15.13             Serial Number     : LP713BX00E
Allow V1 Modules  : No

Up Time           : 32 days             Memory  - Total  : 128,839,680
CPU Util (%)      : 0                            Free    : 65,802,416
```

```
IP Mgmt - Pkts Rx : 5,372,271          Packet   - Total  : 6750
          Pkts Tx : 298,054            Buffers    Free   : 5086
                                                  Lowest : 4441
                                                  Missed : 0
```

Configuring Option 82

For information on Option 82, see the sections beginning with **DHCP Option 82** on page 52.

Syntax:

```
dhcp-relay option 82 [append [validate] | replace [validate] | drop [validate] |
keep] [ip | mac | mgmt-vlan]
```

append

Configures the switch to append an Option 82 field to the client DHCP packet. If the client packet has existing Option 82 fields assigned by another device, the new field is appended to the existing fields.

The appended Option 82 field includes the switch Circuit ID (inbound port number*) associated with the client DHCP packet and the switch Remote ID. The default switch remote ID is the MAC address of the switch on which the packet was received from the client.

To use the incoming VLAN's IP address or the Management VLAN IP address (if configured) for the remote ID instead of the switch MAC address, use the `ip` or `mgmt-vlan` option (below.)

replace

Configures the switch to replace existing Option 82 fields in an inbound client DHCP packet with an Option 82 field for the switch.

The replacement Option 82 field includes the switch circuit ID (inbound port number*) associated with the client DHCP packet and the switch remote ID. The default switch remote ID is the MAC address of the switch on which the packet was received from the client.

To use the incoming VLAN's IP address or the Management VLAN IP address (if configured) for the remote ID instead of the switch MAC address, use the `ip` or `mgmt-vlan` option (below.)

drop

Configures the routing switch to unconditionally drop any client DHCP packet received with existing Option 82 fields. This means that such packets will not be forwarded. Use this option where access to the routing switch by untrusted clients is possible.

If the routing switch receives a client DHCP packet without an Option 82 field, it adds an Option 82 field to the client and forwards the packet. The added Option 82 field includes the switch circuit ID (inbound port number*) associated with the client DHCP packet and the switch remote ID. The default switch remote ID is the MAC address of the switch on which the packet was received from the client.

To use the incoming VLAN's IP address or the Management VLAN IP address (if configured) for the remote ID instead of the switch MAC address, use the `ip` or `mgmt-vlan` option (below.)

keep

For any client DHCP packet received with existing Option 82 fields, configures the routing switch to forward the packet as-is, without replacing or adding to the existing Option 82 fields.

validate

Operates when the routing switch is configured with append, replace, or drop as a forwarding policy. With `validate` enabled, the routing switch applies stricter rules to an incoming Option 82 server response to determine whether to forward or drop the response. For more information, see **Validation of server response packets** on page 58.

[ip | mac | mgmt-vlan]

Specifies the remote ID suboption that the switch uses in Option 82 fields added or appended to DHCP client packets. The type of remote ID defines DHCP policy areas in the client requests sent to the DHCP server. If a remote ID suboption is not configured, the routing switch defaults to the `mac` option. See **Option 82 field content** on page 54.

- `ip:`

  Specifies the IP address of the VLAN on which the client DHCP packet enters the switch.
- `mac:`

  Specifies the routing switch's MAC address. (The MAC address used is the same MAC address that is assigned to all VLANs configured on the routing switch.) This is the default setting.
- `mgmt-vlan:`

  Specifies the IP address of the (optional) management VLAN configured on the routing switch. Requires that a management VLAN is already configured on the switch. If the management VLAN is multinetted, the primary IP address configured for the management VLAN is used for the remote ID.If you enter the `dhcp-relay option 82` command without specifying either `ip` or `mac`, the MAC address of the switch on which the packet was received from the client is configured as the remote ID. For information about the remote ID values used in the Option 82 field appended to client requests, see **Option 82 field content** on page 54.

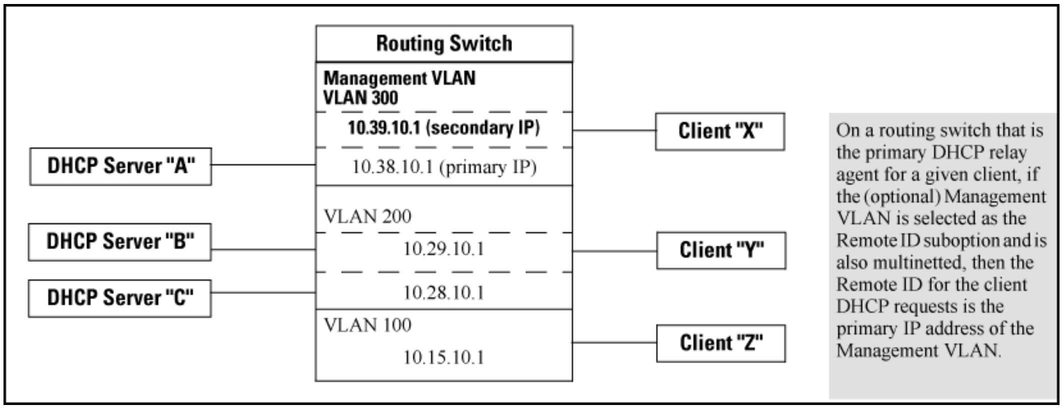
Example

In the routing switch shown below, option 82 has been configured with `mgmt-vlan` for the remote ID.

```
switch(config)# dhcp-relay option 82 append mgmt-vlan
```

The resulting effect on DHCP operation for clients X, Y, and Z is shown in the following table.

Figure 6: *DHCP Option 82 when using the management VLAN as the remote ID suboption*



On a routing switch that is the primary DHCP relay agent for a given client, if the (optional) Management VLAN is selected as the Remote ID suboption and is also multinetted, then the Remote ID for the client DHCP requests is the primary IP address of the Management VLAN.

Table 4: *DHCP operation for the topology in Figure DHCP Option 82 when using the management VLAN as the remote ID suboption*

Client	Remote ID	giaddr	DHCP server	
X	10.38.10.1	10.39.10.1	A only	If a DHCP client is in the management VLAN, its DHCP requests can go only to a DHCP server that is also in the management VLAN. Routing to other VLANs is not allowed.
Y	10.38.10.1	10.29.10.1	B or C	Clients outside of the management VLAN can send DHCP requests only to DHCP servers outside of the management VLAN. Routing to the management VLAN is not allowed.
Z	10.38.10.1	10.15.10.1	B or C	

Operating notes

- This implementation of DHCP relay with Option 82 complies with the following RFCs:
  - RFC 2131
  - RFC 3046
- Moving a client to a different port allows the client to continue operating as long as the port is a member of the same VLAN as the port through which the client received its IP address. However, rebooting the client after it moves to a different port can alter the IP addressing policy the client receives if the DHCP server is configured to provide different policies to clients accessing the network through different ports.
- The IP address of the primary DHCP relay agent receiving a client request packet is automatically added to the packet, and is identified as the giaddr (gateway interface address.) (That is, the giaddr is the IP address of the VLAN on which the request packet was received from the client.) For more information, see RFC 2131 and RFC 3046.
- DHCP request packets from multiple DHCP clients on the same relay agent port will be routed to the same DHCP servers. When using 802.1X on a switch, a port's VLAN membership may be changed by a RADIUS server responding to a client authentication request. In this case the DHCP servers accessible from the port may change if the VLAN assigned by the RADIUS server has different DHCP helper addresses than the VLAN used by unauthenticated clients.
- Where multiple DHCP servers are assigned to a VLAN, a DHCP client request cannot be directed to a specific server. Thus, where a given VLAN is configured for multiple DHCP servers, all of these servers should be configured with the same IP addressing policy.
- Where routing switch "A" is configured to insert its MAC address as the remote ID in the Option 82 fields appended to DHCP client requests, and upstream DHCP servers use that MAC address as a policy boundary for assigning an IP addressing policy, then replacing switch "A" makes it necessary to reconfigure the upstream DHCP servers to recognize the MAC address of the replacement switch. This does not apply in the case where an upstream relay agent "A" is configured with `option 82 replace`, which removes the Option 82 field originally inserted by switch "A."
- Relay agents without Option 82 can exist in the path between Option 82 relay agents and an Option 82 server. The agents without Option 82 forward client requests and server responses without any effect on Option 82 fields in the packets.
- If the routing switch cannot add an Option 82 field to a client's DHCP request because the message size exceeds the MTU size, the request is forwarded to the DHCP server without Option 82 data and an error message is logged in the switch's Event Log.
- Because routing is not allowed between the management VLAN and other VLANs, a DHCP server must be available in the management VLAN if clients in the management VLAN require a DHCP server.

- If the management VLAN IP address configuration changes after `mgmt-vlan` has been configured as the remote ID suboption, the routing switch dynamically adjusts to the new IP addressing for all future DHCP requests.
- The management VLAN and all other VLANs on the routing switch use the same MAC address.

Overview of DHCP

The DHCP client sends broadcast request packets to the network; the DHCP servers respond with broadcast packets that offer IP parameters, such as an IP address for the client. After the client chooses the IP parameters, communication between the client and server is by unicast packets.

HPE routing switches provide the DHCP relay agent to enable communication from a DHCP server to DHCP clients on subnets other than the one the server resides on. The DHCP relay agent transfers DHCP messages from DHCP clients located on a subnet without a DHCP server to other subnets. It also relays answers from DHCP servers to DHCP clients.

The DHCP relay agent is transparent to both the client and the server. Neither side is aware of the communications that pass through the DHCP relay agent. As DHCP clients broadcast requests, the DHCP relay agent receives the packets and forwards them to the DHCP server. During this process, the DHCP relay agent increases the hop count by one before forwarding the DHCP message to the server. A DHCP server includes the hop count from the DHCP request that it receives in the response that it returns to the client.

DHCP packet forwarding

The DHCP relay agent on the routing switch forwards DHCP client packets to all DHCP servers that are configured in the table administrated for each VLAN.

Unicast forwarding

The packets are forwarded using unicast forwarding if the IP address of the DHCP server is a specific host address. The DHCP relay agent sets the destination IP address of the packet to the IP address of the DHCP server and forwards the message.

Broadcast forwarding

The packets are forwarded using broadcast forwarding if the IP address of the DHCP server is a subnet address or IP broadcast address (255.255.255.255.) The DHCP relay agent sets the DHCP server IP address to broadcast IP address and is forwarded to all VLANs with configured IP interfaces (except the source VLAN.)

Enabling DHCP relay operation

For the DHCP relay agent to work on the switch, you must complete the following steps:

Procedure

1. Enable DHCP relay on the routing switch (the default setting.)
2. Ensure that a DHCP server is servicing the routing switch.
3. Enable IP routing on the routing switch.
4. Ensure that there is a route from the DHCP server to the routing switch and back.
5. Configure one or more IP helper addresses for specified VLANs to forward DHCP requests to DHCP servers on other subnets.

Hop count in DHCP requests

When a DHCP client broadcasts requests, the DHCP relay agent in the routing switch receives the packets and forwards them to the DHCP server (on a different subnet, if necessary.) During this process, the DHCP relay agent increments the hop count before forwarding DHCP packets to the server. The DHCP server, in turn, includes the hop count from the received DHCP request in the response sent back to a DHCP client.

As a result, the DHCP client receives a non-zero hop count in the DHCP response packet. Because some legacy DHCP/BootP clients discard DHCP responses that contain a hop count greater than one, they may fail to boot up properly. Although this behavior is in compliance with RFC 1542, it prevents a legacy DHCP/BootP client from being automatically configured with a network IP address.

DHCP Option 82

Option 82 is called the relay agent information option and is inserted by the DHCP relay agent when forwarding client-originated DHCP packets to a DHCP server. Servers recognizing the relay agent information option may use the information to implement IP address or other parameter assignment policies. The DHCP server echoes the option back verbatim to the relay agent in server-to-client replies, and the relay agent strips the option before forwarding the reply to the client.

The relay agent information option is organized as a single DHCP option that contains one or more suboptions that convey information known by the relay agent. The initial suboptions are defined for a relay agent that is co-located in a public circuit access unit. These include a circuit ID for the incoming circuit and a remote ID that provides a trusted identifier for the remote high-speed modem.

The routing switch can operate as a DHCP relay agent to enable communication between a client and a DHCP server on a different subnet. Without Option 82, DHCP operation modifies client IP address request packets to the extent needed to forward the packets to a DHCP server. Option 82 enhances this operation by enabling the routing switch to append an Option 82 field to such client requests. This field includes two suboptions for identifying the routing switch (by MAC address or IP address) and the routing switch port the client is using to access the network. A DHCP server with Option 82 capability can read the appended field and use this data as criteria for selecting the IP addressing it will return to the client through the usual DHCP server response packet. This operation provides several advantages over DHCP without Option 82:

- An Option 82 DHCP server can use a relay agent's identity and client source port information to administer IP addressing policies based on client and relay agent location within the network, regardless of whether the relay agent is the client's primary relay agent or a secondary agent.
- A routing switch operating as a primary Option 82 relay agent for DHCP clients requesting an IP address can enhance network access protection by blocking attempts to use an invalid Option 82 field to imitate an authorized client, or by blocking attempts to use response packets with missing or invalid Option 82 suboptions to imitate valid response packets from an authorized DHCP server.
- An Option 82 relay agent can also eliminate unnecessary broadcast traffic by forwarding an Option 82 DHCP server response only to the port on which the requesting client is connected, instead of broadcasting the DHCP response to all ports on the VLAN.

NOTE

The routing switch's DHCP relay information (Option 82) feature can be used in networks where the DHCP servers are compliant with RFC 3046 Option 82 operation. DHCP servers that are not compliant with Option 82 operation ignore Option 82 fields.

Some client applications can append an Option 82 field to their DHCP requests.

It is not necessary for all relay agents on the path between a DHCP client and the server to support Option 82, and a relay agent without Option 82 should forward DHCP packets regardless of whether they include Option 82 fields. However, Option 82 relay agents should be positioned at the DHCP policy boundaries in a network to provide maximum support and security for the IP addressing policies configured in the server.

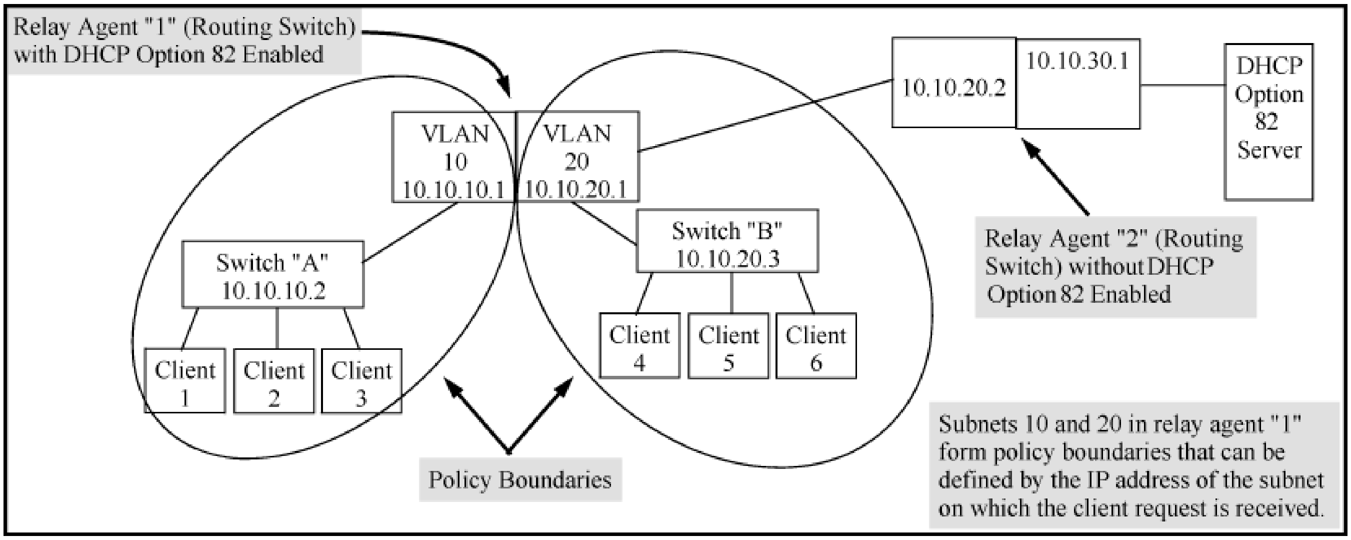
For more information, see the documentation provided with the server application.

Option 82 server support

To apply DHCP Option 82, the routing switch must operate in conjunction with a server that supports Option 82. (DHCP servers that do not support Option 82 typically ignore Option 82 fields.) Also, the routing switch applies Option 82 functionality only to client request packets being **routed** to a DHCP server. DHCP relay with Option 82 does not apply to **switched** (non-routed) client requests.

For information on configuring policies on a server running DHCP Option 82, see the documentation provided for that application.

Figure 7: *Example of a DHCP Option 82 application*


Relay Agent "1" (Routing Switch) with DHCP Option 82 Enabled
VLAN 10 10.10.10.1
VLAN 20 10.10.20.1
10.10.20.2
10.10.30.1
DHCP Option 82 Server
Switch "A" 10.10.10.2
Switch "B" 10.10.20.3
Relay Agent "2" (Routing Switch) without DHCP Option 82 Enabled
Client 1
Client 2
Client 3
Client 4
Client 5
Client 6
Policy Boundaries
Subnets 10 and 20 in relay agent "1" form policy boundaries that can be defined by the IP address of the subnet on which the client request is received.

General DHCP Option 82 requirements and operation

Requirements

DHCP Option 82 operation is configured at the global config level and requires the following:

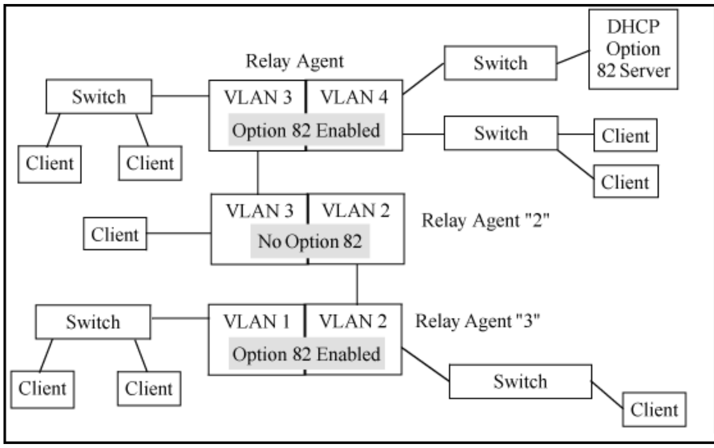
- IP routing enabled on the switch
- DHCP-relay option 82 enabled (global command level)
- Routing switch access to an Option 82 DHCP server on a different subnet than the clients requesting DHCP Option 82 support
- One IP helper address configured on each VLAN supporting DHCP clients

General DHCP-relay operation with Option 82

Typically, the first (primary) Option 82 relay agent to receive a client's DHCP request packet appends an Option 82 field to the packet and forwards it toward the DHCP server identified by the IP helper address configured on the VLAN in which the client packet was received. Other, upstream relay agents used to forward the packet may append their own Option 82 fields, replace the Option 82 fields they find in the packet, forward the packet without adding another field, or drop the packet. (Intermediate next-hop routing switches without Option 82 capability can be used to forward—route—client request packets with Option 82 fields.) Response packets from an Option 82 server are routed back to the primary relay agent (routing switch) and include an IP addressing assignment for the requesting client and an exact copy of the Option 82 data the server received with the client request. The relay agent strips off the Option 82 data and forwards the response packet out the port indicated in the response as the

Circuit ID (client access port.) Under certain validation conditions described later in this section, a relay agent detecting invalid Option 82 data in a response packet may drop the packet.

Figure 8: *Example of DHCP Option 82 Operation in a Network with a Non-Compliant Relay Agent*



Relay Agent 1 adds an Option 82 field to a client request, and then forwards the request toward the server. This includes any client requests received from Relay Agent 2 without an Option 82 field.

Note: DHCP Option 82 does not operate with clients on VLAN 4 because DHCP requests from these clients are not routed.

Relay Agent 2 does not add an Option 82 field to client requests before forwarding the requests. However, any client requests received from Relay Agent 3 will be forwarded with the Option 82 fields that were added by Relay Agent 3.

Relay Agent 3 adds an Option 82 field to a client request and then forwards the request.

Option 82 field content

The remote ID and circuit ID subfields comprise the Option 82 field a relay agent appends to client requests. A DHCP server configured to apply a different IP addressing policy to different areas of a network uses the values in these subfields to determine which DHCP policy to apply to a given client request.

Remote ID

This configurable subfield identifies a policy area that comprises either the routing switch as a whole (by using the routing switch MAC address) or an individual VLAN configured on the routing switch (by using the IP address of the VLAN receiving the client request.)

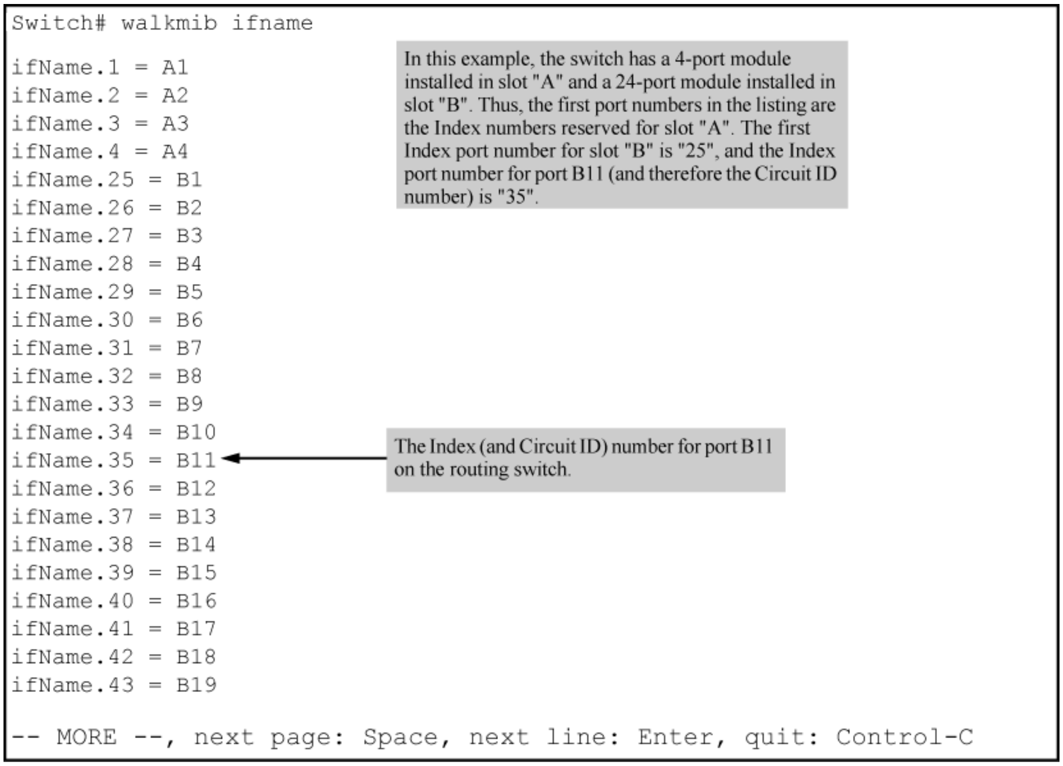
- Use the IP address option if the server will apply different IP addressing policies to DHCP client requests from ports in different VLANs on the same routing switch.
- Use the management VLAN option if a management VLAN is configured and you want all DHCP clients on the routing switch to use the same IP address. (This is useful if you are applying the same IP addressing policy to DHCP client requests from ports in different VLANs on the same routing switch.) Configuring this option means the management VLAN's IP address appears in the remote ID subfield of all DHCP requests originating with clients connected to the routing switch, regardless of the VLAN on which the requests originate.
- Use the MAC address option if, on a given routing switch, it does not matter to the DHCP server which VLAN is the source of a client request (that is, use the MAC address option if the IP addressing policies supported by the target DHCP server do not distinguish between client requests from ports in different VLANs in the same routing switch.)

Circuit ID

This nonconfigurable subfield identifies the port number of the physical port through which the routing switch received a given DHCP client request and is necessary to identify if you want to configure an Option 82 DHCP server to use the Circuit ID to select a DHCP policy to assign to clients connected to the port. This number is the identity of the inbound port. On HPE fixed-port switches, the port number used for the circuit ID is always the same as the physical port number shown on the front of the switch. On HPE chassis switches, where a dedicated, sequential block of internal port numbers are reserved for each slot, regardless of whether a slot is occupied, the circuit ID for a given port is the sequential index number for that port position in the slot. (To view the index number assignments for ports in the routing switch, use the `walkmib ifname` command.)

Using `walkmib` to determine the circuit ID for a port on an HPE chassis

For example, the circuit ID for port B11 on an HPE switch is "35”, as shown in the following example.



```
Switch# walkmib ifname

ifName.1 = A1
ifName.2 = A2
ifName.3 = A3
ifName.4 = A4
ifName.25 = B1
ifName.26 = B2
ifName.27 = B3
ifName.28 = B4
ifName.29 = B5
ifName.30 = B6
ifName.31 = B7
ifName.32 = B8
ifName.33 = B9
ifName.34 = B10
ifName.35 = B11
ifName.36 = B12
ifName.37 = B13
ifName.38 = B14
ifName.39 = B15
ifName.40 = B16
ifName.41 = B17
ifName.42 = B18
ifName.43 = B19

-- MORE --, next page: Space, next line: Enter, quit: Control-C
```

In this example, the switch has a 4-port module installed in slot "A" and a 24-port module installed in slot "B". Thus, the first port numbers in the listing are the Index numbers reserved for slot "A". The first Index port number for slot "B" is "25", and the Index port number for port B11 (and therefore the Circuit ID number) is "35".

The Index (and Circuit ID) number for port B11 on the routing switch.

For example, suppose you want port 10 on a given relay agent to support no more than five DHCP clients simultaneously. You can configure the server to allow only five IP addressing assignments at any one time for the circuit ID (port) and remote ID (MAC address) corresponding to port 10 on the selected relay agent.

Similarly, if you want to define specific ranges of addresses for clients on different ports in the same VLAN, you can configure the server with the range of IP addresses allowed for each circuit ID (port) associated with the remote ID (IP address) for the selected VLAN.

Forwarding policies

DHCP Option 82 on HPE switches offers four forwarding policies, with an optional validation of server responses for three of the policy types (`append`, `replace`, or `drop`.)

Configuration options for managing DHCP client request packets:

Option 82 configuration	DHCP client request packet inbound to the routing switch	
	Packet has no Option 82 field	Packet includes an Option 82 field
`Append`	Append an Option 82 field	`Append` allows the most detail in defining DHCP policy boundaries. For example, where the path from a client to the DHCP Option 82 server includes multiple relay agents with Option 82 capability, each relay agent can define a DHCP policy boundary and append its own Option 82 field to the client request packet. The server can then determine in detail the agent hops the packet took, and can be configured with a policy appropriate for any policy boundary on the path. NOTE In networks with multiple relay agents between a client and an Option 82 server, `append` can be used only if the server supports multiple Option 82 fields in a client request. If the server supports only one Option 82 field in a request, consider using the `keep` option.
`Keep`	Append an Option 82 field	If the relay agent receives a client request that already has one or more Option 82 fields, `keep` causes the relay agent to retain such fields and forward the request without adding another Option 82 field. But if the incoming client request does not already have any Option 82 fields, the relay agent appends an Option 82 field before forwarding the request. Some applications for `keep` include: • The DHCP server does not support multiple Option 82 packets in a client request, and there are multiple Option 82 relay agents in the path to the server. • The unusual case where DHCP clients in the network add their own Option 82 fields to their request packets, and you do not want any additional fields added by relay agents. This policy does not include the `validate` option (described in the next section) and allows forwarding of all server response packets arriving inbound on the routing switch (except those without a primary relay agent identifier.)

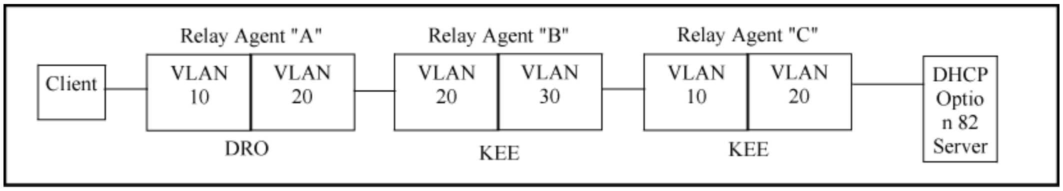
Table Continued

Option 82 configuration	DHCP client request packet inbound to the routing switch	
	Packet has no Option 82 field	Packet includes an Option 82 field
`Replace`	Append an Option 82 field	`Replace` replaces any existing Option 82 fields from downstream relay agents (and/or the originating client) with an Option 82 field for the current relay agent. Some applications for `replace` include: • The relay agent is located at a point in the network that is a DHCP policy boundary, and you want to replace any Option 82 fields appended by down-stream devices with an Option 82 field from the relay agent at the boundary. (This eliminates downstream Option 82 fields you do not want the server to use when determining which IP addressing policy to apply to a client request.) • In applications where the routing switch is the primary relay agent for clients that may append their own Option 82 field, you can use `replace` to delete these fields if you do not want them included in client requests reaching the server.
`Drop`	Append an Option 82 field	`Drop` causes the routing switch to drop an inbound client request with an Option 82 field already appended. If no Option 82 fields are present, `drop` causes the routing switch to add an Option 82 field and forward the request. As a general guideline, configure `drop` on relay agents at the edge of a network, where an inbound client request with an appended Option 82 field may be unauthorized, a security risk, or for some other reason, should not be allowed.

Multiple Option 82 relay agents in a client request path

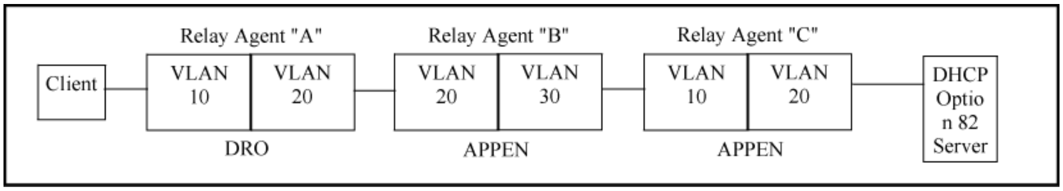
Where the client is one router hop away from the DHCP server, only the Option 82 field from the first (and only) relay agent is used to determine the policy boundary for the server response. Where there are multiple Option 82 router hops between the client and the server, you can use different configuration options on different relay agents to achieve the results you want. This includes configuring the relay agents so that the client request arrives at the server with either one Option 82 field or multiple fields. (Using multiple Option 82 fields assumes that the server supports multiple fields and is configured to assign IP addressing policies based on the content of multiple fields.)

Figure 9: *Example configured to allow only the primary relay agent to contribute an Option 82 field*



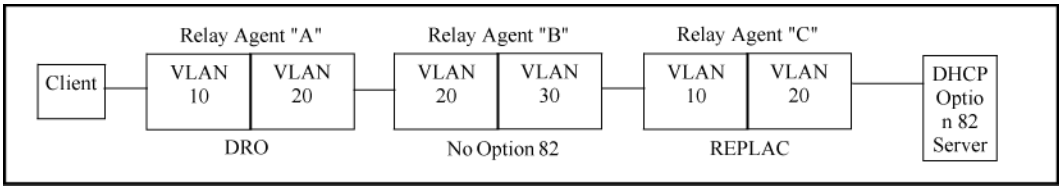
The above combination allows for detection and dropping of client requests with spurious Option 82 fields. If none are found, the drop policy on the first relay agent adds an Option 82 field, which is then kept unchanged over the next two relay agent hops ("B" and "C".) The server can then enforce an IP addressing policy based on the Option 82 field generated by the edge relay agent ("A".) In this example, the DHCP policy boundary is at relay agent 1.

Figure 10: *Example configured to allow multiple relay agents to contribute an Option 82 field*



This is an enhancement of the previous example. In this case, each hop for an accepted client request adds a new Option 82 field to the request. A DHCP server capable of using multiple Option 82 fields can be configured to use this approach to keep a more detailed control over leased IP addresses. In this example, the primary DHCP policy boundary is at relay agent "A," but more global policy boundaries can exist at relay agents "B" and "C."

Figure 11: *Example allowing only an upstream relay agent to contribute an Option 82 field*



Like the first example, above, this configuration drops client requests with spurious Option 82 fields from clients on the edge relay agent. However, in this case, only the Option 82 field from the last relay agent is retained for use by the DHCP server. In this case the DHCP policy boundary is at relay agent "C." In the previous two examples the boundary was with relay "A."

Validation of server response packets

A valid Option 82 server response to a client request packet includes a copy of the Option 82 fields the server received with the request. With validation disabled, most variations of Option 82 information are allowed, and the corresponding server response packets are forwarded.

Server response validation is an option you can specify when configuring Option 82 DHCP for `append`, `replace`, or `drop` operation. See **Forwarding policies** on page 55. Enabling validation on the routing switch can enhance protection against DHCP server responses that are either from untrusted sources or are carrying invalid Option 82 information.

With validation enabled, the relay agent applies stricter rules to variations in the Option 82 fields of incoming server responses to determine whether to forward the response to a downstream device or to drop the response due to invalid (or missing) Option 82 information. The following table describes relay agent management of DHCP server responses with optional validation enabled and disabled

Table 5: *Relay agent management of DHCP server response packets.*

Response packet content	Option 82 configuration	Validation enabled on the relay agent	Validation disabled (the default)
Valid DHCP server response packet without an Option 82 field.	append , replace, or drop[1]	Drop the server response packet.	Forward server response packet to a downstream device.
	keep[2]	Forward server response packet to a downstream device.	Forward server response packet to a downstream device.
The server response packet carries data indicating a given routing switch is the primary relay agent for the original client request, but the associated Option 82 field in the response contains a remote ID and circuit ID combination that did not originate with the given relay agent.	append	Drop the server response packet.	Forward server response packet to a downstream device.
	replace or drop[1]	Drop the server response packet.	Drop the server response packet.

Table Continued

Response packet content	Option 82 configuration	Validation enabled on the relay agent	Validation disabled (the default)
	`keep`[2]	Forward server response packet to a downstream device.	Forward server response packet to a downstream device.
The server response packet carries data indicating a given routing switch is the primary relay agent for the original client request, but the associated Option 82 field in the response contains a **Remote ID** that did not originate with the relay agent.	`append`	Drop the server response packet.	Forward server response packet to a downstream device.
	`replace` or `drop`[1]	Drop the server response packet.	Drop the server response packet.
	`keep`[2]	Forward server response packet to a downstream device.	Forward server response packet to a downstream device.
All other server response packets [3]	`append` , `keep`[2], `replace`, or `drop`[1]	Forward server response packet to a downstream device.	Forward server response packet to a downstream device.

[1] Drop is the recommended choice because it protects against an unauthorized client inserting its own Option 82 field for an incoming request.

[2] A routing switch with DHCP Option 82 enabled with the keep option forwards all DHCP server response packets except those that are not valid for either Option 82 DHCP operation (compliant with RFC 3046) or DHCP operation without Option 82 support (compliant with RFC 2131.)

[3] A routing switch with DHCP Option 82 enabled drops an inbound server response packet if the packet does not have any device identified as the primary relay agent (giaddr=null; see RFC 2131.)

Multinetted VLANs

On a multinetted VLAN, each interface can form an Option 82 policy boundary within that VLAN if the routing switch is configured to use IP for the remote ID suboption. That is, if the routing switch is configured with IP as the remote ID option and a DHCP client request packet is received on a multinetted VLAN, the IP address used in the Option 82 field will identify the subnet on which the packet was received instead of the IP address for the VLAN. This enables an Option 82 DHCP server to support more narrowly defined DHCP policy boundaries instead of defining the boundaries at the VLAN or whole routing switch levels. If the MAC address option (the default) is configured instead, the routing switch MAC address will be used regardless of which subnet was the source of the client request. (The MAC address is the same for all VLANs configured on the routing switch.)

All request packets from DHCP clients in the different subnets in the VLAN must be able to reach any DHCP server identified by the IP helper addresses configured on that VLAN.

Chapter 5
Websites

Networking Websites

Hewlett Packard Enterprise Networking Information Library

www.hpe.com/networking/resourcefinder

Hewlett Packard Enterprise Networking Software

www.hpe.com/networking/software

Hewlett Packard Enterprise Networking website

www.hpe.com/info/networking

Hewlett Packard Enterprise My Networking website

www.hpe.com/networking/support

Hewlett Packard Enterprise My Networking Portal

www.hpe.com/networking/mynetworking

Hewlett Packard Enterprise Networking Warranty

www.hpe.com/networking/warranty

General websites

Hewlett Packard Enterprise Information Library

www.hpe.com/info/EIL

For additional websites, see **Support and other resources**.

Accessing Hewlett Packard Enterprise Support

- For live assistance, go to the Contact Hewlett Packard Enterprise Worldwide website:

  http://www.hpe.com/assistance
- To access documentation and support services, go to the Hewlett Packard Enterprise Support Center website:

  http://www.hpe.com/support/hpesc

Information to collect

- Technical support registration number (if applicable)
- Product name, model or version, and serial number
- Operating system name and version
- Firmware version
- Error messages
- Product-specific reports and logs
- Add-on products or components
- Third-party products or components

Accessing updates

- Some software products provide a mechanism for accessing software updates through the product interface. Review your product documentation to identify the recommended software update method.
- To download product updates:

  Hewlett Packard Enterprise Support Center

    www.hpe.com/support/hpesc

  Hewlett Packard Enterprise Support Center: Software downloads

    www.hpe.com/support/downloads

  Software Depot

    www.hpe.com/support/softwaredepot
- To subscribe to eNewsletters and alerts:

  www.hpe.com/support/e-updates
- To view and update your entitlements, and to link your contracts and warranties with your profile, go to the Hewlett Packard Enterprise Support Center **More Information on Access to Support Materials** page:

  www.hpe.com/support/AccessToSupportMaterials

> ⓘ Access to some updates might require product entitlement when accessed through the Hewlett Packard Enterprise Support Center. You must have an HPE Passport set up with relevant entitlements.

Customer self repair

Hewlett Packard Enterprise customer self repair (CSR) programs allow you to repair your product. If a CSR part needs to be replaced, it will be shipped directly to you so that you can install it at your convenience. Some parts do not qualify for CSR. Your Hewlett Packard Enterprise authorized service provider will determine whether a repair can be accomplished by CSR.

For more information about CSR, contact your local service provider or go to the CSR website:

http://www.hpe.com/support/selfrepair

Remote support

Remote support is available with supported devices as part of your warranty or contractual support agreement. It provides intelligent event diagnosis, and automatic, secure submission of hardware event notifications to Hewlett Packard Enterprise, which will initiate a fast and accurate resolution based on your product's service level. Hewlett Packard Enterprise strongly recommends that you register your device for remote support.

If your product includes additional remote support details, use search to locate that information.

Remote support and Proactive Care information

HPE Get Connected

www.hpe.com/services/getconnected

HPE Proactive Care services

www.hpe.com/services/proactivecare

HPE Proactive Care service: Supported products list

www.hpe.com/services/proactivecaresupportedproducts

HPE Proactive Care advanced service: Supported products list

www.hpe.com/services/proactivecareadvancedsupportedproducts

Proactive Care customer information

Proactive Care central

www.hpe.com/services/proactivecarecentral

Proactive Care service activation

www.hpe.com/services/proactivecarecentralgetstarted

Warranty information

To view the warranty for your product or to view the *Safety and Compliance Information for Server, Storage, Power, Networking, and Rack Products* reference document, go to the Enterprise Safety and Compliance website:

www.hpe.com/support/Safety-Compliance-EnterpriseProducts

Additional warranty information

HPE ProLiant and x86 Servers and Options

www.hpe.com/support/ProLiantServers-Warranties

HPE Enterprise Servers

www.hpe.com/support/EnterpriseServers-Warranties

HPE Storage Products

www.hpe.com/support/Storage-Warranties

HPE Networking Products

www.hpe.com/support/Networking-Warranties

Regulatory information

To view the regulatory information for your product, view the *Safety and Compliance Information for Server, Storage, Power, Networking, and Rack Products*, available at the Hewlett Packard Enterprise Support Center:

www.hpe.com/support/Safety-Compliance-EnterpriseProducts

Additional regulatory information

Hewlett Packard Enterprise is committed to providing our customers with information about the chemical substances in our products as needed to comply with legal requirements such as REACH (Regulation EC No 1907/2006 of the European Parliament and the Council). A chemical information report for this product can be found at:

www.hpe.com/info/reach

For Hewlett Packard Enterprise product environmental and safety information and compliance data, including RoHS and REACH, see:

www.hpe.com/info/ecodata

For Hewlett Packard Enterprise environmental information, including company programs, product recycling, and energy efficiency, see:

www.hpe.com/info/environment

Documentation feedback

Hewlett Packard Enterprise is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback (**docsfeedback@hpe.com**). When submitting your feedback, include the document title, part number, edition, and publication date located on the front cover of the document. For online help content, include the product name, product version, help edition, and publication date located on the legal notices page.

Overview

The HPE mDNS Gateway and Google Chromecast solution adds support for Apple’s Bonjour and Google’s Chromecast discovery from a HPE switch. The solution uses mDNS protocol for discovery and is responsible for handling mDNS packets.

Bonjour

HPE’s mDNS Gateway solution supports Apple’s Bonjour protocol to the switch.

Bonjour is Apple’s implementation of a suite of zero-configuration networking protocols and is supported by both Mac OS X devices (such as laptops and desktops), and Apple iOS devices (such as iPhones and iPads).

Bonjour’s zero-configuration network services benefits include:

- No longer having to assign IP addresses or host names to access network services on Mac OS X and Apple iOS devices
- Applications can leverage Bonjour to automatically detect required services.
- Interacts with other applications to allow for automatic connection of devices.
- Communication and data exchange is possible without user configuration.

Google’s Chromecast

Chromecast is a digital media player developed by Google. The device is a HDMI dongle that plays audio and video content on a high-definition screen by directly streaming it via Wi-Fi from the Internet or a local network. The media is selected, by users, to play on devices by enabling Chromecast mobile and web applications. Casting a tab for sites that are not Google Cast-enabled. mirrors most Google Chrome browser content running on the device (MAC OSX and Windows).

Chromecast uses a simple multicast protocol for discovery and launch. This protocol enables users to mirror their devices on a second screen.

HPE mDNS protocol

HPE supports mDNS protocol implemented as a server. mDNS is the primary method of discovering a Chromecast that supports the v2 API. While SSDP/DIAL support is still present and used by some applications (such as “You Tube”), existing applications have to migrate to the new SDK using the new protocol.

mDNS Gateway

The mDNS gateway, running on a switch, will listen for Bonjour responses and Bonjour queries and forward them to different subnets. Its main function is to forward Bonjour traffic by retransmitting the traffic between reflection enabled VLANs. The switches are configured interfaces in the VLANs for which they are performing packet reflection.

NOTE

The mDNS gateway in a switch acts as an application layer gateway between subnets. An IP interface is required on each of the network that it is reflecting between.

Service filtering

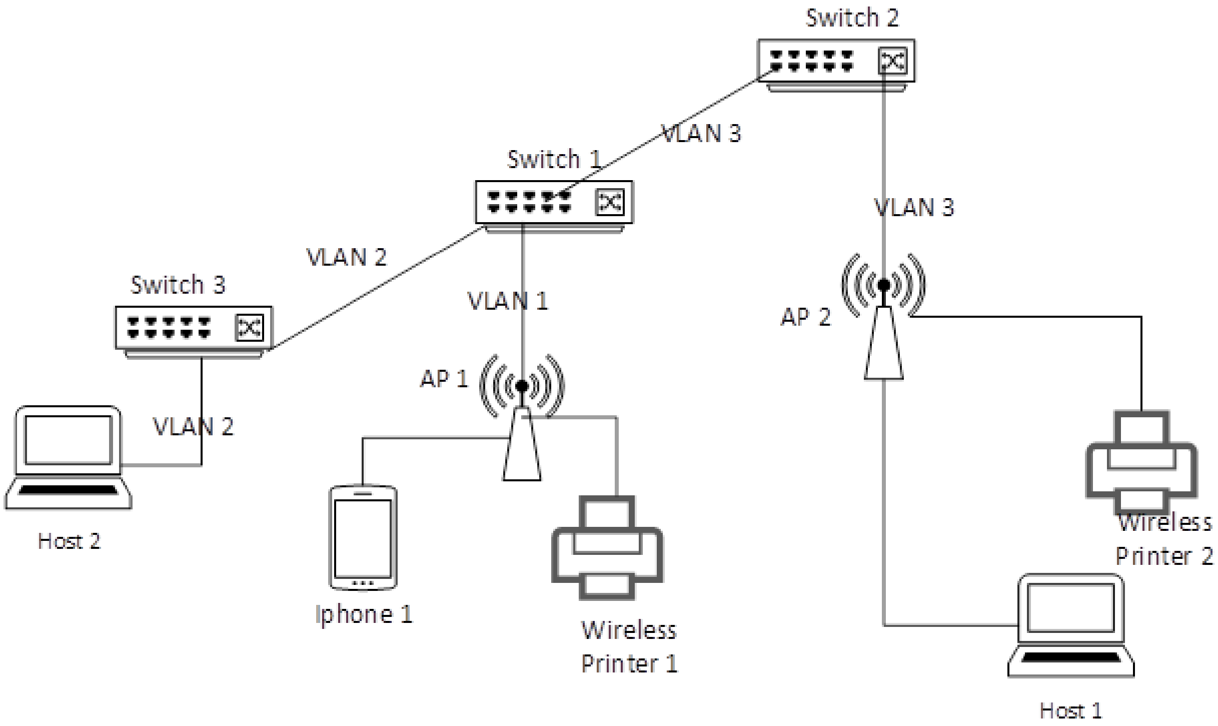
The mDNS profiles feature is responsible for applying filter profiles to mDNS resource records in mDNS response/query packets. The mDNS response/query can be filtered to give better control of the services. Service filtering allows network administrators to manipulate both the responses sent to and coming from clients in order to allow or deny mDNS services. This mechanism prevents clients from being aware of both specified services and announce specific services. These filters can be outbound from the switch to clients or inbound from clients to the switch. Profiles can be applied per-VLAN.

There is a global default which allows or denies traffic that does not match any rule. After a match is found other filter rules are ignored.

NOTE

Service filtering cannot block the connection between devices. For example, if the client knows the remote device's IP address, they can still establish a connection without utilizing the mDNS protocol. Service filtering functions to keep names and addresses out services out of mDNS responses.

Figure 12: *mDNS query and response assessment*



- Switch 1 — Reflection enabled on VLAN 2 and VLAN 3
- Global Filters — set to permit both inbound and outbound mDNS traffic on Switch 1, 2 and 3.
- Specific Filter — Switch 1 – VLAN 3 – Deny –outbound – service type – wireless printer.
- Specific Filter — Switch 1 – VLAN 2 – Permit – inbound – instance name – Host 2.

Wireless printer service process

Process overview of service for a wireless printer:

Procedure

1. Wireless Printer 1 sends an mDNS response advertising printer service in Switch 1 on VLAN 1.
2. Switch 1 has no inbound filter in VLAN 1. The global filter set to **permit all**.
3. Switch 1 checks the outbound filter in VLAN 1. As there is no specific outbound filter, the global status is **permit all**. It will flood the packet in VLAN 1 except the source port.
4. iPhone 1 in VLAN 1 receives the service announcement.
5. Switch 1 checks the reflection status. Reflection is enabled on VLAN 2 and 3.
6. Switch 1 checks the outbound filter in VLAN 2. As there is no specific outbound filter, it will forward the service announcement in VLAN 2.
7. Default action **permit all**.
8. Switch 1 checks the outbound filter in VLAN 3. The outbound filter is set to **deny wireless printer** therefore the packet will not be forwarded to VLAN 3.
9. Switch 3 receives the service advertisement in VLAN 2. It will flood the packet in VLAN 2 except the source port.
10. Host 2 in Switch 3 receives the service announcement.

Wireless Printer advertising printer service

The following procedure depicts an advertising service process for a wireless printer in the form of an example.

Procedure

1. Wireless Printer 2 sends an mDNS response advertising printer service in VLAN 3.
2. Switch 2 does not have any inbound filter in VLAN 3, so it receives the wireless printer service announcement.
3. Switch 2 checks the outbound filter in VLAN 3. There is no specific outbound filter on VLAN 3, so it floods the service announcement in VLAN 3 (except at the source port.)
4. Switch 2 checks the reflection status. Since switch 2 is not enabled, switch 2 does not forward.
5. As there is no inbound filter in VLAN 3 of switch 1, it receives the service announcement on VLAN 3. When switch 1 checks the outbound filter in VLAN 3, there is `deny operation for service type wireless printer` error message. Therefore switch 1 will not flood the packet in VLAN 3.
6. Switch 1 checks the reflection status. The reflection is enabled on VLAN 2 and 3 however VLAN 3 is incoming so the reflection will not function. In VLAN 2 it checks the outbound filter. There is no outbound filter in VLAN 2 so switch 1 forwards the service announcement in VLAN 2.
7. Switch 3 does not have any inbound filter therefore. It receives service announcements in VLAN 2.
8. Switch 2 checks the outbound filter in VLAN 2. As there is no specific outbound filter, the global action is to `permit all` so switch 2 floods the packet in VLAN 2 (except the source port.)
9. Host 2 receives the switch 2 print service announcement.

Host 2 queries for printers

The following procedure depicts a service process for mDNS queries for a wireless printer in the form of an example.

Procedure

1. Host 2 sends an mDNS query for printers.
2. There is no inbound filter in VLAN 2 of Switch 3 therefore it receives the query.
3. Switch 3 checks the outbound filter in VLAN 2. As there is no specific outbound filter the default action is **permit all**.
4. Switch 3 floods the query in VLAN 2 (except the source port.)
5. Switch 1 receives the query and check the inbound filters. Permit for the instance name, Host 2, allows the packet on VLAN 2.
6. Switch 1 checks the outbound filter for VLAN 2. As there is no specific filter and global filter is **permit all**, it will flood the packet in VLAN 2 (except the source port.)

7. Switch 1 checks the reflection status. Reflection is enabled on VLAN 2 and VLAN 3. Since VLAN 2 is an incoming VLAN, it will not pass the reflection on VLAN 2.
8. Switch 1 checks the outbound filters on VLAN 3. There is no rule to deny Host two query and the global filter is set to **permit all** so it will forward the packet to VLAN 3.
9. Switch 2 receives the service and checks for any inbound and outbound filters in VLAN 3.
10. There is no specific inbound and outbound filter in VLAN 3 therefore it will flood the query in VLAN 3 (except the source port.)
11. Reflection is not enabled in Switch 2 therefore it will not pass any further reflection.
12. Wireless printer 2 responses to the query and switch 2 does not have any inbound and outbound filters therefore it will flood the response to VLAN 3 (except the source port.)
13. Switch 1 receives the packet as there are no inbound filters in VLAN 3. VLAN 3 has an outbound filter set to deny wireless printer service. The service will not flood VLAN 3.
14. Switch 1 checks the reflection status which is enabled in VLAN 2 and 3. Since the incoming VLAN is 3, the packet will not forward to VLAN 3.
15. Switch 1 checks the outbound filter in VLAN 2. As there is no specific filter, it will forward the response to VLAN 2.
16. Switch 3 receives the response on VLAN 2 as there is no inbound filter to deny this service.
17. Switch 3 does not have any outbound filters in VLAN 2, so it will flood the response in VLAN 2 (except the source port.)
18. Host 2 receives the Wireless Printer 2 service response.

iPhone 1 queries for printers

The following depicts a service process for iPhone queries for a wireless printer in the form of an example.

1. iPhone 1 sends an mDNS query for printers in switch 1 on VLAN 1.
2. Switch 1 checks the inbound filter in VLAN 1. As there is no specific filters, it receives the query.
3. Switch 1 checks the outbound filter in VLAN 1. As there is no specific filter therefore it flood the packet in VLAN 1 (except the source port.)
4. Switch 1 checks the reflection status. The reflection is enabled on VLAN 2 and 3.
5. Switch 1 checks the outbound filters on VLAN 2 and 3. In VLAN 3 the outbound filter is set to deny wireless printer therefore it will not reflect the packet to VLAN 3. There is no specific outbound filter in VLAN 2 so it will forward the packet to VLAN 2.
6. In switch 1, wireless printer 1 receives the iPhone 1 query and sends a response. Switch 1 checks the inbound filter, outbound filter and floods the response to VLAN 1 (except the source port.)
7. Switch 3 receives the iPhone 1 query and floods the packet in VLAN 2. As there is no specific inbound and outbound filters in switch 3, there is no associated printers in switch 3. There will not be any further response.

Limitations of the mDNS gateware and Chromecast

The following are limitations of the mDNS gateway and Chromecast features:

- IPv6 is not supported.
- In distributed environment enable gateway in one switch to avoid loops.
- Chromecast v1 (DIAL over SSDP) is not supported.
- Custom filters are not supported.For example:

```
rule <name> service *tv*
rule <name> instance *ipad*
```

- mDNS commands are not available from the web and the menu.

- If the user configures both permit and deny for same service/instance and assign that to same VLAN then it is not valid configuration. System will not behave properly.
- If the user has detected the Chromecast device via a permit profile VLAN and is doing a transition to deny profile, VLAN will need to clean the cache memory. Otherwise the system might get connected with already discovered device. It will not try to discover it again. This is an expected behavior.

Enabling mDNS feature

This command is supported In the config context with manager permissions.

Syntax

```
mdns enable
no mdns enable
```

Description

Enable or disables mDNS gateway support on switch.

The default value is disabled.

Create mDNS reflection

This command is supported in the config context.

Syntax

```
mdns gateway vlan VLAN-LIST
no mdns gateway vlan VLAN-LIST
```

Description

Configures the VLAN reflection for mDNS traffic. If the VLAN is not set, the mDNS traffic will not flood to different subnets, it will only flood to the incoming VLAN.

Options

gateway

Enable VLAN for mDNS gateway.

Create or delete a mDNS profile

This command will be supported on config context in manager mode. This is a context command. Separate context is created for this.

Syntax

```
mdns profile PROFILE-NAME
no mdns profile PROFILE-NAME
```

Description

Create or delete an mDNS profile.

Set rules for mDNS profile

This command is supported in the mDNS profile context.

Syntax

```
rule rule-id instance | service NAME action permit | deny
no rule rule-id instance | service NAME action permit | deny
```

Description

Sets rules for each mDNS profile. You can configure specific rule to permit or deny the mDNS packet.

Options

rule

Create or delete a rule for mDNS profile.

instance

Instance name of the client.

service

Service name of the client.

action

Specify the action for mDNS traffic.

permit

Permit the packet upon successful match.

deny

Deny the packet upon successful match.

Set the specific mDNS profile for VLAN

This command is supported in the mDNS profile context.

Syntax

```
vlan VLAN-LIST
no vlan VLAN-LIST
```

Description

Used to set the mDNS profile for a particular VLAN. Based on the rule, the filter permits or denies traffic.

Options

VLAN-LIST

Set the global mDNS profile

This command is supported in the configure context in manager mode.

Syntax

```
mdns default filter in | out action permit | deny
```

Description

Used to set the default action for all VLANs. If there is no specific rule for a particular VLAN, the default action will be applied. By default, the global action is set to deny for both inbound and outbound traffic.

Options

filter

Specify the mDNS filter on this VLAN.

in

Match inbound traffic.

out

Match outbound traffic.

default

Set the action of the mDNS default filter

Show mdns

Syntax

```
show mdns
```

Description

Display the status of the mDNS feature.

Options

mDNS

Display the status of the mDNS feature

Example show mDNS

```
show mDNS
mDNS Configuration
mDNS: Enabled
```

Show mDNS gateway

Syntax

```
show mdns gateway
```

Description

Display the reflection VLAN list of the mDNS gateway.

Options

gateway

mDNS gateway

Example

```
show mDNS gateway

mDNS Gateway Configuration
Gateway VLAN List: 1-10,12
```

Show mDNS profile configuration

Syntax

```
show mdns profile
```

Description

Display mDNS profile configuration information.

Options

profile

mDNS profile information

Example

```
mDNS profile configuration
   Profile Name: Students
   VLANs       : 1-3,25

   Rules:
   ID  Instance          Service              Action
   --- ----------------- -------------------- ------
   1   ANY               AppleTV              Deny
   2   MyComputer        ANY                  Permit

   Profile Name: Professors
   VLANs       : 3-6,10

   Rules:
   ID  Instance          Service              Action
   --- ----------------- -------------------- ------
   1   ANY               AppleTV              Deny
   2   MyComputer        ANY                  Permit
```

Show mDNS profile name

Syntax

```
show mdns profile PROFILE-NAME
```

Description

Display mDNS profile name information.

Options

PROFILE-NAME

Specify the profile name.

Example

```
mDNS profile configuration
   Profile Name: Students
   VLANs       : 1-3,25

   Rules:
   ID  Instance          Service              Action
   --- ----------------- -------------------- ------
   1   ANY                  AppleTV                    Deny
   2   MyComputer           ANY                        Permit
```

Show mDNS

```
mDNS enable
mDNS gateway vlan 1-2
mDNS profile "abcd"
   rule 1 instance Host1 action permit
   rule 2 service AppleTv action deny
   vlan 1-2
   exit

vlan 1
   name "DEFAULT_VLAN"
   untagged 1-24
   ip address dhcp-bootp
   exit

vlan 2
   name "VLAN2"
   untagged 2
   ip address 10.1.1.1 255.255.255.0
   exit
```

Debug mDNS

Syntax

```
debug mdns
```

Description

Enable or disable mDNS debug logging.

Usage

```
debug mdns
no debug mdns
```

Validation rules

Rule	Error/Warning/Prompt
Profile name exceeds max length	The profile name exceeds the maximum length of %d.
Profile name already exist. It should be unique.	The profile name already exists.
Profile name contains invalid characters	The profile name contains invalid characters.
Trying to delete mDNS profile which does not exist.	The profile is not found.
Trying to add Profile beyond the max limit.	Cannot add the profile. It reached the maximum limit.

Table Continued

Rule	Error/Warning/Prompt
Instance name exceeds	The instance name exceeds the maximum length %d.
Instance name contains invalid characters	The instance name contains invalid characters.
Service name exceeds max length	The service name exceeds the maximum length of %d.
Service name contains invalid characters	The rules for Service Names [RFC6335] state that they may be no more than 15 characters long, consisting of only letters, digits, and hyphens, must begin and end with a letter or digit, must not contain consecutive hyphens, and must contain at least one letter.
Trying to add rule beyond the max limit.	Cannot add rule. It reached the maximum limit.
Trying to add gateway vlan beyond the limit.	Maximum number of mDNS gateway VLANs is %s.
Trying to add profile vlan beyond the limit.	Maximum number of mDNS profile VLANs is %s.
Trying to add rule which is already present.	The rule is already configured with this ID.
Trying to delete rule which is not found.	Rule ID %s is not found.
Trying to show mDNS profile which does not exist.	The profile is not found.
Gateway vlan cannot be configured as secondary vlan	mDNS gateway VLAN cannot be configured on secondary VLAN. It should be configured on the primary VLAN
Profile vlan cannot be configured as secondary vlan	mDNS profile VLAN cannot be configured on secondary VLAN. It should be configured on the primary VLAN.
Secondary vlan cannot be configured as gateway vlan	Secondary VLAN cannot be configured on mDNS gateway VLAN.
Secondary vlan cannot be configured as gateway vlan	Secondary VLAN cannot be configured on mDNS profile VLAN.

RMON table

RMON event	Details
RMON_mDNS_ENABLED	Proposed Display: I 05/22/13 20:39:20 04633 mDNS: mDNS is enabled.
RMON_mDNS_DISABLED	Proposed Display: I 05/22/13 20:39:20 04633 mDNS: mDNS is disabled.
RMON_mDNS_PKT_MAX_LIMIT	Proposed Display: W 05/22/13 20:49:12 04635 mDNS: mDNS packets are dropped. It has exceeded the maximum limit of %d packets per second.