



Cisco Nexus 1000V for KVM Layer 2 Configuration Guide, Release 5x

First Published: August 01, 2014

Last Modified: November 21, 2014

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <http://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2014 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1

New and Changed Information 1

New and Changed Information 1

CHAPTER 2

Configuring MAC Address Tables 3

Information About MAC Address Tables 3

Guidelines and Limitations 4

Default Settings 4

Configuring the MAC Address Table 4

Configuring a Static MAC Address 4

Configuring the Aging Time 5

Clearing Dynamic Addresses from the MAC Address Table 6

Verifying the MAC Address Table Configuration 6

Feature History for the MAC Address Table 7

CHAPTER 3

Configuring VLANs 9

Information About VLANs 9

Guidelines and Limitations 10

Default Settings 11

Configuring a VLAN 11

Creating a VLAN 11

Configuring VLAN Characteristics 13

Verifying the Configuration 15

Feature History for VLANs 15

CHAPTER 4

Configuring Private VLANs 17

Information About Private VLANs 17

Private VLAN Ports 18

Communication Between Private VLAN Ports 20

Guidelines and Limitations	20
Default Settings	20
Configuring a Private VLAN	21
Enabling or Disabling the Private VLAN Feature Globally	21
Configuring a VLAN as a Primary VLAN	22
Configuring a VLAN as a Secondary VLAN	23
Associating the VLANs in a PVLAN	24
Configuring a Layer 2 Port Profile as a Promiscuous Trunk Port	25
Configuring a Private VLAN Promiscuous Access Port	27
Associating a Promiscuous Access Port with a Private VLAN	28
Removing a Private VLAN Configuration	29
Verifying a Private VLAN Configuration	30
Configuration Examples for Private VLANs	30
Feature History for Private VLANs	32

CHAPTER 5**Configuring IGMP Snooping 33**

Information about IGMP Snooping	33
Introduction	33
IGMPv1 and IGMPv2	34
IGMPv3	34
Prerequisites for IGMP Snooping	35
Default Settings	35
Configuring IGMP Snooping	36
Enabling or Disabling IGMP Snooping Globally for the VSM	36
Configuring IGMP Snooping on a VLAN	37
Verifying the IGMP Snooping Configuration	38
Feature History for IGMP Snooping	38



New and Changed Information

This chapter contains the following sections:

- [New and Changed Information, page 1](#)

New and Changed Information

Table 1: New and Changed Features

Content	Description	Changed in Release	Where Documented
Private VLAN Port Profiles	This feature is introduced.	5.2(1)SK3(2.1)	Configuring Private VLANs, on page 17



Configuring MAC Address Tables

This chapter contains the following sections:

- [Information About MAC Address Tables, page 3](#)
- [Guidelines and Limitations, page 4](#)
- [Default Settings, page 4](#)
- [Configuring the MAC Address Table, page 4](#)
- [Verifying the MAC Address Table Configuration, page 6](#)
- [Feature History for the MAC Address Table, page 7](#)

Information About MAC Address Tables

Layer 2 ports correlate the MAC address on a packet with the Layer 2 port information for that packet using the MAC address table. A MAC address table is built using the MAC source addresses of the frames received. When a frame is received for a MAC destination address not listed in the address table, the frame is flooded to all LAN ports of the same VLAN with the exception of the port that received the frame. When the destination station replies, the relevant MAC source addresses and port IDs are added to the address table. Subsequent frames are forwarded to a single LAN port without flooding all LAN ports.

You can configure MAC addresses, which are called static MAC addresses, to statically point to specified interfaces on the device. These static MAC addresses override any dynamically learned MAC addresses on those interfaces. You cannot configure broadcast or multicast addresses as static MAC addresses. The static MAC entries are retained across reboots if you copy the static MAC addresses configuration to the startup configuration by using the `copy running-config startup-config` command.

The address table per VEM can store up to 32,000 MAC entries. An aging timer triggers removal of addresses from the table when they remain inactive for the default time of 300 seconds. The aging timer can be configured on a global basis but not per VLAN.

You can configure the length of time an entry remains in the MAC address table, clear the table, and so forth.

Guidelines and Limitations

- The forwarding table for each VLAN in a VEM can store up to 4094 MAC addresses.
- You can configure only 1024 static MAC addresses on a single interface.

Default Settings

Table 2: Default MAC Address Aging Time

Parameters	Default
Aging time	300 seconds

Configuring the MAC Address Table

Configuring a Static MAC Address

Use this procedure to configure a MAC address to statically point to a specific interface.

Before You Begin

- You are logged in to the CLI in EXEC mode.
- You cannot configure broadcast or multicast addresses as static MAC addresses.
- Static MAC addresses override dynamically-learned MAC addresses on an interface.



Note

Be aware that the Cisco NX-OS commands may differ from those used in Cisco IOS.

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters global configuration mode.
Step 2	switch(config)# mac address-table static <i>mac_address</i> vlan <i>vlan-id</i> [drop]	Adds a static MAC address in the Layer 2 MAC address table and saves it in the running configuration.
Step 3	switch(config)# show mac address static interface [<i>type if_id</i>]	(Optional) Displays static MAC addresses.

	Command or Action	Purpose
Step 4	switch(config)# copy running-config startup-config	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

```
switch# configure terminal
switch(config)# mac address static
switch(config)# show mac address static
switch(config)#
```

Configuring the Aging Time

Use this procedure to configure the amount of time that packet source MAC addresses, and the ports on which they are learned, remain in the MAC table containing the Layer 2 information.



Note

The aging time is a global setting that cannot be configured per VLAN. Although it is a global setting, you can also configure MAC aging time in interface configuration mode or VLAN configuration mode.

Before You Begin

You are logged in to the CLI in EXEC mode.



Note

Be aware that the Cisco NX-OS commands may differ from those used in Cisco IOS.

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters global configuration mode.
Step 2	switch# mac address-table aging-time <i>seconds</i>	Specifies and saves in the running configuration the amount of time that will elapse before an entry in the Layer 2 MAC address table is discarded. Allowable entries include: <ul style="list-style-type: none"> • 120 to 918000 seconds (default is 300) • If you specify zero (0), MAC aging is disabled.

```
switch# configure terminal
switch(config)# mac address-table aging-time 600
switch(config)# show mac address-table aging-time
Vlan Aging Time
-----
```

```

101    600
100    600
1      600
switch#

```

Clearing Dynamic Addresses from the MAC Address Table

Before You Begin

You are logged in to the CLI in EXEC mode.



Note

Be aware that the Cisco NX-OS commands may differ from those used in Cisco IOS.

Procedure

	Command or Action	Purpose
Step 1	switch# clear mac address-table dynamic [vlan vlan_id]	Clears the dynamic address entries from the Layer 2 MAC address table.
Step 2	switch# show mac address-table [vlan vlan_id]	(Optional) Displays the MAC address table. Note If the switch has several modules and interfaces, you should not use the show mac address-table command. The command will take a long time to complete. Instead, we recommend that you use a more focused show command, for example, for a specific VLAN.

The following example clears the entire MAC address table of all dynamic entries:

```

switch# clear mac address-table dynamic
switch#

```

The following example clears the MAC address table of only those dynamic MAC addresses learned on VLAN 5:

```

switch# clear mac address-table dynamic vlan 5
switch#

```

Verifying the MAC Address Table Configuration

Use one of the following commands to verify the configuration:

Command	Purpose
show mac address-table	Displays the MAC address table. Note If the switch has several modules and interfaces, you should not use the show mac address-table command. The command will take a long time to complete. Instead, we recommend that you use a more focused show command, for example, for a specific module or VLAN.
show mac address-table module <i>module-number</i>	Displays the MAC address table for a specific module.
show mac address-table static	Displays information about the MAC address table static entries.
show mac address-table static inc veth	Displays the static MAC address of vEthernet interfaces in case a VEM physical port learns a dynamic MAC and the packet source is in another VEM on the same VSM.
show mac address static interface [<i>type if_id</i>]	Displays all static MAC addresses.
show mac address-table aging-time	Displays the aging time in the MAC address table.
show mac address-table count	Displays a count of MAC address entries.
show interface <i>interface_id</i> mac	Displays the MAC addresses and the burn-in MAC address for an interface.

Feature History for the MAC Address Table

Feature Name	Release	Description
MAC Address Tables	Release 5.2(1)SK1(2.1)	This feature was introduced



Configuring VLANs

This chapter contains the following sections:

- [Information About VLANs, page 9](#)
- [Guidelines and Limitations, page 10](#)
- [Default Settings, page 11](#)
- [Configuring a VLAN, page 11](#)
- [Verifying the Configuration, page 15](#)
- [Feature History for VLANs, page 15](#)

Information About VLANs

vEthernet interfaces that are assigned to specific VLANs are tagged with the VLAN when transmitted. A vEthernet interface that is not assigned to a specific VLAN, or assigned to VLAN 0, is transmitted as untagged on the physical NIC interfaces. When the VLAN is not specified, it is assumed to be 1.

The following table summarizes the actions taken on packets that are received by the Virtual Ethernet Module (VEM) based on VLAN tagging.

Table 3: VEM Action on VLAN Tagging

Port Type	Packet received	Action
Access	Tagged	The packet is dropped.
Access	Untagged	The VEM adds an access VLAN to the packet.
Trunk	Tagged	No action is taken on the packet.
Trunk	Untagged	The VEM adds a native VLAN tag to the packet.

Guidelines and Limitations

VLAN configuration has the following guidelines and limitations:

- You configure VLANs through OpenStack as a VM subnet.

You must consistently use OpenStack for all VM network and subnet configuration. If you use *both* OpenStack and the VSM to configure VM networks and subnets, the OpenStack and the VSM configurations can become out-of-sync and result in faulty or inoperable network deployments.

- In accordance with the IEEE 802.1Q standard, Cisco Nexus 1000V can use the VLANs within the range of 1-4094 (see the following table).

Table 4: Cisco Nexus 1000V VLAN Numbering

VLANs Numbers	Range	Usage
1	Normal	Cisco Nexus 1000V default. You can use this VLAN, but you cannot modify or delete it.
2–1005	Normal	You can create, use, modify, and delete these VLANs.
1006–4094	Extended	<p>You can create, name, and use these VLANs. You cannot change the following parameters:</p> <ul style="list-style-type: none"> State is always active. VLAN is always enabled. You cannot shut down these VLANs. <p>The extended system ID is always automatically enabled.</p>
3968–4047 and 4094	Internally allocated	<p>You cannot use, create, delete, or modify these VLANs. You can display these VLANs.</p> <p>Cisco Nexus 1000V allocates these 80 VLANs, plus VLAN 4094, for features, like diagnostics, that use internal VLANs for their operation.</p> <p>For information about diagnostics, see the <i>Cisco Nexus 1000V for KVM System Management Configuration Guide</i>.</p>

Default Settings

Table 5: Default VLAN Settings

Parameters	Default
VLAN assignment for all interfaces and all ports configured as switchports	VLAN 1
VLAN name	VLANxxxx where xxxx represent four numeric digits (including leading zeroes) equal to the VLAN ID number
Shut state	No shutdown
Operational state	Active
External switch tagging (EST)	Enabled
IGMP snooping	Enabled

Configuring a VLAN

Creating a VLAN

You must configure VLANs as VM subnets using the OpenStack Horizon Dashboard or the OpenStack CLI.

You must consistently use OpenStack for all VM network and subnet configuration. If you use *both* OpenStack and the VSM to configure VM networks and subnets, the OpenStack and the VSM configurations can become out-of-sync and result in faulty or inoperable network deployments.

Use this procedure to do the following:

- Create a single VLAN that does not already exist.
- Create a range of VLANs that do not already exist.
- Delete an existing VLAN.

**Note**

All interfaces and all ports configured as switchports are in VLAN 1 by default.

Before You Begin

- You are logged in to the CLI in EXEC mode.
- VLAN characteristics are configured in the VLAN configuration mode.

- You are familiar with the VLAN numbering.
- Newly-created VLANs remain unused until Layer 2 ports are assigned to them.
- When you delete a specified VLAN, the ports associated to that VLAN are shut down and no traffic flows. When you delete a specified VLAN from a trunk port, only that VLAN is shut down and traffic continues to flow on all the other VLANs through the trunk port. However, the system retains all the VLAN-to-port mapping for that VLAN, and when you reenables, or re-create, that specified VLAN, the system automatically reinstates all the original ports to that VLAN. Note that the static MAC addresses and aging time for that VLAN are not restored when the VLAN is reenables.

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters global configuration mode.
Step 2	switch(config)# show vlan	(Optional) Displays the VLANs that already exist.
Step 3	switch(config)# { no } vlan { <i>vlan-id</i> <i>vlan-range</i> }	Creates or deletes, and saves in the running configuration, a VLAN or a range of VLANs. Note If you enter a VLAN ID that is assigned to an internally allocated VLAN, the system returns an error message. From the VLAN configuration mode, you can also create and delete VLANs. If a VLAN has been defined as a system VLAN on any port profile, then you cannot delete that VLAN.
Step 4	switch(config-vlan)# show vlan id <i>vlan-id</i>	(Optional) Displays the VLAN configuration.
Step 5	switch(config-vlan)# copy running-config startup-config	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

In the following example VLAN 5 is created and you are automatically placed into the VLAN configuration mode for VLAN 5:

```
switch# configure terminal
switch(config)# vlan 5
switch(config-vlan)#
```

The following example shows the range, VLAN 15-20, being created. The VLANs in the range are activated, and you are automatically placed into VLAN configuration mode for VLANs 15-20.

**Note**

If you create a range of VLANs that includes an unusable VLAN, all VLANs in the range are created except those that are unusable; and Cisco Nexus 1000V returns a message listing the failed VLANs.

```
switch# configure terminal
switch(config)# vlan 15-20
switch(config-vlan)#
```

The following example shows VLAN 3967 being deleted, using the no form of the command:

```
switch# configure terminal
switch(config)# no vlan 3967
switch(config)#
```

The following example displays the VLAN 5 configuration:

```
switch# configure terminal
switch(config)# vlan 5
switch(config-vlan)# show vlan id 5
```

```
VLAN Name                Status    Ports
-----
5      VLAN0005                active
VLAN Type
----
5      enet
Remote SPAN VLAN
-----
Disabled

Primary  Secondary  Type          Ports
-----
n1000v(config-vlan)# copy run start
[#####] 100%
n1000v(config)#
```

Configuring VLAN Characteristics

Use this procedure to configure the following for a VLAN that has already been created:

**Note**

Commands entered in the VLAN configuration mode are immediately saved to the running configuration.

- Name the VLAN.
- The operational state (active, suspend) of the VLAN.
- The VLAN media type .
- Shut down switching on the VLAN.

Before You Begin

You are logged in to the CLI in EXEC mode.

**Note**

Some characteristics cannot be modified on some VLANs. For more information, see the VLAN numbering described in the [Guidelines and Limitations](#) section.

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters global configuration mode.
Step 2	switch(config)# vlan { <i>vlan-id</i> <i>vlan-range</i> }	Enters VLAN configuration mode for the specified VLAN. Note If the VLAN does not already exist, the system creates it and then enters the VLAN configuration mode for that VLAN.
Step 3	switch(config-vlan)# name <i>vlan-name</i>	Adds a name to the VLAN of up to 32 alphanumeric characters. <ul style="list-style-type: none"> You cannot change the name of VLAN1 nor the VLANs reserved for internal use. The default name is VLANxxxx where xxxx represent four numeric digits (including leading zeroes) equal to the VLAN ID number.
Step 4	switch(config-vlan)# state { active suspend }	Changes the operational state of the VLAN and saves it in the running configuration. Allowable entries are: <ul style="list-style-type: none"> Active (default) Suspend While the VLAN state is suspended, the ports associated with this VLAN are shut down, and that VLAN does not pass any traffic. Note You cannot suspend the state for the default VLAN or VLANs 1006 to 4094.
Step 5	switch(config-vlan)# no shutdown	Enables VLAN switching in the running configuration. Allowable entries are: <ul style="list-style-type: none"> no shutdown (default) shutdown Note You cannot shut down the default VLAN, VLAN1, or VLANs 1006 to 4094.
Step 6	switch(config-vlan)# show vlan [<i>id vlan-id</i>]	(Optional) Displays the VLAN configuration.

	Command or Action	Purpose
Step 7	switch(config-vlan)# copy running-config startup-config	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

```
n1000v# configure terminal
n1000v(config)# vlan 5
n1000v(config-vlan)# name accounting
n1000v(config-vlan)# state active
n1000v(config-vlan)# no shutdown
n1000v(config-vlan)# show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	
5	VLAN0005	active	
2166	VLAN2166	active	
2167	VLAN2167	active	
2168	VLAN2168	active	
2169	VLAN2169	active	
2170	VLAN2170	active	

Verifying the Configuration

Use one of the following commands to verify the configuration:

Command	Purpose
show running-config vlan <i>vlan-id</i>	Displays VLAN information in the running configuration.
show vlan [all-ports brief id <i>vlan-id</i> name <i>name</i> dot1q tag native]	Displays the specified VLAN information.
show vlan summary	Displays a summary of VLAN information.

Feature History for VLANs

Feature Name	Release	Description
VLANs	Release 5.2(1)SK1(2.1)	This feature was introduced



Configuring Private VLANs

This chapter contains the following sections:

- [Information About Private VLANs, page 17](#)
- [Private VLAN Ports, page 18](#)
- [Communication Between Private VLAN Ports, page 20](#)
- [Guidelines and Limitations, page 20](#)
- [Default Settings, page 20](#)
- [Configuring a Private VLAN, page 21](#)
- [Verifying a Private VLAN Configuration, page 30](#)
- [Configuration Examples for Private VLANs, page 30](#)
- [Feature History for Private VLANs, page 32](#)

Information About Private VLANs

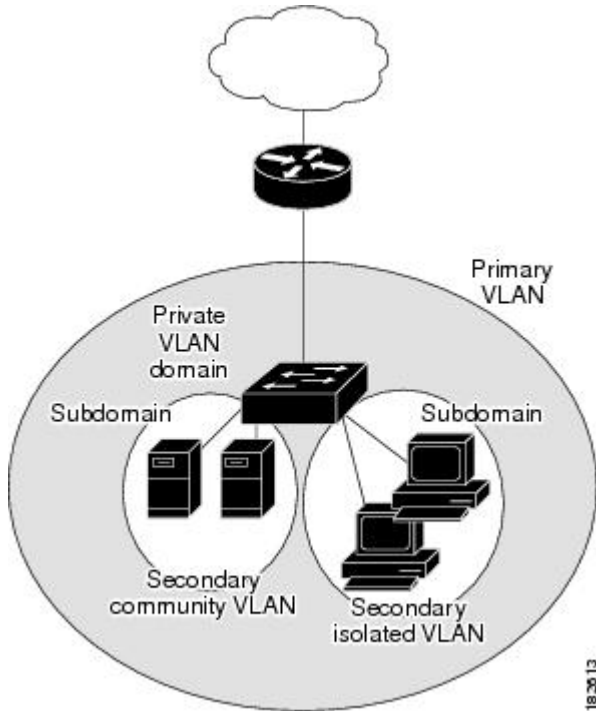
PVLANs achieve Layer 2 isolation through the use of three separate port designations, each having its own unique set of rules that regulate each connected endpoint's ability to communicate with other connected endpoints within the same private VLAN domain.

Private VLAN Domains

A PVLAN domain consists of one or more pairs of VLANs. The primary VLAN makes up the domain; and each VLAN pair makes up a subdomain. The VLANs in a pair are called the primary VLAN and the secondary

VLAN. All VLAN pairs within a private VLAN have the same primary VLAN. The secondary VLAN ID is what differentiates one subdomain from another. See the following figure.

Figure 1: Private VLAN Domain



Spanning Multiple Switches

PVLANS can span multiple switches, just like regular VLANs. Inter-switch link ports do not need to be aware of the special VLAN type and carry frames tagged with these VLANs just like they do any other frames. PVLANS ensure that traffic from an isolated port in one switch does not reach another isolated or community port in a different switch even after traversing an inter-switch link. By embedding the isolation information at the VLAN level and by transporting it with the packet, it is possible to maintain consistent behavior throughout the network. The mechanism that restricts Layer 2 communication between two isolated ports in the same switch also restricts Layer 2 communication between two isolated ports in two different switches.

Private VLAN Ports

Within a PVLAN domain, there are three separate port designations. Each port designation has its own unique set of rules that regulate the ability of one endpoint to communicate with other connected endpoints within the same private VLAN domain. The three port designations are as follows:

- promiscuous
- isolated
- community

Primary VLANs and Promiscuous Ports

The primary VLAN encompasses the entire PVLAN domain. It is a part of each subdomain and provides the Layer 3 gateway out of the VLAN. A PVLAN domain has only one primary VLAN. Every port in a PVLAN domain is a member of the primary VLAN.

A promiscuous port can talk to all other types of ports; it can talk to isolated ports as well as community ports and vice versa. Layer 3 gateways, DHCP servers, and other trusted devices that need to communicate with the customer endpoints are typically connected with a promiscuous port. A promiscuous port can be either an access port or a hybrid/trunk port according to the terminology presented in Annex D of the IEEE 802.1Q specification.

Secondary VLANs and Host Ports

Secondary VLANs provide Layer 2 isolation between ports in a PVLAN domain. A PVLAN domain can have one or more subdomains. A subdomain is made up of a VLAN pair that consists of the primary VLAN and a secondary VLAN. Because the primary VLAN is a part of every subdomain, secondary VLANs differentiate the VLAN subdomains.

To communicate to the Layer 3 interface, you must associate a secondary VLAN with at least one of the promiscuous ports in the primary VLAN. You can associate a secondary VLAN to more than one promiscuous port within the same PVLAN domain, for example, if needed for load balancing or redundancy. A secondary VLAN that is not associated with any promiscuous port cannot communicate with the Layer 3 interface.

A secondary VLAN can be one of the following types:

- **Isolated VLANs**—Isolated VLANs use isolated host ports. An isolated port cannot talk to any other port in that private VLAN domain except for promiscuous ports. If a device needs to have access only to a gateway router, it should be attached to an isolated port. An isolated port is typically an access port, but in certain applications, it can also be a hybrid or trunk port.

An isolated VLAN allows all its ports to have the same degree of segregation that could be obtained from using one separate dedicated VLAN per port. Only two VLAN identifiers are used to provide this port isolation.

**Note**

While multiple community VLANs can be in a private VLAN domain, one isolated VLAN can serve multiple customers. All endpoints that are connected to its ports are isolated at Layer 2. Service providers can assign multiple customers to the same isolated VLAN and be assured that their Layer 2 traffic cannot be sniffed by other customers that share the same isolated VLAN.

- **Community VLANs**—Community VLANs use community host ports. A community port (c1 or c2 in the above figure) is part of a group of ports. The ports within a community can communicate at Layer 2 with one another and can also talk to any promiscuous port. For example, if an ISP customer has four devices and wants them isolated from those devices of other customers but still be able to communicate among themselves, community ports should be used.

**Note**

Because trunks can support a VLAN that carries traffic between its ports, VLAN traffic can enter or leave the device through a trunk interface.

Communication Between Private VLAN Ports

The following table shows how access is permitted or denied between PVLAN port types.

Table 6: Communication Between PVLAN Ports

	Isolated	Promiscuous	Community 1	Community 2	Interswitch Link Port ¹
Isolated	Deny	Permit	Deny	Deny	Permit
Promiscuous	Permit	Permit	Permit	Permit	Permit
Community 1	Deny	Permit	Permit	Deny	Permit
Community 2	Deny	Permit	Deny	Permit	Permit
Interswitch Link Port	Deny ²	Permit	Permit	Permit	Permit

¹ An interswitch link port is a regular port that connects two switches and that happens to carry two or more VLANs.

² This behavior applies to traffic that traverses inter-switch link ports over an isolated VLAN only. Traffic from an inter-switch link port to an isolated port will be denied if it is in the isolated VLAN. Traffic from an inter-switch link port to an isolated port will be permitted if it is in the primary VLAN.

Guidelines and Limitations

Private VLANs have the following configuration guidelines and limitations:

- Control VLANs, packet VLANs, and management VLANs must be configured as regular VLANs and not as PVLANS.
- You should create port profiles with PVLAN configuration and associate them to uplink ports as part of OpenStack deployment.
- For configuring PVLANS on vETH interfaces, publish the port profiles with PVLAN configuration to OpenStack and associate them as policy profiles as part of creating a VM interface.

Default Settings

Table 7: Default VLAN Settings

Parameters	Default
Private VLANs	Disabled

Configuring a Private VLAN

The following section guides you through the private VLAN configuration process. After completing each procedure, return to this section to make sure that you have completed all required procedures in the correct sequence.

Procedure

-
- Step 1** Enable or disable the PVLAN feature globally. See [Enabling or Disabling the Private VLAN Feature Globally, on page 21](#).
 - Step 2** Configure one or more VLANs as primary VLAN(s) on the VSM. See [Configuring a VLAN as a Primary VLAN, on page 22](#).
 - Step 3** Configure a VLAN as a secondary VLAN on the VSM. See [Configuring a VLAN as a Secondary VLAN, on page 23](#).
 - Step 4** Associate secondary VLANs to a PVLAN. See [Associating the VLANs in a PVLAN, on page 24](#).
 - Step 5** Configure PVLAN port profiles for host uplink and OpenStack VMs. For more information, see the *Cisco Nexus 1000V for KVM Port Profile Configuration Guide*.
 - Step 6** Create a network segment in OpenStack for each PVLAN. For more information, see the *Cisco Nexus 1000V for KVM Virtual Network Configuration Guide*.
-

Enabling or Disabling the Private VLAN Feature Globally

You can globally enable or disable the PVLAN feature.

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters global configuration mode.
Step 2	switch(config)# [no] feature private-vlan	Globally enables or disables the PVLAN feature.
Step 3	switch(config-vlan)# show feature	(Optional) Displays features available and whether they are enabled globally.
Step 4	switch(config-vlan)# copy running-config startup-config	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

This example shows how to enable or disable the PVLAN feature globally:

```
switch# configure terminal
switch(config)# feature private-vlan
switch(config-vlan)# show feature
Feature Name      Instance  State
-----
dhcp-snooping    1        enabled
http-server      1        enabled
ippool           1        enabled
lACP             1        enabled
lisp             1        enabled
lisp-helper      1        enabled
netflow          1        disabled
port-profile-roles 1        enabled
private-vlan     1        enabled
sshServer        1        enabled
tacacs           1        enabled
telnetServer     1        enabled
switch(config-vlan)#
```

Configuring a VLAN as a Primary VLAN

You can configure a VLAN to function as the primary VLAN in a PVLAN.

Before You Begin

- Log in to the CLI in EXEC mode.
- You have already enabled the private VLAN feature using the [Enabling or Disabling the Private VLAN Feature Globally](#), on page 21.
- Know that the VLAN that you are configuring as a primary VLAN already exists in the system as a normal VLAN, and you know the VLAN ID.



Note If the VLAN does not already exist, you are prompted to create it when you create the primary VLAN. For information about creating a VLAN, see [Creating a VLAN](#), on page 11.

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters global configuration mode.
Step 2	switch(config)# vlan <i>primary-vlan-id</i>	Enters VLAN configuration mode for the specified VLAN and configures the primary VLAN ID in the running configuration.
Step 3	switch(config-vlan)# private-vlan primary	Designates the primary VLAN as a private VLAN in the running configuration.

	Command or Action	Purpose
Step 4	switch(config-vlan)# exit	Exits VLAN configuration mode. Note You must exit VLAN configuration mode for the configurations to take effect.
Step 5	switch(config)# show vlan private-vlan	(Optional) Displays the PVLAN configuration.
Step 6	switch(config)# copy running-config startup-config	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

This example shows how to configure a VLAN as a primary VLAN:

```
switch# configure terminal
switch(config)# vlan 202
switch(config-vlan)# private-vlan primary
n1000v(config-vlan)# exit
switch(config)# show vlan private-vlan
Primary Secondary Type Ports
-----
202 primary
```

switch(config)#

Configuring a VLAN as a Secondary VLAN

You can configure a VLAN to function as the secondary VLAN in a PVLAN.

Before You Begin

- Log in to the CLI in EXEC mode.
- You have already enabled the private VLAN feature using the [Enabling or Disabling the Private VLAN Feature Globally](#), on page 21.
- Know that the VLAN that you are configuring as a secondary VLAN already exists in the system as a normal VLAN, and you know the VLAN ID.



Note

If the VLAN does not already exist, you are prompted to create it when you create the secondary VLAN. For information about creating a VLAN, see [Creating a VLAN](#), on page 11.

- Know whether you want the secondary VLANs to be community VLANs or isolated VLANs, and the VLAN IDs for each.

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters global configuration mode.
Step 2	switch(config)# vlan <i>secondary-vlan-id</i>	Enters VLAN configuration mode for the specified VLAN and configures the secondary VLAN ID in the running configuration.
Step 3	switch(config-vlan)# private-vlan {community isolated}	Designates the VLAN as either a community or isolated private VLAN in the running configuration.
Step 4	switch(config-vlan)# exit	Exits VLAN configuration mode. Note You must exit the VLAN configuration mode for the configurations to take affect.
Step 5	switch(config)# show vlan private-vlan	(Optional) Displays the PVLAN configuration.
Step 6	switch(config)# copy running-config startup-config	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

This example shows how to configure a VLAN as a secondary VLAN:

```
switch# configure terminal
switch(config)# vlan 303
switch(config-vlan)# private-vlan community
switch(config-vlan)# exit
switch(config)# show vlan private-vlan
Primary  Secondary  Type              Ports
-----  -
303      303             community
switch(config)#
```

Associating the VLANs in a PVLAN

You can associate the primary VLANs in a PVLAN with the secondary VLANs.

Before You Begin

- Log in to the CLI in EXEC mode.
- Know that the primary VLAN for this PVLAN is already configured as a PVLAN.
- Know that the secondary VLANs for this PVLAN are already configured as PVLANS.
- Know the secondary VLAN IDs to be associated for each primary VLAN ID.

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters global configuration mode.
Step 2	switch(config)# vlan <i>primary-vlan-id</i>	Enters VLAN configuration mode and associates the VLANs to function as a PVLAN in the running configuration.
Step 3	switch(config-vlan)# private-vlan association {add remove} secondary vlan-id	Associates a specified secondary VLAN with the primary VLAN to function as a PVLAN in the running configuration. To associate additional secondary VLANs, repeat this step.
Step 4	switch(config-vlan)# exit	Exits VLAN configuration mode.
Step 5	switch(config)# show vlan private-vlan	(Optional) Displays the PVLAN configuration.
Step 6	switch(config)# copy running-config startup-config	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

This example shows how to associate VLANs in a PVLAN:

```
switch# configure terminal
switch(config)# vlan 202
switch(config-vlan)# private-vlan association add 303
switch(config-vlan)# exit
switch(config)# show vlan private-vlan
Primary  Secondary  Type           Ports
-----  -
202      303          community
switch(config)#
```

Configuring a Layer 2 Port Profile as a Promiscuous Trunk Port

You can configure a Layer 2 interface as a promiscuous trunk port that does the following:

- Combines multiple promiscuous ports into a single trunk port.
- Carries all normal VLANs.
- Carries multiple PVLAN primary VLANs each with selected secondary VLANs.

**Note**

A promiscuous port can be either access or trunk. If you have one primary VLAN, you can use a promiscuous access port. If you have multiple primary VLANs, you can use a promiscuous trunk port.

Before You Begin

- Log in to the CLI in EXEC mode.
- Know that the **private-vlan mapping trunk** command does not decide or override the trunk configuration of a port.
- Know that the port is already configured in a regular trunk mode before adding the PVLAN trunk configurations.
- Know that primary VLANs must be added to the list of allowed VLAN for the promiscuous trunk port.
- Know that secondary VLANs are not configured in the allowed VLAN list.
- Know that the trunk port can carry normal VLANs in addition to primary VLANs.
- Know that you can map up to 64 primary VLANs to their secondary VLANs in one promiscuous trunk port.

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters global configuration mode.
Step 2	switch(config)# port-profile type ethernet <i>name</i>	Places you in port-profile mode.
Step 3	switch(config-port-prof)# switchport mode trunk	Designates that the interfaces are to be used as trunking ports.
Step 4	switch(config-port-prof)# switchport mode private-vlan trunk promiscuous	In the running configuration, designates the interface as a promiscuous PVLAN trunk port.
Step 5	switch(config-port-prof)# switchport private-vlan trunk allowed vlan <i>vlan_range</i>	Sets the allowed VLANs and VLAN IDs when the interface is in PVLAN trunking mode.
Step 6	switch(config-port-prof)# switchport private-vlan mapping trunk <i>primary_vlan_ID {secondary_vlan_list add secondary_vlan_list remove secondary_vlan_list}</i>	Maps the PVLAN trunk port to a primary VLAN and to selected secondary VLANs in the running configuration. Multiple PVLAN pairs can be specified so that a promiscuous trunk port can carry multiple primary VLANs.
Step 7	switch(config-port-prof)# no shut	Enables the port profile.
Step 8	switch(config-port-profile)# publish port-profile	Pushes the port profile to the VEMs and to the OpenStack controller.
Step 9	switch(config-port-profile)# state enabled	Enables the port profile and applies its configuration to the assigned ports.

	Command or Action	Purpose
Step 10	switch(config-if)# copy running-config startup-config	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

This example shows how to configure a Layer 2 port profile as a promiscuous trunk port:

```
switch # configure terminal
switch(config)# port-profile type eth allaccess1
switch(config-port-prof)# switchport mode trunk
switch(config-port-prof)# switchport mode private-vlan trunk promiscuous
switch(config-port-prof)# switchport private-vlan trunk allowed vlan 2,202,150-155
switch(config-port-prof)# switchport private-vlan mapping trunk 202 303
switch(config-port-prof)# no shut
switch(config-port-prof)# publish port-profile
switch(config-port-prof)# state enabled
```

Configuring a Private VLAN Promiscuous Access Port

You can configure a port to be used as a promiscuous access port in a PVLAN.

Before You Begin

- Log in to the CLI in EXEC mode.
- Know the name of the interface that will function as a promiscuous access port.

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters global configuration mode.
Step 2	switch(config)# interface type [<i>slot/port</i> <i>number</i>]	Enters interface configuration mode for the specified interface.
Step 3	switch(config-if)# switchport mode private-vlan promiscuous	Designates that the interface is to function as a promiscuous access port for a PVLAN in the running configuration.
Step 4	switch(config-if)# show interface type [<i>slot/port</i> <i>number</i>]	(Optional) Displays the interface configuration.
Step 5	switch(config-if)# copy running-config startup-config	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

This example shows how to configure a PVLAN promiscuous access port:

```
switch# configure terminal
switch(config)# interface eth3/2
switch(config-if)# switchport mode private-vlan promiscuous
switch(config-if)# show interface eth3/2
Ethernet3/2 is up
  Hardware is Ethernet, address is 0050.5655.2e85 (bia 0050.5655.2e85)
  MTU 1500 bytes, BW -1942729464 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA
  Port mode is promiscuous
  full-duplex, 1000 Mb/s
  Beacon is turned off
  Auto-Negotiation is turned on
  Input flow-control is off, output flow-control is off
  Rx
    276842 Input Packets 100419 Unicast Packets
    138567 Multicast Packets 37856 Broadcast Packets
    25812138 Bytes
  Tx
    128154 Output Packets 100586 Unicast Packets
    1023 Multicast Packets 26545 Broadcast Packets 26582 Flood Packets
    11630220 Bytes
    173005 Input Packet Drops 37 Output Packet Drops

switch(config-if)#
```

Associating a Promiscuous Access Port with a Private VLAN

You can associate the promiscuous access port with the primary and secondary VLANs in a PVLAN.

Before You Begin

- Log in to the CLI in EXEC mode.
- Know the VLAN IDs of the primary and secondary VLANs in the PVLAN.
- Know the primary and secondary VLANs that are already configured as PVLAN.
- Know the name of the interface functioning in the PVLAN as a promiscuous access port.

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters global configuration mode.
Step 2	switch(config)# interface <i>type [slot/port number]</i>	Enters interface configuration mode for the specified interface.
Step 3	switch(config-if)# switchport private-vlan mapping <i>primary_vlan_ID {secondary_vlan_list add secondary_vlan_list remove secondary_vlan_list}</i>	Associates the promiscuous access port with the VLAN IDs in the PVLAN in the running configuration.
Step 4	switch(config-if)# show interface <i>type [slot/port number]</i>	(Optional) Displays the interface configuration.

	Command or Action	Purpose
Step 5	switch(config-if)# copy running-config startup-config	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

This example shows how to associate a promiscuous access port with a PVLAN:

```
switch# configure terminal
switch(config)# interface eth3/2
switch(config-if)# switchport private-vlan mapping 202 303
switch(config-if)# show vlan private-vlan
-----
Primary  Secondary  Type           Ports
-----
202      303          community      Eth3/2
switch(config-if)#
```

Removing a Private VLAN Configuration

You can remove a PVLAN configuration and return the VLAN to normal VLAN mode.

Before You Begin

- Log in to the CLI in EXEC mode.
- The VLAN is configured as a private VLAN, and you know the VLAN ID.
- When you remove a PVLAN configuration, the ports associated with it become inactive.

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters global configuration mode.
Step 2	switch(config)# vlan private vlan-id	Enters the VLAN configuration mode for the specified VLAN.
Step 3	switch(config-vlan)# no private-vlan {community isolated primary}	Removes the specified VLAN from a PVLAN in the running configuration. The private VLAN configuration is removed from the specified VLAN(s). The VLAN is returned to normal VLAN mode. The ports associated with the VLAN are inactive.
Step 4	switch(config-vlan)# exit	Exits VLAN configuration mode.
Step 5	switch(config)# show vlan private-vlan	(Optional) Displays the PVLAN configuration.

	Command or Action	Purpose
Step 6	switch(config)# copy running-config startup-config	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

This example shows how to remove a PVLAN configuration:

```
switch# configure terminal
switch(config)# vlan 202
switch(config-vlan)# no private-vlan association secondary vlan-ids
switch(config-vlan)# no private-vlan primary
switch(config-vlan)# exit
switch(config)# show vlan private-vlan
Primary  Secondary  Type
-----  -
switch(config)#
```

Verifying a Private VLAN Configuration

Use the following commands to verify a private VLAN configuration:

Command	Purpose
show feature	Displays features available and whether they are enabled globally.
show running-config vlan <i>vlan-id</i>	Displays VLAN information.
show vlan private-vlan [<i>type</i>]	Displays information about PVLANS.
show interface switchport	Displays information about all interfaces configured as switchports.

Configuration Examples for Private VLANs

Example: PVLAN Trunk Port

This example shows how to configure interface Ethernet 2/6 as the following:

- PVLAN trunk port
- Mapped to primary PVLAN 202 which is associated with secondary VLANs 303 and 440
- Mapped to primary PVLAN 210 which is associated with secondary VLANs 310 and 450

```
switch# configure terminal
switch(config)# vlan 303,310
```

```

switch(config-vlan)# private-vlan community
switch(config-vlan)# exit
switch(config)# vlan 440,450
switch(config-vlan)# private-vlan isolated
switch(config-vlan)# exit
switch(config)# vlan 202
switch(config-vlan)# private-vlan primary
switch(config-vlan)# private-vlan association 303,440
switch(config-vlan)# exit
switch(config)# vlan 210
switch(config-vlan)# private-vlan primary
switch(config-vlan)# private-vlan association 310,450
switch(config-vlan)# exit

switch# configure terminal
switch(config)# int eth2/6
switch(config-if)# switchport mode private-vlan trunk promiscuous
switch(config-if)# switchport private-vlan trunk allowed vlan all
switch(config-if)# switchport private-vlan mapping trunk 202 303, 440
switch(config-if)# switchport private-vlan mapping trunk 210 310, 450
switch(config-if)# show interface switchport
Name: Ethernet2/6
  Switchport: Enabled
Operational Mode: Private-vlan trunk promiscuous
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: 1-3967,4048-4093
Administrative private-vlan primary host-association: none
  Administrative private-vlan secondary host-association: none
  Administrative private-vlan primary mapping: none
  Administrative private-vlan secondary mapping: none
  Administrative private-vlan trunk native VLAN: 1
  Administrative private-vlan trunk encapsulation: dot1q
  Administrative private-vlan trunk normal VLANs: 1-3967, 4048-4093
  Administrative private-vlan trunk private VLANs: (202,303) (202,440) (210,310) (210,450)
Operational private-vlan: 202,210,303,310,440,450
switch(config-if)#

```

Example: PVLAN Using Port Profiles

This example configuration shows how to configure interface eth2/6 using port-profile, uppvlanpromtrunk156.

In this configuration, packets from secondary interfaces 153, 154, and 155 are translated into the PVLAN 156:

```

vlan 153-154
  private-vlan community
vlan 155
  private-vlan isolated
vlan 156
  private-vlan association 153-155
  private-vlan primary

switch# show run int eth2/6

version 4.0(1)
interface Ethernet2/6
switchport
inherit port-profile uppvlanpromtrunk156

switch# show port-profile name uppvlanpromtrunk156
port-profile uppvlanpromtrunk156
description:
status: enabled
capability privileged: no
capability uplink: yes
port-group: uppvlanpromtrunk156
config attributes:
switchport mode private-vlan trunk promiscuous
switchport private-vlan trunk allowed vlan all

```

```

switchport private-vlan mapping trunk 156 153-155
no shutdown
evaluated config attributes:
switchport mode trunk
switchport trunk allowed vlan all
switchport private-vlan mapping trunk 156 153-155
no shutdown
assigned interfaces:
Ethernet2/6

switch# show interface eth 2/6 switchport
Name: Ethernet2/6
  Switchport: Enabled
  Switchport Monitor: Not enabled
  Operational Mode: Private-vlan trunk promiscuous
  Access Mode VLAN: 1 (default)
  Trunking Native Mode VLAN: 1 (default)
  Trunking VLANs Enabled: 1-3967,4048-4093
  Administrative private-vlan primary host-association: none
  Administrative private-vlan secondary host-association: none
  Administrative private-vlan primary mapping: none
  Administrative private-vlan secondary mapping: none
  Administrative private-vlan trunk native VLAN: 1
  Administrative private-vlan trunk encapsulation: dot1q
  Administrative private-vlan trunk normal VLANs: 1-155,157-3967,4048-4093
  Administrative private-vlan trunk private VLANs: (156,153) (156,155)
  Operational private-vlan: 156,153,155 inherit port-profile uppvlanpromtrunk156
switch#

```

Feature History for Private VLANs

Feature Name	Feature Name	Releases
Private VLAN	5.2(1)SK3(2.1)	This feature was introduced.



Configuring IGMP Snooping

This chapter contains the following sections:

- [Information about IGMP Snooping, page 33](#)
- [Prerequisites for IGMP Snooping, page 35](#)
- [Default Settings, page 35](#)
- [Configuring IGMP Snooping, page 36](#)
- [Verifying the IGMP Snooping Configuration, page 38](#)
- [Feature History for IGMP Snooping, page 38](#)

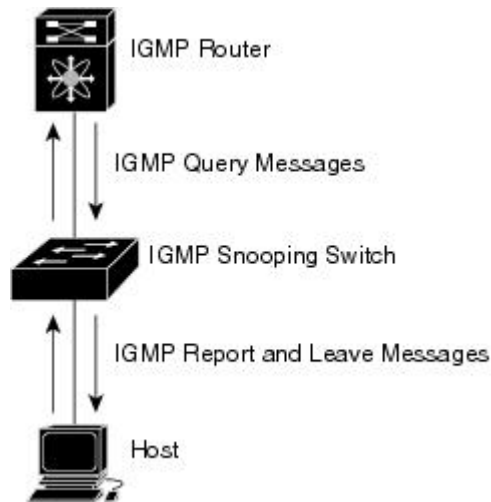
Information about IGMP Snooping

Introduction

The Internet Group Management Protocol (IGMP) snooping software examines Layer 2 IP multicast traffic within a VLAN to discover the ports where interested receivers reside. Using the port information, IGMP snooping can reduce bandwidth consumption in a multi-access LAN environment to avoid flooding the entire VLAN. The IGMP snooping feature tracks which ports are attached to multicast-capable routers to help the routers forward IGMP membership reports. The IGMP snooping software responds to topology change notifications. By default, IGMP snooping is enabled on the device.

The following figure shows an IGMP snooping switch that sits between the host and the IGMP router. The IGMP snooping switch snoops the IGMP membership reports and Leave messages and forwards them only when necessary to the connected IGMP routers.

Figure 2: IGMP Snooping Switch



The IGMP snooping software operates upon IGMPv1, IGMPv2, and IGMPv3 control plane packets where Layer 3 control plane packets are intercepted and influence the Layer 2 forwarding behavior.

The Cisco Nexus 1000V IGMP snooping implementation has the following proprietary features:

- Multicast forwarding based on an IP address rather than a MAC address.
- Optimized multicast flooding (OMF) that forwards unknown traffic to routers only and performs no data driven state creation.

For more information about IGMP snooping, see RFC 4541.

IGMPv1 and IGMPv2

IGMPv2 supports the fast leave feature. The fast leave feature does not send last member query messages to hosts. As soon as the software receives an IGMP leave message, the software stops forwarding multicast data to that port.

IGMPv1 does not provide an explicit IGMP leave message, so the software must rely on the membership message timeout to indicate that no hosts remain that want to receive multicast data for a particular group.

Report suppression is not supported and is disabled by default.

IGMPv3

IGMPv3 snooping provides constrained flooding based on the group IP information in the IGMPv3 reports. Report suppression is not supported and disabled by default. In addition, explicit tracking is not supported and disabled by default. Instead, the fast leave feature is used for handling leave messages.

Prerequisites for IGMP Snooping

IGMP snooping has the following prerequisites:

- You are logged in to the switch.
- A querier must be running on the uplink switches on the VLANs that contain multicast sources and receivers.

When the multicast traffic does not need to be routed, you must configure an external switch to query membership. On the external switch, define the query feature in a VLAN that contains multicast sources and receivers but no other active query feature. In the Cisco Nexus 1000V, report suppression is not supported and is disabled by default.

When an IGMP snooping query feature is enabled on an upstream switch, it sends out periodic IGMP queries that trigger IGMP report messages from hosts wanting to receive IP multicast traffic. IGMP snooping listens to these IGMP reports to identify accurate forwarding.

Default Settings

Table 8: Default IGMP Snooping Settings

Parameters	Default
IGMP snooping	Enabled
IGMPv3 Explicit tracking	Disabled (Not supported.)
IGMPv2 Fast leave	Enabled (Cannot be disabled.)
Last member query interval	1 second
Link-local groups suppression	Enabled
Snooping querier	Disabled
IGMPv1/v2 Report suppression	Disabled
IGMPv3 Report suppression	Disabled

Configuring IGMP Snooping

Enabling or Disabling IGMP Snooping Globally for the VSM

You can enable or disable IGMP snooping globally for the VSM. IGMP snooping is enabled globally on the VSM by default. If you enable IGMP snooping globally, you can turn IGMP snooping off individually for each VLAN. If you disable IGMP snooping globally, then IGMP snooping on all VLANs is disabled regardless of their individual settings.

Before You Begin

You are logged in to the CLI in EXEC mode.

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters global configuration mode.
Step 2	switch(config)# [no] ip igmp snooping	Enables or disables IGMP snooping in the running configuration for all VLANs. The default is enabled. If you have previously disabled the feature then you can enable it with this command.
Step 3	switch(config)# show ip igmp snooping [vlan <i>vlan-id</i>]	(Optional) Displays the configuration for verification.
Step 4	switch(config)# copy running-config startup-config	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

```
switch# configure terminal
switch(config)# no ip igmp snooping
switch(config)# show ip igmp snooping
Global IGMP Snooping Information:
IGMP Snooping disabled
Optimised Multicast Flood (OMF) enabled
IGMPv1/v2 Report Suppression disabled
IGMPv3 Report Suppression disabled
Link Local Groups Suppression enabled
VPC Multicast optimization disabled

IGMP Snooping information for vlan 1
IGMP snooping disabled
Optimised Multicast Flood (OMF) disabled
IGMP querier none
Switch-querier disabled
IGMPv3 Explicit tracking enabled
IGMPv2 Fast leave enabled
IGMPv1/v2 Report suppression disabled
IGMPv3 Report suppression disabled
Link Local Groups suppression enabled
Router port detection using PIM Hellos, IGMP Queries
Number of router-ports: 0
```



```
Number of groups: 0
VLAN vPC function disabled
Active ports:
```

```
switch(config)#
```

Configuring IGMP Snooping on a VLAN

Use this procedure to configure IGMP snooping on a VLAN. IGMP snooping is enabled by default for all VLANs in the VSM.

Before You Begin

You are logged in to the CLI in EXEC mode.



Note

If IGMP snooping is disabled globally, it takes precedence over the VLAN state.

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters global configuration mode.
Step 2	switch(config)# vlan configuration <i>vlan-id</i>	Enters configuration mode for the specified VLAN.
Step 3	switch(config-vlan-config)# [no] ip igmp snooping	Enables or disables IGMP snooping in the running configuration for the specific VLAN. If IGMP snooping is enabled for the VSM, then IGMP snooping is enabled for the VLAN by default. Note IGMP snooping must be enabled globally (the default) in order to toggle it on or off per VLAN. If IGMP snooping is disabled globally, then it cannot be enabled per VLAN.
Step 4	switch(config-vlan-config)# [no] ip igmp snooping mrouter interface <i>type if_id</i>	(Optional) Configures a static connection for the VLAN to a multicast router in the running configuration. The interface to the router must be in the specified VLAN. You can specify the interface by the type and the number.
Step 5	switch(config-vlan-config)# [no] ip igmp snooping static-group <i>group-ip-addr interface type if_id</i>	(Optional) Configures a VLAN Layer 2 port as a static member of a multicast group in the running configuration. You can specify the interface by the type and the number.
Step 6	switch(config-vlan-config)# [no] ip igmp snooping link-local-groups-suppression	(Optional) Configures link-local groups suppression. The default is enabled.

	Command or Action	Purpose
		Note You can apply link-local groups suppression to all interfaces in the VSM by entering this command in global configuration mode.
Step 7	switch(config-vlan-config)# show ip igmp snooping [vlan <i>vlan-id</i>]	(Optional) Displays the configuration for verification.
Step 8	switch(config-vlan-config)# copy running-config startup-config	(Optional) (Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

Verifying the IGMP Snooping Configuration

Use the following commands to verify the IGMP snooping configuration information.

Command	Purpose
show ip igmp snooping [vlan <i>vlan-id</i>]	Displays IGMP snooping configuration by VLAN.
show ip igmp snooping groups [vlan <i>vlan-id</i>] [detail]	Displays IGMP snooping information about groups by VLAN.
show ip igmp snooping querier [vlan <i>vlan-id</i>]	Displays IGMP snooping queriers by VLAN.
show ip igmp snooping mroute [vlan <i>vlan-id</i>]	Displays multicast router ports by VLAN.

Feature History for IGMP Snooping

Feature Name	Release	Description
IGMP Snooping	Release 5.2(1)SK1(2.1)	This feature was introduced.