

# set protocols igmp-snooping vlan-id enable

The Internet Group Management Protocol (IGMP) is used to establish multicast group membership on IPv4 networks, making it an important component of IP multicast. It is used for one-to-many applications such as video streaming and gaming. IGMP snooping involves the process of listening for IGMP traffic between hosts and routers, enabling a switch to learn which devices are involved in which IP multicast conversations. This enables multicasts to be filtered from links and ports where they're not needed, thus reducing network traffic. IGMP snooping is typically disabled by default on network switches. This document details how to enable IGMP if desired, on a per-VLAN basis.

## Command Syntax

```
set protocols igmp-snooping vlan-id <vlan-id> enable <true | false>
```

## Parameter

Parameter	Description
<b>vlan-id</b> <vlan-id>	Specifies a VLAN ID. The value is an integer that ranges from 1 to 4094.
<b>enable</b> <true   false>	Enable or disable the VLAN-based IGMP snooping function. The value is <b>true</b> or <b>false</b> . <ul style="list-style-type: none"><li><b>true</b>: enables the VLAN-based IGMP snooping function.</li><li><b>false</b>: disables the VLAN-based IGMP snooping function.</li></ul> The default value is <b>false</b> .

## Usage Guidelines

After the global IGMP snooping is enabled by using `set protocols igmp-snooping enable` command, IGMP snooping in the VLAN is disabled by default. To enable IGMP snooping in a VLAN, you also need to enable the VLAN-based IGMP snooping function.

After IGMP snooping is enabled in a VLAN, it will take effect only on interfaces that have already been added to this VLAN.

## Example

- Enable the VLAN-based IGMP snooping function.

```
admin@Xorplus# set protocols igmp-snooping vlan-id 2 enable true
admin@Xorplus# commit
```