Пример настройки IGMP Snooping

При получении коммутатором группового трафика (широковещательного или многоадресного) он начинает передавать кадры через все порты. Такое поведение хорошо подходит для широковещательной передачи, когда кадры предназначены для всех подключенных к коммутатору узлов. Однако в случае многоадресной рассылки кадр предназначен для небольшого числа узлов. Исходя из логики работы коммутатора, кадры многоадресной рассылки будут пересылаться, в том числе, в те сегменты сети, где ни один узел не заинтересован в их получении. Таким образом, это приведет к неэффективному использованию полосы пропускания сети. Если многоадресного трафика много, встает задача его ограничения на канальном уровне.

Функция IGMP Snooping работает на канальном уровне модели OSI и предотвращает лавинную рассылку многоадресных пакетов. Когда она активирована, коммутатор отслеживает IGMP-сообщения (запросы и ответы), передаваемые между узлами-подписчиками и маршрутизаторами многоадресной рассылки и использует их содержимое для построения таблицы передачи многоадресного трафика. Формируя данную таблицу, коммутатор осуществляет передачу многоадресного трафика только тем узлам, которые в нем заинтересованы.

В таблицу передачи многоадресного трафика могут добавляться статические записи. Они создаются вручную администратором сети в том случае, если подключенные к коммутатору узлы не поддерживают протокол IGMP, но хотят получать трафик определенной многоадресной группы.

Если в сети нет маршрутизатора многоадресной рассылки и источник многоадресного трафика подключен напрямую к коммутатору, то необходимо настроить **IGMP Snooping Querier** в соответствующей VLAN на коммутаторе.

Функция **IGMP Snooping Fast Leave**, активированная на коммутаторе, позволяет мгновенно исключить порт из таблицы передачи многоадресного трафика при получении им сообщения о выходе из группы. Это позволяет прекратить передачу по сети ненужных потоков данных и более эффективно использовать полосу пропускания. Функция IGMP Snooping Fast Leave полезна в приложениях IPTV, так как с ее помощью можно уменьшить время при переключении пользователей между телевизионными каналами. Следует отметить, что порт будет удален из таблицы передачи многоадресного трафика только в том случае, если к нему больше не подключено ни одного узла-подписчика. Функция IGMP Snooping Fast Leave активируется в VLAN.

Примечание к настройке

Рассматриваемый пример настройки подходит для следующих серий коммутаторов: DGS-1250, DGS-1510, DGS-1520, DGS-3130, DGS-3630, DXS-3610.

Задача 1

В сети реализован сервис многоадресной рассылки. Клиенты, среди которых имеются подписчики многоадресной рассылки, подключены к коммутаторам второго уровня. Нужно обеспечить передачу многоадресной рассылки только подписчикам.

Задача решается настройкой IGMP Snooping на коммутаторе второго уровня.

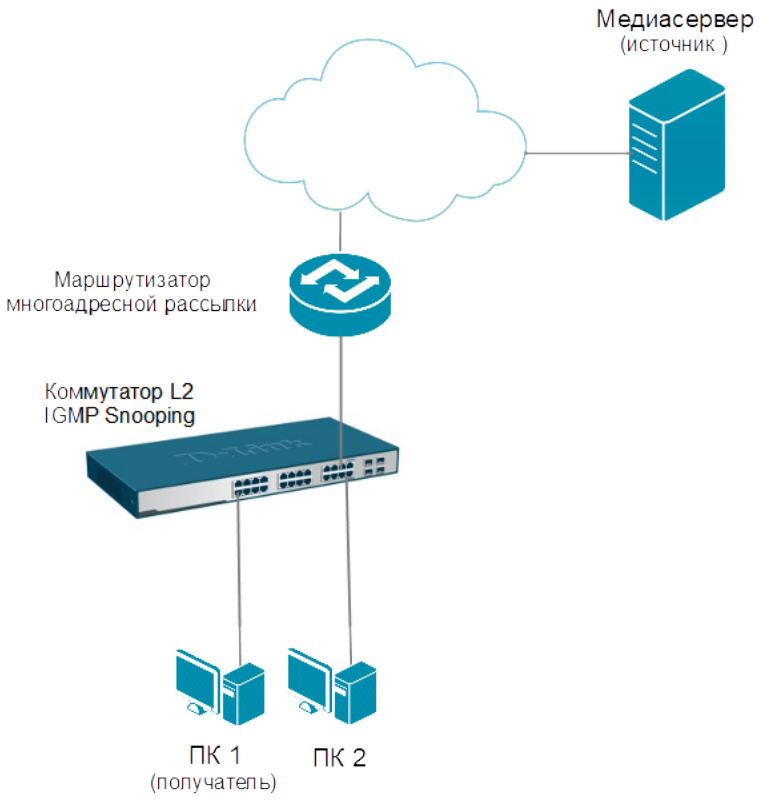

Рис. 1 Схема подключения

Настройка коммутатора

1. Активируйте функцию IGMP Snooping глобально на коммутаторе:

```
Switch# configure terminal
Switch(config)# ip igmp snooping
```


© 2023 D-Link

2. Активируйте функцию IGMP Snooping в указанной VLAN (в примере VLAN по умолчанию):

```
Switch(config)# vlan 1
Switch(config-vlan)# ip igmp snooping
```

3. Включите фильтрацию многоадресного трафика, чтобы избежать его передачи узлам, не являющимся подписчиками многоадресной рассылки. Ограничьте количество создаваемых записей в таблице передачи многоадресного трафика:

```
Switch(config-vlan)# multicast filtering-mode filter-unregistered
Switch(config-vlan)# exit
Switch(config)#interface range ethernet 1/0/1-24
Switch(config-if-range)#ip igmp snooping limit 100 vlan 1
Switch(config-if-range)#exit
```

4. Активируйте функцию IGMP Snooping Fast Leave:

```
Switch(config)# vlan 1
Switch(config-vlan)# ip igmp snooping fast-leave
Switch(config-vlan)# end
```

Задача 2

В сети реализован сервис многоадресной рассылки. Клиенты, среди которых имеются подписчики многоадресной рассылки, подключены к коммутаторам второго уровня, но маршрутизатор многоадресной рассылки в сети отсутствует. Нужно обеспечить передачу многоадресной рассылки только подписчикам.

Задача решается настройкой IGMP Snooping на коммутаторе второго уровня. Коммутатор настраивается в качестве IGMP Snooping Querier в указанной VLAN.

© 2023 D-Link

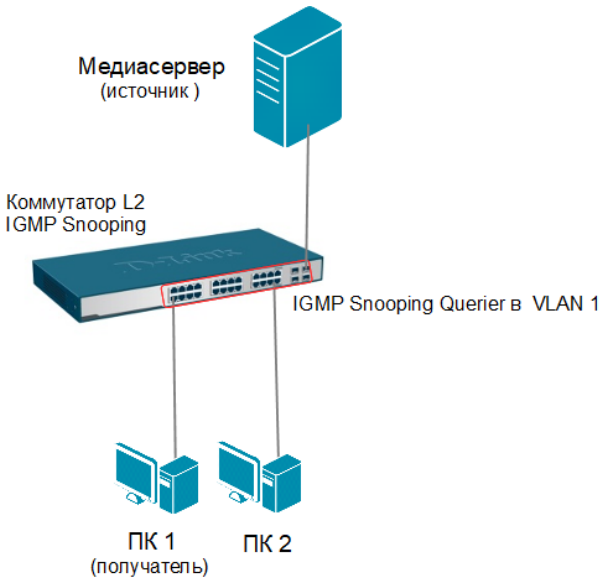

Рис. 2 Схема сети

1. Активируйте функцию IGMP Snooping глобально на коммутаторе:

```
Switch# configure terminal
Switch(config)# ip igmp snooping
```

2. Активируйте функцию IGMP Snooping и настройте коммутатор в качестве IGMP Snooping Querier в указанной VLAN (в примере VLAN по умолчанию):

```
Switch(config)# vlan 1
Switch(config-vlan)# ip igmp snooping
Switch(config-vlan)# ip igmp snooping querier
```

3. Настройте интервал отправки коммутатором сообщений IGMP Query (по умолчанию 125 секунд) и максимальное время ответа на них (по умолчанию 10 секунд):

```
Switch(config-vlan)# ip igmp snooping query-interval 200
Switch(config-vlan)# ip igmp snooping query-max-response-time 20
```

4. Включите фильтрацию многоадресного трафика, чтобы избежать его передачи узлам, не являющимся подписчиками многоадресной рассылки:

```
Switch(config-vlan)# multicast filtering-mode filter-unregistered
```

5. Активируйте функцию IGMP Snooping Fast Leave:

© 2023 D-Link

```
Switch(config-vlan)# ip igmp snooping fast-leave
Switch(config-vlan)# exit
```

6. Ограничьте количество создаваемых записей в таблице передачи многоадресного трафика:

```
Switch(config)#interface range ethernet 1/0/1-24
Switch(config-if-range)#ip igmp snooping limit 100 vlan 1
Switch(config-if-range)#end
```


© 2023 D-Link