Пример настройки IGMP Snooping через Web-интерфейс

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-3000.

Задача

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

Задача решается настройкой **IGMP Snooping** на коммутаторе второго уровня.

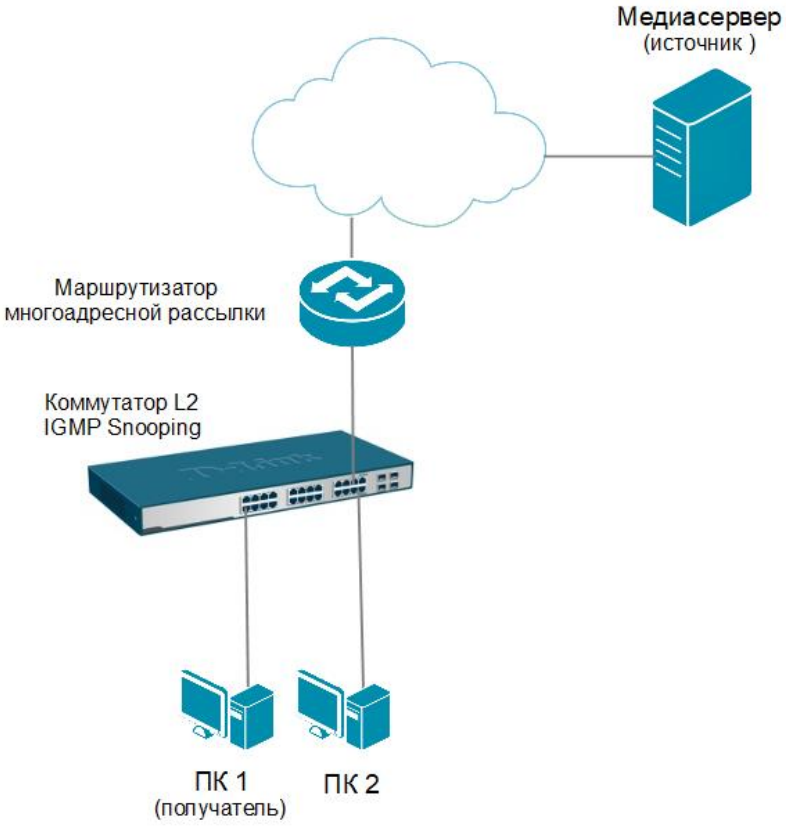
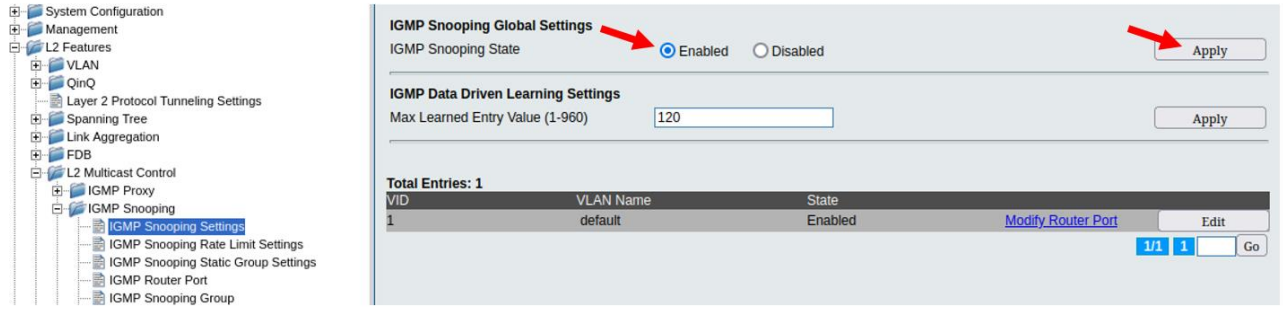


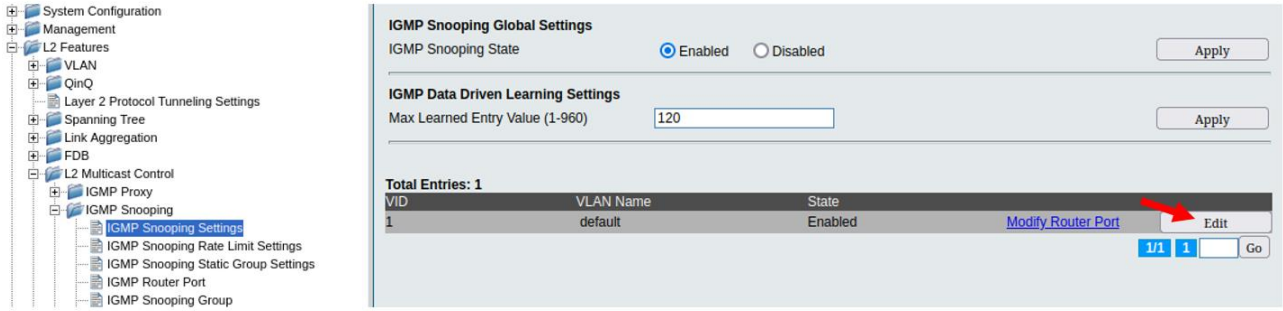
Рис. 1 Схема подключения

Настройка коммутатора

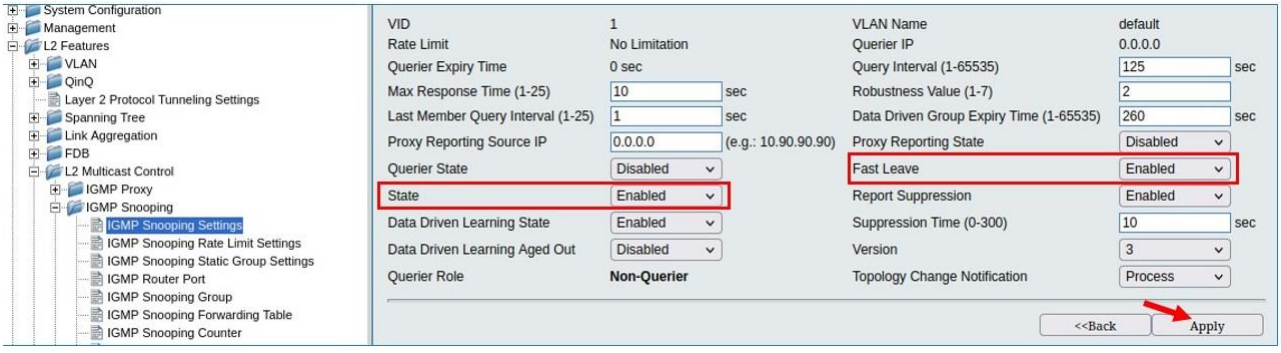
1. Выберите пункт меню **L2 Multicast Control** → **IGMP Snooping** → **IGMP Snooping Settings**. Активируйте функцию **IGMP Snooping** глобально на коммутаторе, выбрав радиокнопку **Enabled** в поле **IGMP Snooping State**. Нажмите **Apply**.



2. Активируйте функции **IGMP Snooping** и **IGMP Snooping Fast Leave** в требуемой VLAN (в примере – VLAN по умолчанию). Нажмите кнопку **Edit** в строке соответствующей VLAN.

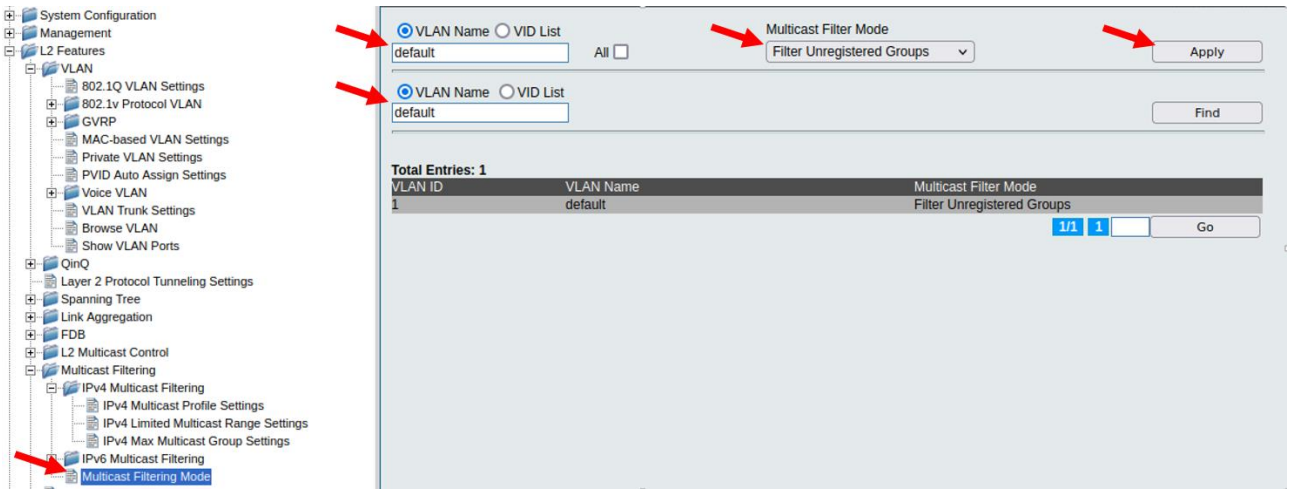


В открывшемся окне выберите **Enabled** в полях **State** и **Fast Leave**. Остальные параметры можно оставить по умолчанию. Нажмите **Apply**.



3. Выберите пункт меню **Multicast Filtering** → **Multicast Filtering Mode**. Включите фильтрацию многоадресного трафика, чтобы избежать его передачи узлам, не являющимся подписчиками многоадресной рассылки.

Введите имя VLAN, в которой необходимо включить фильтрацию, в поля **VLAN name** (в примере – **default**). В списке **Multicast Filter Mode** выберите **Filter Unregistered Groups** и нажмите **Apply**.



4. Перейдите в пункт меню **Save** → **Save Configuration** и сохраните настройки коммутатора.