Особенности использования коммутаторов в составе ГС с IP коммутацией.

Станция Chameleon является станцией с IP коммутацией. Это означает что все модули ГС подключены к IP коммутатору, через который они обмениваются информацией и видеопотоками. Такая архитектура обеспечивает высочайшую гибкость и почти неограниченные возможности для формирования функционала станции. При организации информационного обмена в станции используется идеология «общего котла» - все информационные потоки (видео/аудио сервисы), которые должны быть доступны для всех модулей станции посылаются в виде IP мультикастовых потоков в центральный коммутатор, из которого любой модуль может запросить любой поток, обработать его и, при необходимости, вернуть обратно. Для реализации такой идеологии используется мультикастовый формат передачи. Такие потоки, в отличие от юникастовых потоков, доступны для приема всеми модулями, а не только теми которым поток адресован. В станции с IP коммутацией более 95% трафика составляет мультикастовый трафик.

Накопившийся практический опыт показал, что работа коммутатора с таким трафиком имеет свои специфические особенности. Использование неподходящих или неправильно сконфигурированных коммутаторов является одной из основных причин проблем в работе такой станции.

Рассмотрим работу IP коммутатора с традиционным для него юникастовым трафиком. Юникастовый трафик – это трафик обеспечивающий передачу потоков от одного конкретного блока к другому конкретному блоку. Пример такой передачи показан на рисунке 1.

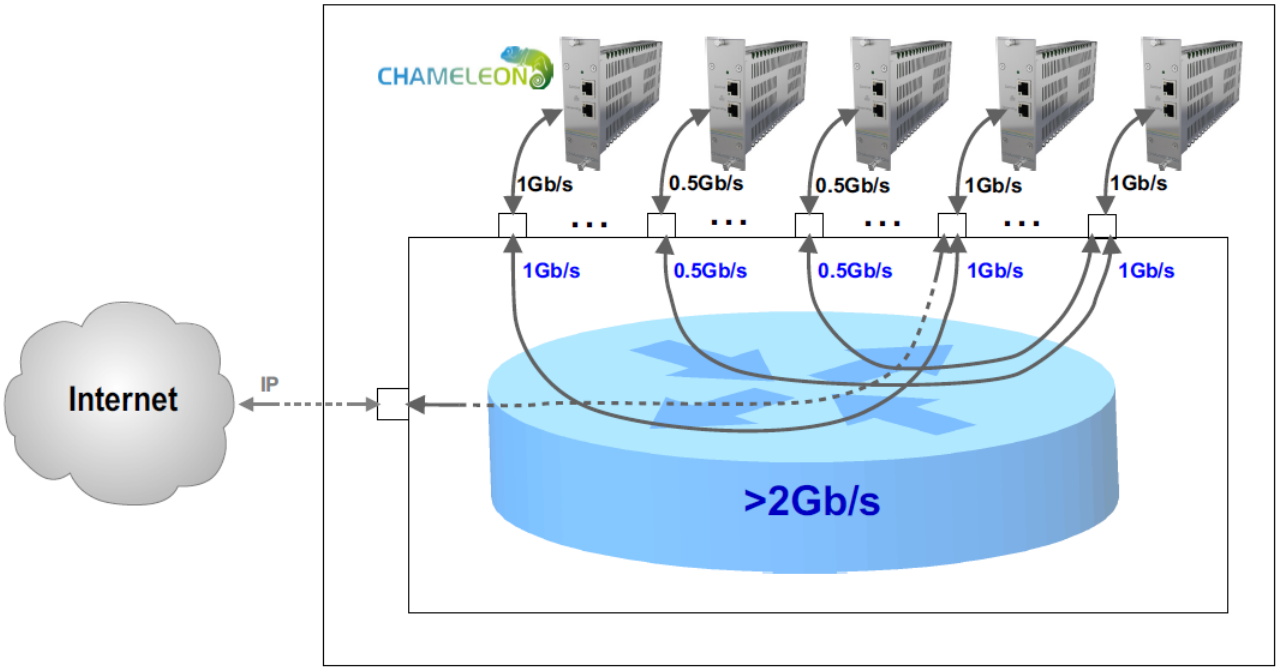


Рисунок 1. Работа IP коммутатора при передаче юникастового трафика.

На этом рисунке схематично изображен гигабитный IP коммутатор[1]. Для простоты считаем что вся пропускная способность любого из портов ввода/вывода составляет 1Гб (не будем учитывать наличие служебной информации). Из рисунка видно, что здесь модули обмениваются информацией между собой не перегружая порты ввода/вывода. Это обеспечивается работой контроллера коммутатора, который соединяет между собой «мостами» только те порты блоков, которые участвуют во взаимном обмене информацией. Из рисунка также видно что в коммутационном ядре коммутатора трафик значительно больше, чем на каждом отдельном порту и составляет сумму всех потоков портов. Поэтому качественные IP коммутаторы имеют коммутационное ядро с пропускной способностью в десятки раз выше пропускной способности отдельного порта. И эта пропускная способность выбирается тем выше, чем больше портов обслуживает коммутатор.

На рисунке 2 показана работа такого же коммутатора, с теми же потоками, но передаваемыми в мультикастовом формате. В этом случае, так как мультикастовые потоки должны быть доступны для всех модулей, все потоки в коммутаторе суммируются и подаются на все порты коммутатора. Это приводит к быстрой перегрузке портов коммутатора и прекращению нормального его функционирования. В этом случае не спасает имеющийся значительный запас по пропускной способности коммутационного ядра, так как перегрузка происходит на уровне портов.

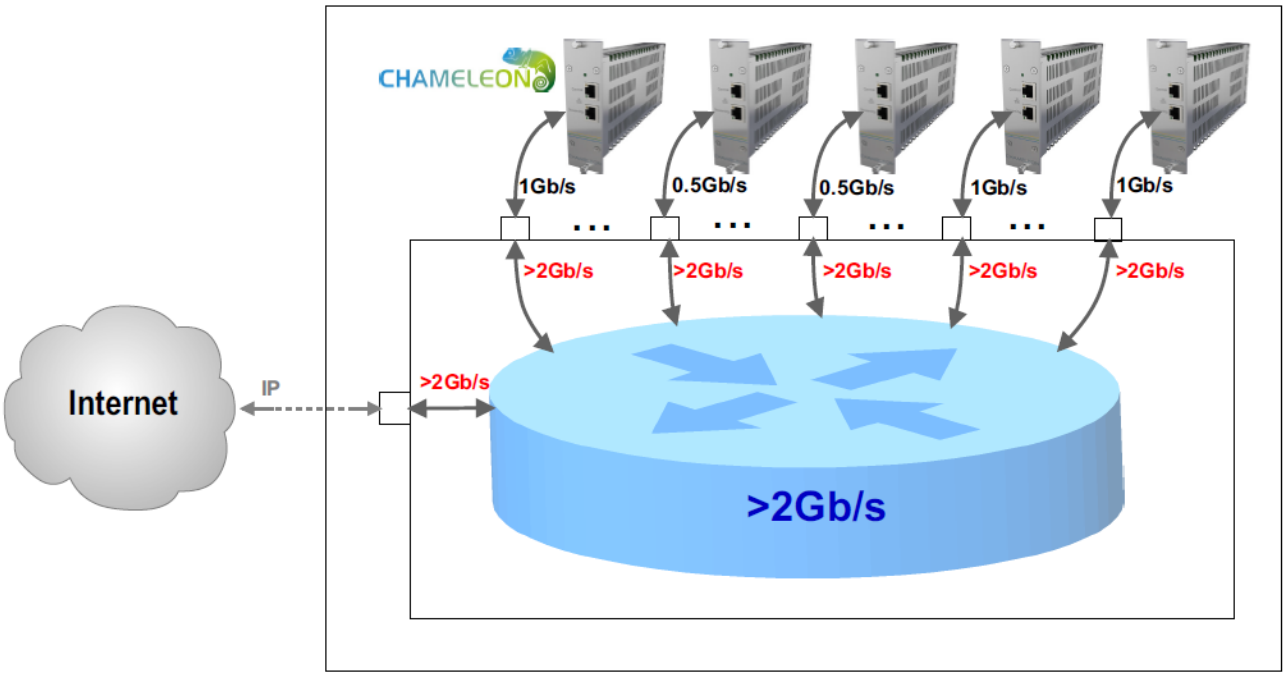


Рисунок 2. Работа неуправляемого коммутатора при передаче мультикастового трафика.

Для того чтобы решить подобные проблемы в продвинутые коммутаторы вводят специальный режим, называемый «IGMP snooping». В этом режиме коммутатор «слушает» запросы от своих внешних портов и

[1] Термин «гигабитный» относится к пропускной способности портов, а не к производительности ядра коммутатора. Производительность ядра коммутатора, как правило, значительно превышает пропускную способность портов.

направляет в них не весь, а только запрошенный ими мультикастовый трафик. Таким образом, в каждый порт направляется не весь, а только запрошенный им трафик. Работа коммутатора с подобным режимом показана на рисунке 3.

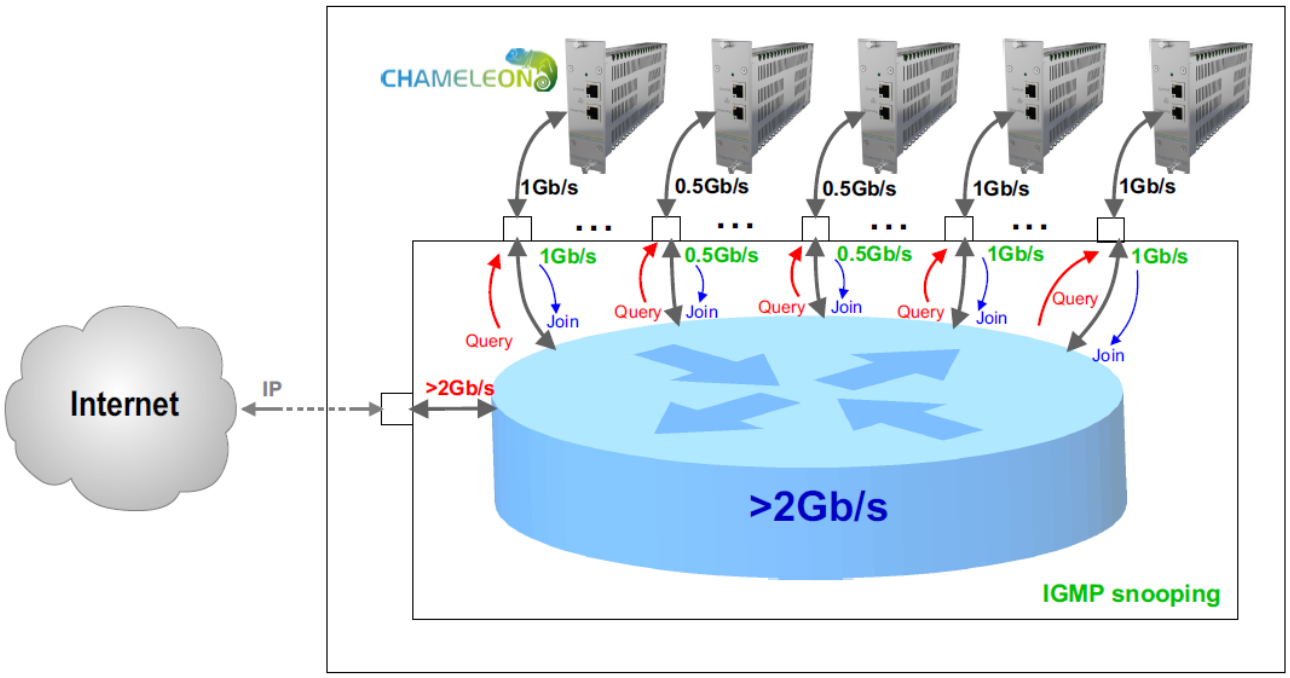


Рисунок 3. Работа коммутатора с режимом «IGMP snooping» при передаче мультикастового трафика.

Здесь контроллер коммутатора отслеживает запросы на подключение к мультикастовому потоку (Join) поступающие с каждого порта и направляет в этот порт только те мультикастовые потоки, которые были запрошены. Таким образом удается избежать перегрузки портов неиспользуемым мультикастовым трафиком. Правда на рисунке показано, что даже при использовании режима «IGMP snooping», возможна перегрузка портов, используемых для подключения станции к сети верхнего уровня, например сети Интернет. Пояснение к этой особенности будут даны далее. Для юникастового трафика коммутатор работает также как показано на рисунке 1.

Коммутаторы с «IGMP snooping» могут использоваться не только для объединения отдельных модулей станции Chameleon, но и для объединения нескольких шасси станции, например GN50, в общую головную станцию, как показано на рисунке 4. Ведь проблема перегрузки портов неуправляемым мультикастовым трафиком актуальна и на уровне объединения нескольких шасси, входящих в ГС.

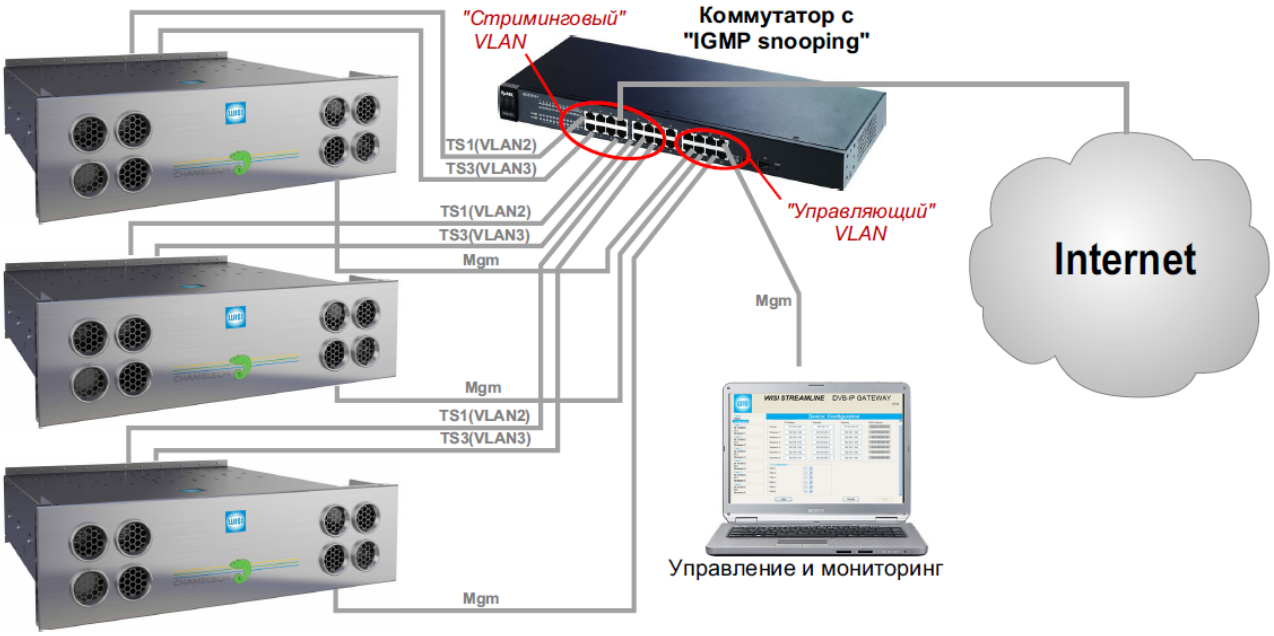


Рисунок 4. Объединение нескольких шасси GN50 в головную станцию.

Из приведенного описания и рисунков можно сделать вывод что коммутатор с поддержкой «IGMP snooping» оптимален для использования в станции с IP коммутацией.

Тестирование коммутаторов для станции Chameleon.

Для того чтобы можно было дать рекомендации по настройке и использованию подобных коммутаторов в составе станции Chameleon, было проведено тестирование IP коммутаторов с поддержкой «IGMP snooping».

Было протестировано несколько моделей гигабитных коммутаторов, поддерживающих режим «IGMP snooping»:

1. D-Link DGS-1100-8 (8 портов);
2. D-Link DGS-1210-28 (24+4 порта);
3. D-Link DGS-1500-28 (24+4 порта);
4. ZyXEL GS-1510-24 (24 порта);
5. ZyXEL (X)GS-1910-24 (24 порта).

В процессе тестирования выяснился ряд важных особенностей, которые необходимо учитывать при использовании коммутаторов в составе ГС.

Querier.

При тестировании оказалось, что без принятия специальных мер коммутаторы корректно работают в составе станции только первые 1-3 минуты после подключения, а затем блокируют передачу мультикастового трафика.

При исследовании причин этого явления выяснилось, что при включении станции подключение портов к запрошенным мультикастовым группам производится контроллером коммутатора по сигналам подключения Join поступающим от модулей при включении. Но для дальнейшего поддержания соединения коммутатору требуется получение от модуля

периодического подтверждения (Join) необходимости соединения. Для этого в IP сети используется Querier – приложение, которое периодически опрашивает модули на предмет подтверждения требуемых мультикастовых потоков. Коммутаторы D-Link DGS-1100-8 и ZyXEL GS-1510-24 такого Querier в своем составе не имеют, поэтому оказались непригодны для работы в составе ГС.

Кроме того встроенный Querier коммутатора должен уметь корректно производить процедуру арбитража при подключении к IP сети верхнего уровня. Ведь, если ГС подключается к сети верхнего уровня, то в ней, как правило, уже есть свой Querier. Чтобы избежать сетевых конфликтов в оборудовании, встроенный Querier коммутатора должен в этом случае автоматически отключиться. Из оставшихся трех коммутаторов, коммутаторы D-Link DGS-1210-28 и D-Link DGS-1500-28 не обеспечили корректной обработки мультикастового трафика[2].

При подключении ГС к IP сети верхнего уровня была отмечена и еще одна особенность. Если из порта верхней сети поступают запросы от Querier, то коммутатор автоматически назначает этот порт как Router port и открывает его для всего мультикастового трафика ядра, что может вызвать перегрузку этого порта. Для того чтобы избежать его перегрузки можно использовать, например, агрегацию портов. Но решение этих вопросов выходит за рамки данного документа.

В итоге, из исследуемых коммутаторов, с первого раза успешно прошел все тесты только коммутатор **ZyXEL** (X)**GS-1910-24**. Этот коммутатор имеет 24 медных гигабитных порта, из которых 4 могут быть заменены на четыре 1Gb SFP (GS 1910-24) или на четыре 10Gb SFP (XGS-1910-24). Есть также версия этого коммутатора на 48 портов **ZyXEL** (X)**GS-1910-48**.

Коммутатор позволяет организовать раздельные виртуальные сети (VLAN) для управления и стриминга с разными режимами передачи мультикастового трафика. Это требуется для обеспечения надежного и безопасного управления ГС.

Так как настройка коммутатора для использования его в составе ГС с IP коммутацией достаточно сложна, ниже приводится пример пошаговой настройки коммутатора (X)GS-1910-24.

[2] После контактов со службой поддержки D-Link, ПО коммутаторов было доработано и коммутаторы с версией ПО 2013 года корректно обрабатывают мультикастовый трафик.

Настройка коммутатора ZyXEL (X)GS-1910 для работы в составе ГС Chameleon и Tangram.

В данном разделе описывается порядок настройки коммутатора ZyXEL (X)GS-1910-24 для работы в составе станции Chameleon с IP коммутацией.

Наиболее эффективно использование такого коммутатора в составе станции на базе шасси GN40. Но также возможно использование данного коммутатора для объединения групп модулей в шасси GN50 или шасси GN01/GN20.

В данном примере рассматривается настройка коммутатора с начальными заводскими установками (состояние на момент поставки – IP адрес, пароль, логин и т.д.).

Перед началом настройки необходимо подключить патчкордами к коммутатору порты «Control» и «Streaming» всех модулей Chameleon и подать питание на коммутатор и модули.

Подключить управляющий компьютер к порту коммутатора в группе, предназначенной для объединения модулей Chameleon. В данном примере это порт 24 из группы портов коммутатора 16-24. Сетевую плату компьютера нужно настроить со следующими параметрами:

- **IP = 192.168.1.x** , где x – число от 2 до 254, не используемое в модулях Chameleon, подключенных к коммутатору. В данном примере настройки использован адрес 192.168.1.2
- **Netmask = 255.255.255.0**
- **Gateway = 0.0.0.0** - здесь можно указать любое значение или не указывать вовсе.
- **DNS серверы** – можно указать любое значение или не указывать вовсе.

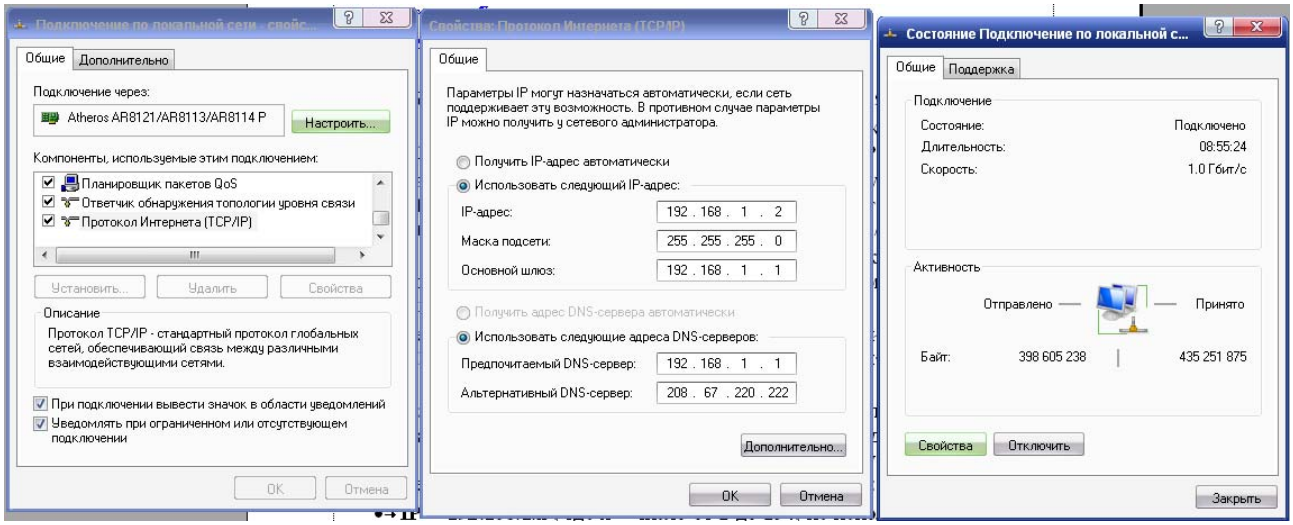


Рисунок 5.

Затем необходимо проделать следующие действия:

1. Запустить любой WEB браузер, например Mozilla Firefox, и набрать в адресной строке адрес 192.168.1.1 (адрес по умолчанию web интерфейса коммутатора). В появившемся окне набрать логин: **admin** и пароль: **1234**. После чего нажать кнопку «OK».

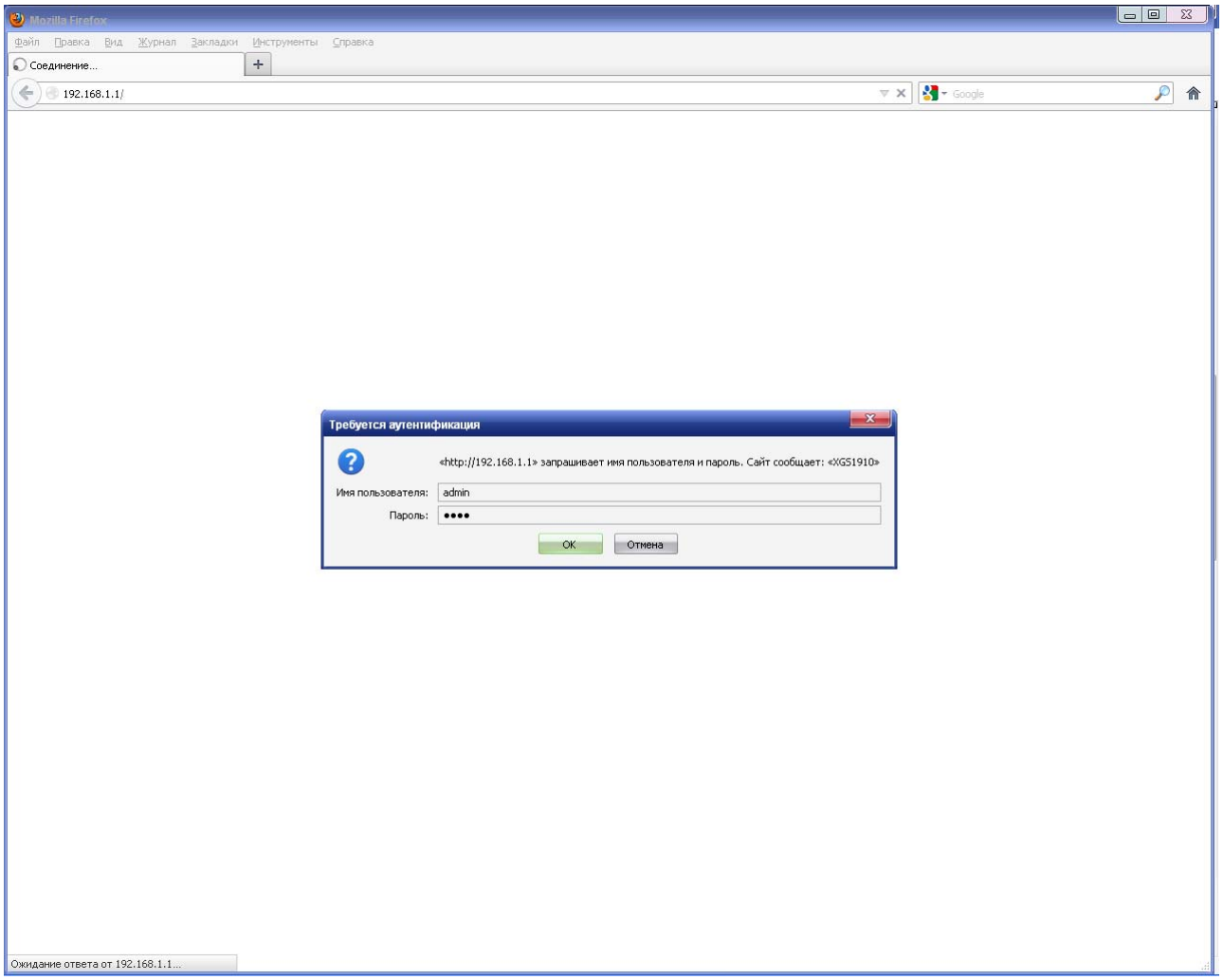


Рисунок 6.

2. В открывшемся окне пройти по пунктам меню **Configuration > IPMC > IGMP Snooping > Basic Configuration**. В открывшемся меню установить галочку в пункте «**Snooping Enabled**» и убрать в пункте «**Unknown Multicast Flooding Enabled**». Остальные пункты оставить свободными. После этого нажать на кнопку «**Apply**».

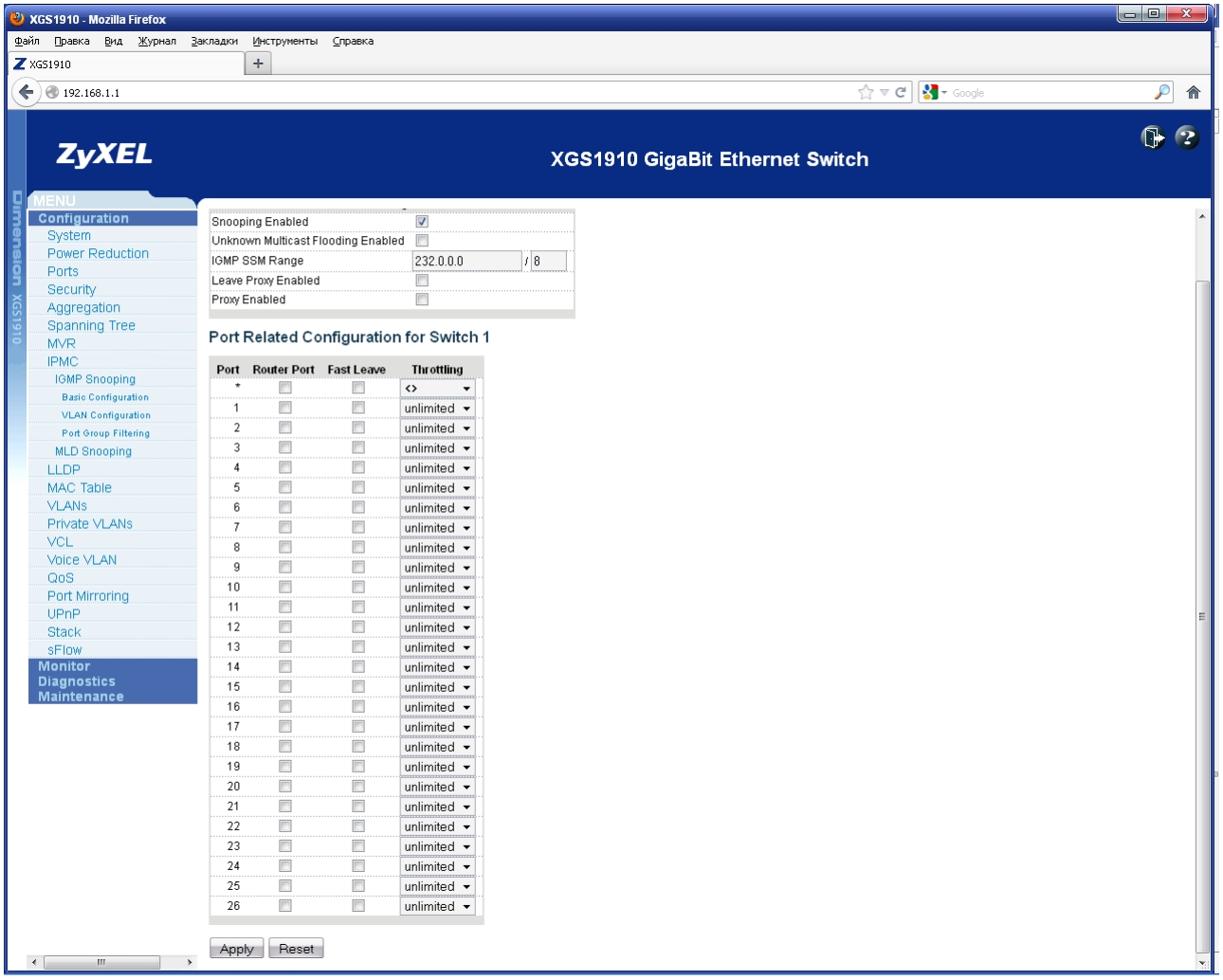


Рисунок 7.

3. После этого перейти в пункт меню «**VLAN Configuration**». В этом меню нажать на кнопку «**Add New IGMP VLAN**». В появившейся строке задать VLAN ID = 1 и поставить галочку в пунктах «**Snooping Enabled**» и «**IGMP Querier**». Значение **QI(sec)** рекомендуется уменьшить до 60 сек. После этого нажать на кнопку «**Apply**». С этого момента коммутатор работает в режиме IGMP snooping.

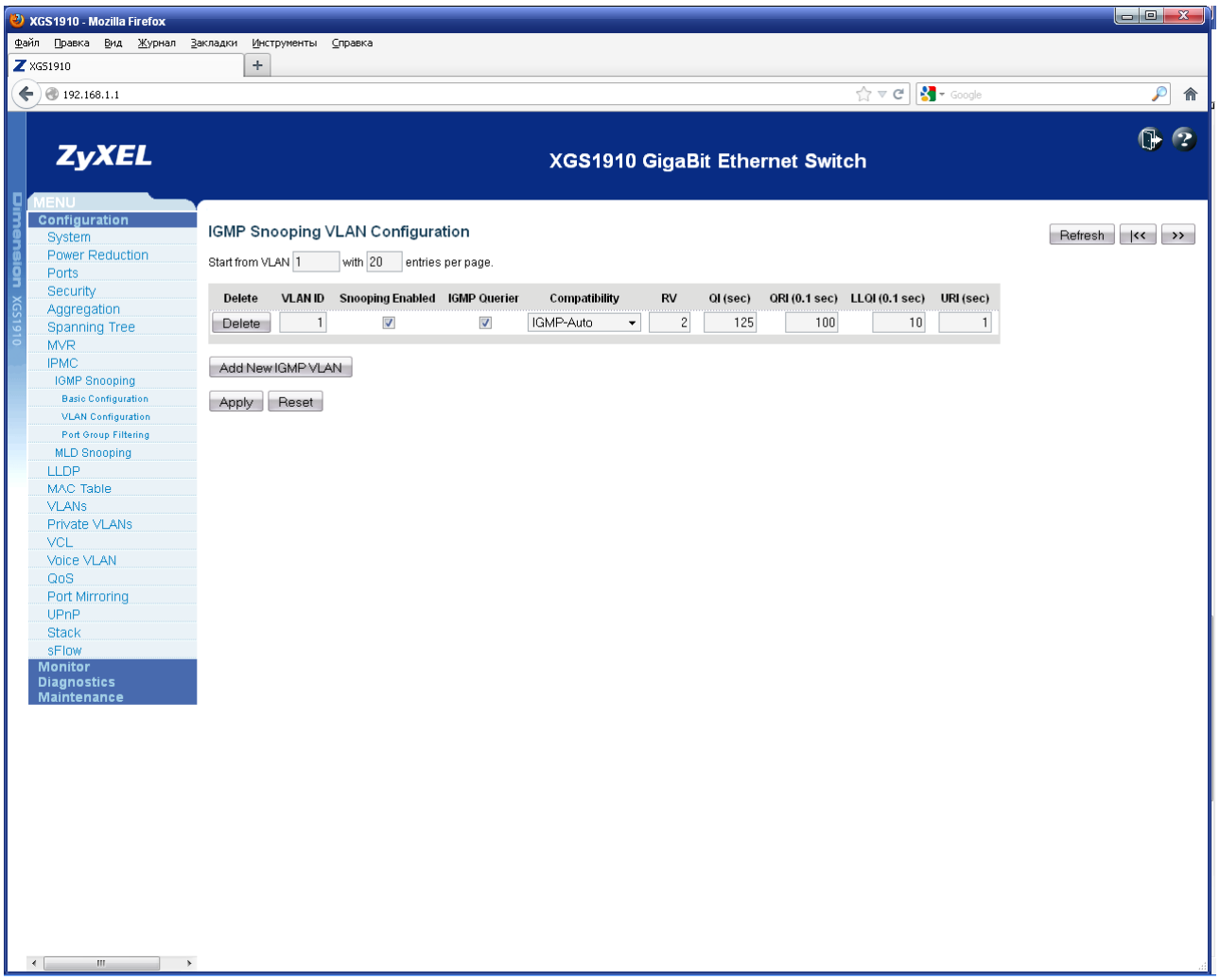


Рисунок 8.

4. Проверить функционирование IGMP snooping можно если при работающей станции в режиме мультикастового обмена зайти в пункт меню **Monitor > IPMC > IGMP Snooping > Groups Information**. В открывшемся окне вы увидите таблицу в которой отображены все мультикастовые потоки, которые имеют подписчиков и адреса портов, которые подписаны на эти группы.

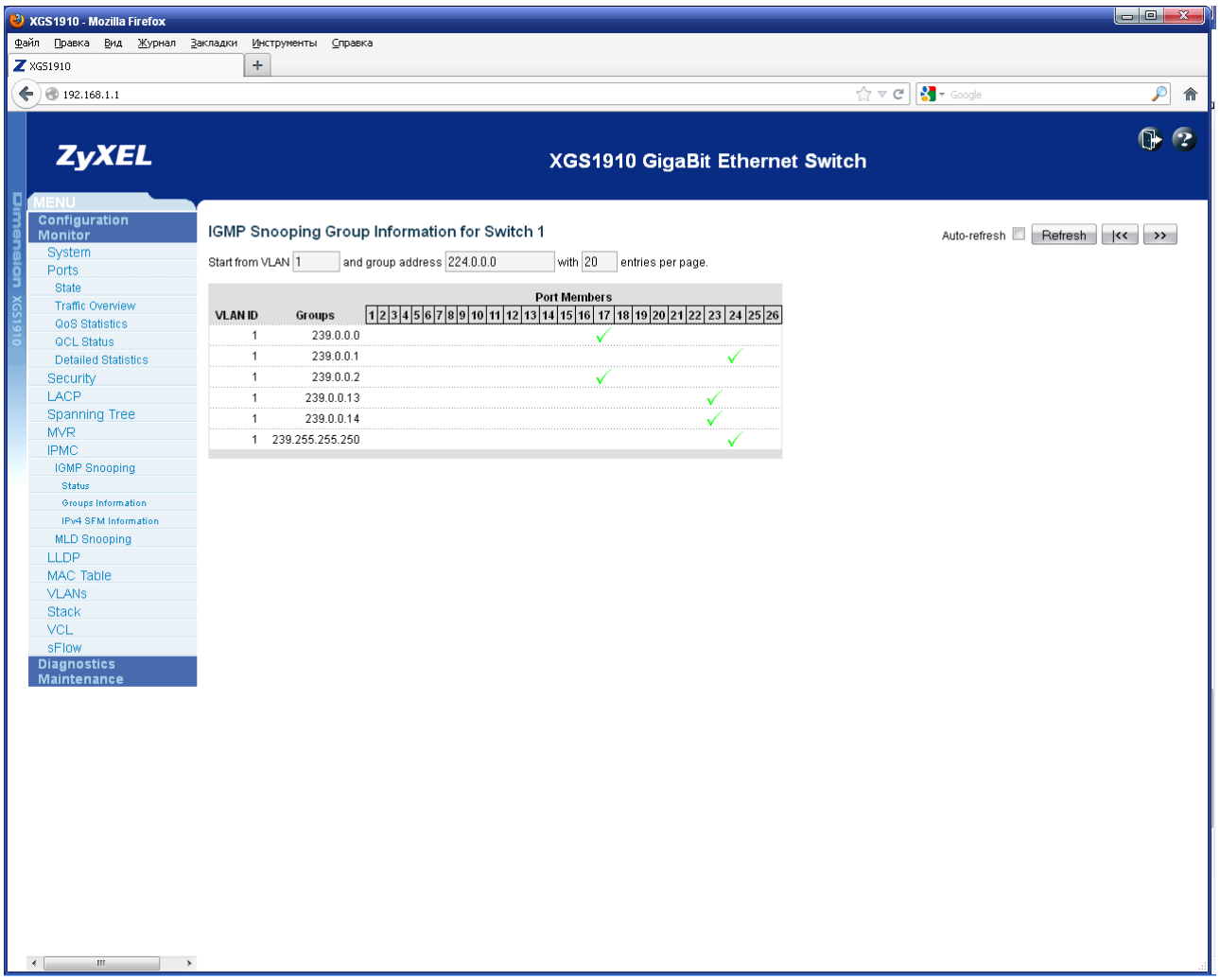
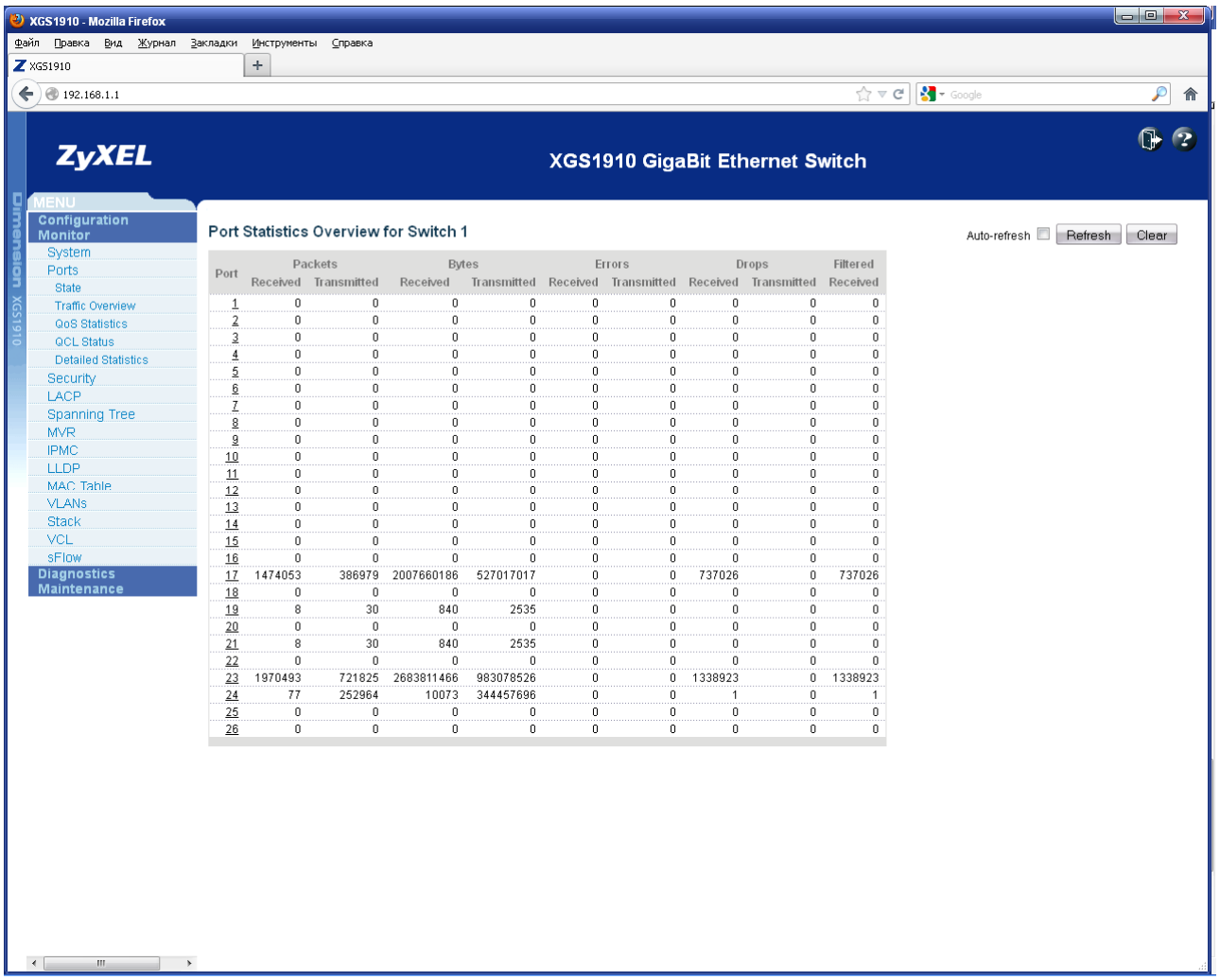


Рисунок 9.

5. Также можно проконтролировать трафик, проходящий по портам. Для этого нужно пройти по пунктам меню: **Monitor > Ports > Traffic Overview**. В открывшемся окне можно проконтролировать объем трафика прием/передача по каждому порту. В приведенном примере видно, что часть трафика не затребованного модулями отфильтровывается, трафик на портах различен и зависит от того, к каким сервисам подключен порт.



Port	Packets		Bytes		Errors		Drops		Filtered
	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received
1	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0	0	0
17	1474053	386979	2007660186	527017017	0	0	737026	0	737026
18	0	0	0	0	0	0	0	0	0
19	8	30	840	2535	0	0	0	0	0
20	0	0	0	0	0	0	0	0	0
21	8	30	840	2535	0	0	0	0	0
22	0	0	0	0	0	0	0	0	0
23	1970493	721825	2683811466	983078526	0	0	1338923	0	1338923
24	77	252964	10073	344457696	0	0	1	0	1
25	0	0	0	0	0	0	0	0	0
26	0	0	0	0	0	0	0	0	0

Рисунок 10.

Настройка VLAN в коммутаторе.

В предыдущем примере коммутатор настраивался таким образом, что все его порты, входящие по умолчанию в default VLAN с VLAN ID=1 начинали работать в режиме IGMP snooping. В реальной же станции чаще всего требуется чтобы стриминговые порты модулей Chameleon находились в отдельном от портов управления VLAN.

Для того, чтобы создать такой VLAN в коммутаторе ZyXEL (X)GS-1910-24 нужно: переключить управляющий компьютер на порт, который не войдет в создаваемый VLAN, войти в web интерфейс коммутатора и проделать следующие операции:

6. Пройти по пунктам меню: **Configuration > VLANs > VLAN Membership**. В открывшемся окне нажать на кнопку «**Add New VLAN**». В появившейся строке задать VLAN ID = 13 (можно любое другое значение от 2 до 4095), задать имя сети (в данном примере StreamingVLAN) и поставить галочки под номерами портов, которые вы хотите включить в этот VLAN (17-24 в данном примере). Эти же порты двойным щелчком мыши нужно удалить из default VLAN (VID=1). После этого нажать на кнопку «**Apply**».

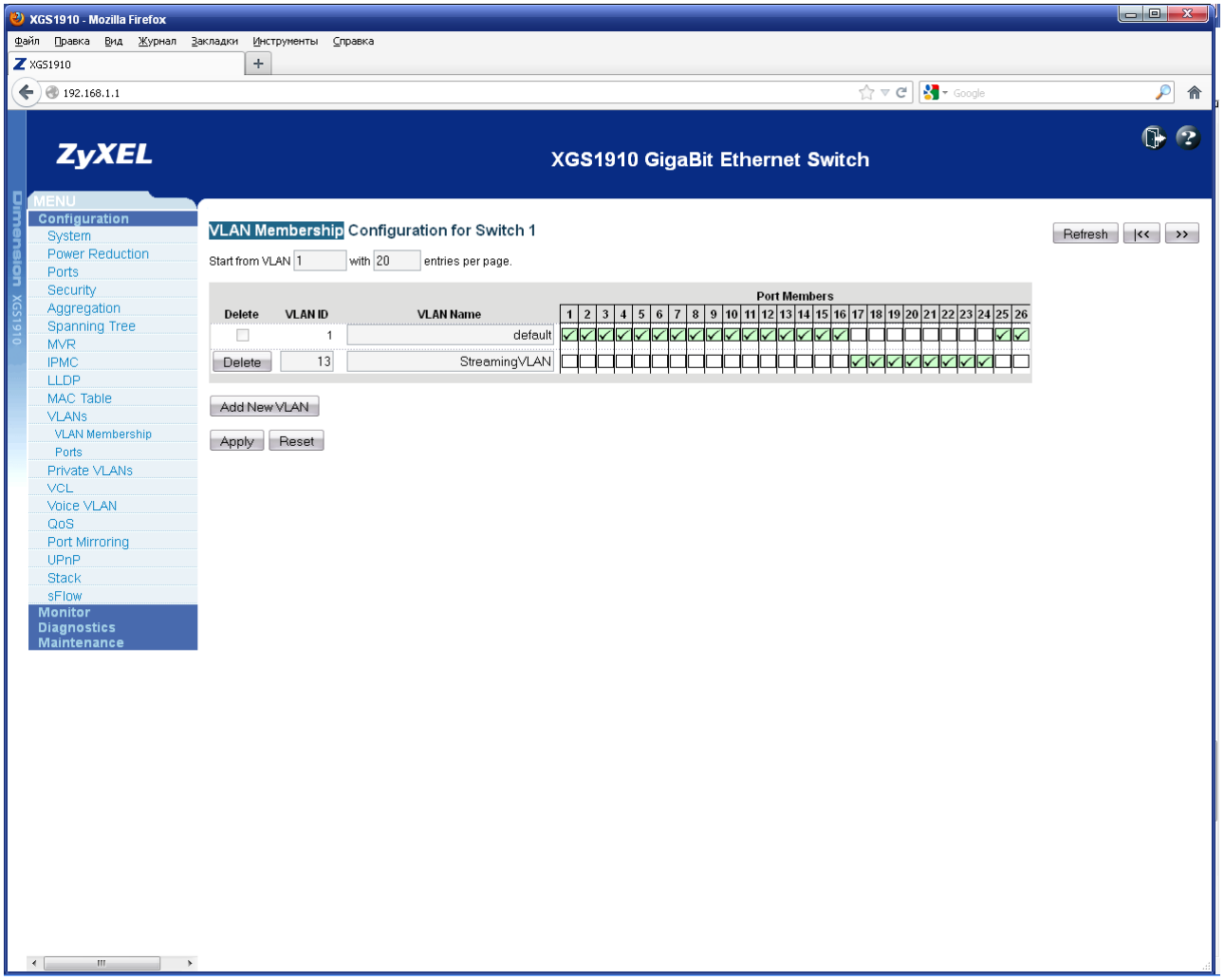


Рисунок 11.

7. Затем нужно пройти по пунктам меню: **Configuration > VLANs > Ports.** В открывшемся окне, в столбце **Tx Tag** всем портам, входящим в создаваемый VLAN, задать режим **Untag_all**, а в столбце **ID** указать значение 13 (VID создаваемого VLAN). После этого нажать на кнопку «**Apply**».

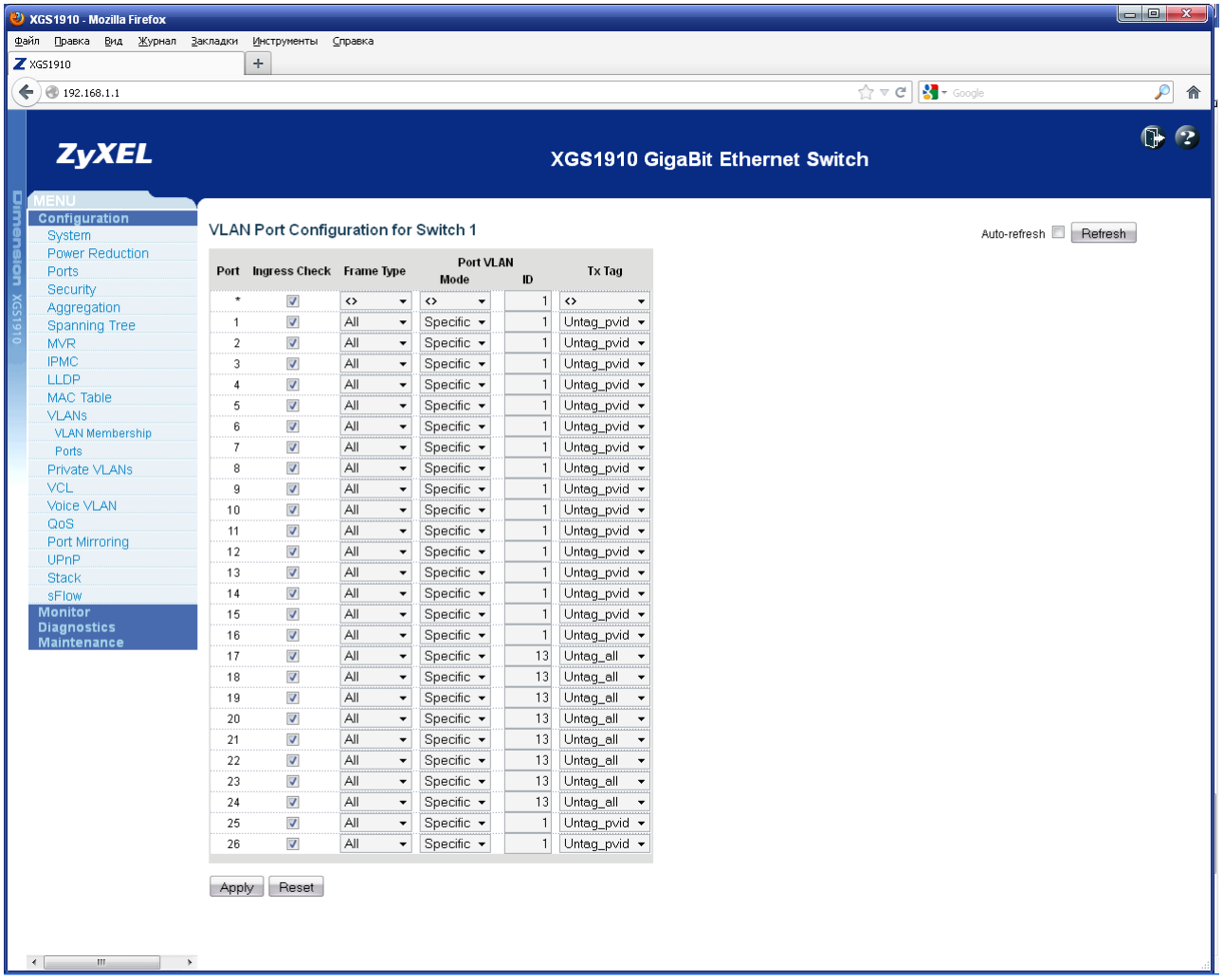


Рисунок 12.

8. После этого нужно перейти в пункт меню **Configuration > IPMC > IGMP Snooping > VLAN Configuration**. В этом меню нажать на кнопку «**Add New IGMP VLAN**». В появившейся строке задать VLAN ID = 13 и поставить галочку в пунктах «**Snooping Enabled**» и «**IGMP Querier**». Одновременно, для примера, снимите галочки в пунктах «**Snooping Enabled**» и «**IGMP Querier**» для сети с VLAN ID = 1. После этого нажмите на кнопку «**Apply**». С этого момента сеть с VLAN ID = 13 в коммутаторе функционирует как стриминговая с поддержкой режима IGMP snooping, а сеть с VLAN ID = 1 работает как простая широковещательная сеть.

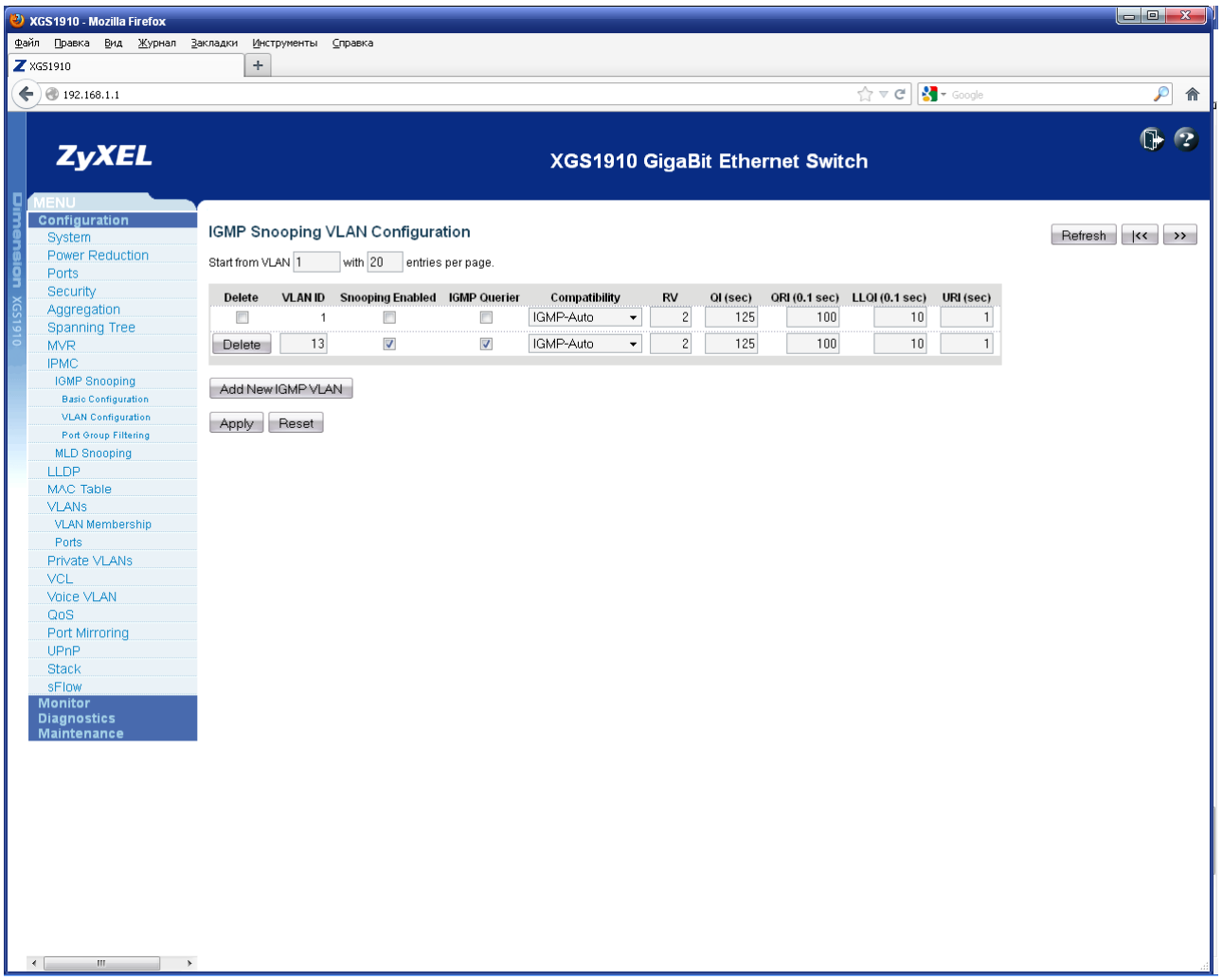


Рисунок 13.

Коммутатор позволяет создавать множество VLAN с различными параметрами, но описание этих возможностей выходит за границы данного документа. Дополнительную информацию по коммутатору и его настройке вы можете найти на сайте www.zyxel.ru .