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 почти неограниченные возможности И для формирования функционала станции. При организации информационного используется идеология «обшего котла» обмена станшии все В 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 ІР коммутатор¹. 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 портов. Поэтому качественные IP коммутаторы потоков 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.





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-1500-28 обеспечили D-Link DGS-1210-28 И не корректной обработки мультикастового трафика².

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.х**, где х 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.

 Полключение по покальной сети спойс. 2 	Свойства: Протокол Интернета (ТСРИР) 🛛 😵 🔀	🔺 Состояние Подключение по локальной с 🛛 🔋 💌
Общие Дополнительно	Общие	Общие Поддержка
Подключение через:	Параметры IP могут назначаться автоматически, если сеть поддерживает эту возможность. В противном случае параметры IP можно получить у сетевого администратора. Получить IP-адрес автоматически У Использовать следующий IP-адрес: IP-адрес: 132.188.1.2	Подключение Состояние: Подключено Длительность: 08:55:24 Скорость: 1.0 Гбит/с
К Ш К К К К К К К К К К К К К К К К К К	Маска подсети: 255.255.255.0 Основной шлюз: 192.168.1.1	Активность-
Описание Протокол TCP/IP - стандартный протокол глобальных сегей, обеспечивающий связь между различными взаимодействующими сетями.	Получать зарес UNS-сереера загонятивски Фиспользовать следующие адреса DNS-серееров: Предпочитаемый DNS-сереер: 192.168.1.1	Байт: 398 605 238 435 251 875
При подключении вывести значок в области уведомлений Уведомлять при ограниченном или отсутствующем подключении	Альтернагиеным и тоэтсереер. 208 . 67 . 220 . 222	Свойства Отключить
ОК. Отмена	ОК Отмена	Закрыть

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 б.

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».

102 168 1 1	1				A a A	
92.100.1.1					M V C	
ZvXEL					XGS1910 GigaBit Ethernet Switch	
ENU				-		
onfiguration	Snoopi	ing Enabled		V		
Dower Deduction	Unknow	wn Multicast F	looding Enable	ed 📃		
Ports	IGMP S	SSM Range		232.0.0.0		
Security	Leave	Proxy Enabled				
Aggregation	Proxy E	nabled				
Spanning Tree	_		_			
MVR	Port F	Related Co	onfiguratio	n for Switch 1		
IPMC	Dort	Pourtor Dort	EactLoar	Throttling		
IGMP Snooping	*	Router Port	rast Leave			
Basic Configuration	1			unlimited -		
VLAN Configuration				uniimited 👻		
Port Group Filtering	2			unlimited -		
MLD Snooping	3			unlimited -		
LLDP	4			unlimited 👻		
MAC Table	5			unlimited 👻		
VLANS	6			unlimited 👻		
Private VLANS	7			unlimited 👻		
VUL	8			unlimited 👻		
Oos	9			unlimited 👻		
Port Mirroring	10			unlimited 👻		
HPnP	11			unlimited 👻		
Stack	12			unlimited 👻		
sFlow	13			unlimited 👻		
lonitor	14			unlimited 👻		
iagnostics	15			unlimited 👻		
laintenance	16			unlimited 👻		
	17			unlimited 👻		
	18			unlimited 👻		
	19			unlimited 🔻		
	20			unlimited -		
	20	 		unlimited -		
	21			unlimited =		
	22			unlimited -		
	23			unimiteu 🔻		
	24			urilimitea 🔻		
	25			unilmited 🔻		
	26			unlimited 🔻		

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.

910	+ ☆▼	C Soogle	
ZyXEL	XGS1910 GigaBit Ethernet Switch		G
NU nfiguration ystem ower Reduction orts ecurity .ggregation panning Tree MC IGMP Snooping Basic Configuration PAC Coofficient MLD Snooping MLD Snoo	IGMP Snooping VLAN Configuration Start from VLAN 1 with 20 entries per page. Delete VLAN ID Snooping Enabled IGMP Querier Compatibility RV OI (sec) ORI (0.1 sec) LLOI (0.1 Delete 1 2 I GMP-Auto - 2 125 100 Add NewIGMP VLAN Apply Reset	1 sec) URI (sec) 10 1	Refresh

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.

192.168.1.1						☆ ▼ C 🚼 - Google	ß
ZyXEL				XGS1910 (GigaBit Ethernet S	witch	0
ENU onfiguration onitor System	IGMP Sno		Ip Information for Switc	h 1 with 20 entrie	s per page	Auto-refresh 🔲 Ref	fresh I<< >>
Ports State Traffic Overview QoS Statistics	VLAN ID	Groups 239.0.0.0	123456789101112	Port Members 13 14 15 16 17 18 19	20 21 22 23 24 25 26		
Detailed Statistics Security ACP	1	239.0.0.1 239.0.0.2 239.0.0.13	P	~			
AVR PMC IGMP Snooping	1 2	239.0.0.14 39.255.255.250	1		······		
Groups Information IPv4 SFM Information MLD Snooping							
AC Table /LANs Stack							
/CL Flow agnostics aintenance							

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.

Packets Packets 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	for Switch 1 Byth Received 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	es Transmitted 0 0 0 0 0 0	XGS1910 Errors Received Trar 0 0 0	Gigal Ismitted	Drops Received Transm 0	nitted	itch Filtered Received	Auto-refresh 🗌 Refresh Cle
Packets Packets ecceived Transmitted 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	for Switch 1 Byte Received 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	es Transmitted 0 0 0 0 0 0	Errors Received Trai 0 0 0	asmitted O O O	Drops Received Transn 0 0	nitted O O	Filtered Received	Auto-refresh 🗌 Refresh Cle
Packets Packets @ 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	For Switch 1 Byte Received 0 0 0 0 0 0 0 0	es Transmitted O O O O O	Errors Received Tran 0 0 0	ismitted O O	Drops Received Transn 0	nitted O O	Filtered Received	Auto-refresh 🗌 Refresh Cle
Packets aceived Transmitted 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Byte Received 0 0 0 0 0 0 0 0 0	es Transmitted O O O O O	Errors Received Tran 0 0 0 0	nsmitted O O	Drops Received Transm 0 0	nitted O O	Filtered Received	
acceived Transmitted 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Received 0 0 0 0 0 0 0 0 0 0	Transmitted 0 0 0 0 0	Received Tran	ismitted O O O	Received Transn 0 0	nitted O O	Received O	
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0		0 0 0 0	0 0 0 0	0 0 0	0	0	0	
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	0 0 0 0 0 0	0 0 0 0	0 0 0	0	0	0	0	
0 0 0 0 0 0 0 0 0 0 0 0 0 0	0 0 0 0	0 0 0	0	0			0	
0 0 0 0 0 0 0 0 0 0	0 0 0 0	0	0		0	0	0	
0 0 0 0 0 0 0 0	U 0 0	U.	~	0	0	0	0	
0 0 0 0			U 0	U 0	U 0	U	U	
0 0		0	0		0	0	0	
	0	0	0	Ŭ	0	Ű	0	
0 0	0	0	0	0	0	0	0	
0 0	0	0	0	0	0	0	0	
0 0	0	0	0	0	0	0	0	
0 0	0	0	0	0	0	0	0	
0 0	0	0	0	0	0	0	0	
U U	U 0	U 0	U 0	U 0	U 0	0	0	
0 0		0	0 0	0	0	0	0	
474053 386979	2007660186	527017017	0		737026	Ű	737026	
0 0	0	0	0	0	0	0	0	
8 30	840	2535	0	0	0	0	0	
0 0	0	0	0	0	0	0	0	
8 30	840	2535	0	0	0	0	0	
0 0	0	0	0	0	0	0	0	
970493 721825 77 252064	∠083811466 10073	9830/8526	U 0	U	1338923	U	1338923	
n 2J2904	10073 N	0807544457090 N	0	0		0	0	
0 0		0	Ŭ	Ŭ	Ŭ	Ŭ	Ŭ	
	0 0 0 0 0 0 474053 386979 0 0 8 300 0 0 970493 721825 77 252964 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0 0 0 0 0 474053 386079 2007660186 0 0 0 0 8 30 840 0 0 0 0 970493 771825 2683811466 0 0 0 0 0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 474053 386979 2007660186 527017017 0 0 0 0 0 8 30 840 2535 0 0 0 0 970493 721825 2683811466 983078526 77 252964 10073 344457696 0 0 0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 474053 386979 2007660186 527017017 0	0 0	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 474053 386979 2007660186 527017017 0 0 77026 0 0 0 0 0 0 0 0 8 30 840 2535 0 0 0 0 9 0 0 0 0 0 0 0 0 970493 721825 2683811466 983078526 0 0 1338923 77 252964 10073 344457696 0 0 0 0 0 0 0 0 0 0 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».

ZyXEL					2	XGS1910 G	gaBit Ethernet S	witch	
U figuration stem	VLAN	l Port Config	juration fo	r Switch 1				Auto-refresh 🗐	Refresh
wer Reduction rts	Port	Ingress Check	Frame Type	Port VL Mode	AN ID	Tx Tag			
curity areastion	*	V	<u>ه</u>	<> ▼	1	↔ –			
anning Tree	1	V	All 🗸	Specific 👻	1	Untag_pvid 👻			
R	2	V	All 🗸	Specific -	1	Untag_pvid 👻			
С	3	V	All 🗸	Specific -	1	Untag pvid 👻			
P	4		All	Specific -	1	Untag pvid 👻			
C Table	5		All •	Specific •	1	Untag pvid 💌			
Ns				Specific -	1	Unteg pvid -			
AN Membership	7			Specific -		Unter puid -			
rts		X	All	Specific •		Unter mid			
ate VLANs	8		All	Specific -		Untag_pvid +			
- 	9	V	All 🔻	Specific -	1	Untag_pvid 👻			
	10	V	All 🖣	Specific -	1	Untag_pvid 👻			
, Mirrorina	11	V	All 🖣	Specific 🔻	1	Untag_pvid 👻			
P	12	V	All 🔻	Specific 🔻	1	Untag_pvid 👻			
:k	13	V	All 🖣	Specific 👻	1	Untag_pvid 👻			
)W	14	V	All 🖣	Specific 👻	1	Untag_pvid 👻			
tor	15		All 🖣	Specific 👻	1	Untag_pvid 👻			
10STICS tenance	16	V	All 🖣	Specific 👻	1	Untag_pvid 👻			
centanioe	17	V	All 🔻	Specific 👻	13	Untag_all 👻			
	18	V	All 🗸	Specific 👻	13	Untag_all 👻			
	19	V	All 🔻	Specific -	13	Untag_all 👻			
	20		All 🗸	Specific -	13	Untag_all 👻			
	21	<u> </u>	All 🖣	Specific -	13	Untag all 👻			
	22		All 🔻	Specific -	13	Untag all 🔻			
	22		All	Specific -	13	Untag all 👻			
	23		ΔII -	Specific -	13	Untag_all -			
	24		All -	Specific -	1.1	Unteg pyid -			
	20	X		Specific -		Untag_pviu •			
	26	V	All	specific -		Untag_pvia ▼			

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.

ZyXEL IENU Configuration		XGS1910 GigaBit Eth	ernet Switch	•
/ENU Configuration				
System Power Reduction S	IGMP Snooping VLAN Configuration Start from VLAN 1 with 20 entries per pag	je.		Refresh I<<
Security Aggregation Spanning Tree MVR IPMC ICMP Snooping Basic Configuration VLAN Configuration Prot Group Filtering MLD Snooping LLDP MAC Table VLANS VLAN Membership Prots Private VLANS VCL Voice VLAN QoS Pott Mirroring Unco	Delete VLAN ID Snooping Enabled IGMP (1 Delete 13 Add New IGMP VLAN Apply Reset	Ouerier Compatibility RV OI (sec) □ IGMP-Auto	ORI (0.1 sec) LLOI (0.1 sec) URI (sec) 5 100 10 1 5 100 10 1 5 100 10 1	
UPnP Stack sFlow Monitor Diagnostics Maintenance				

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 <u>www.zyxel.ru</u>.