

А. А. Кязымов¹, А. А. Терешонок¹¹ ФГАОУ ВО «Российский государственный университет нефти и газа (НИУ) имени И. М. Губкина», Москва, Россия**ЭКСПЕРИМЕНТАЛЬНЫЙ АНАЛИЗ УЯЗВИМОСТЕЙ IGMPV2 И СРАВНИТЕЛЬНАЯ ОЦЕНКА МЕТОДОВ ЗАЩИТЫ НА L2+ КОММУТАТОРАХ РАЗЛИЧНЫХ ВЕНДОРОВ**

Аннотация. Работа посвящена экспериментальному анализу атаки поддельным сообщением IGMP Leave и способов защиты multicast-групп на коммутаторах Cisco Catalyst 2960, Eltex MES1428 и MikroTik CRS326. В статье описаны базовые принципы IGMPv2 и IGMP snooping, которые позволяют коммутатору поддерживать сведения о подписчиках и направлять multicast-трафик на нужные порты. В эксперименте измерялось время удаления порта клиента из таблицы группы после получения Leave-сообщения: для Cisco указано около 2–3 с, для Eltex — менее 1 с, для MikroTik — около 10 с. Далее авторы рассматривают статическую привязку multicast-группы к порту, ограничение числа групп, фильтрацию IGMP ACL и настройку Last Member Query Interval и Count. В таблице приведены наблюдаемые интервалы реакции для нескольких сочетаний таймера и количества запросов; эти данные показывают компромисс между скоростью удаления подписчика и устойчивостью к ложным сообщениям. Статья отдельно отмечает эксплуатационные ограничения статических привязок и обсуждает переход к IGMPv3. Результаты относятся к трем проверенным моделям и указанным параметрам стенда, поэтому не описывают все реализации протокола. Материал формулирует практические варианты снижения риска потери multicast-доставки и подчеркивает необходимость проверять настройки на используемой модели коммутатора. Оценка отражает описанный стенд и выбранные значения таймеров, а не полный набор реализаций IGMP snooping. Результаты ограничены описанной лабораторной конфигурацией. Адреса группы в статической команде и иллюстрирующем выводе различаются, поэтому показанный вывод не подтверждает результат именно этой команды.

Ключевые слова: IGMPv2, IGMP snooping, multicast, L2+ коммутаторы, сетевая безопасность, атака, защита.

Введение

С развитием технологий групповой передачи данных, таких как IP-телевидение, видеоконференции, онлайн-трансляции и системы оповещения, возрастают требования к эффективности и безопасности доставки трафика множеству получателей. Протокол IGMP версии 2, описанный в RFC 2236 [1], является основным протоколом управления членством в multicast-группах в сетях IPv4. Однако его архитектура, разработанная в эпоху доверительных сетей, содержит ряд уязвимостей, позволяющих злоумышленнику нарушать доступность сервисов или перехватывать трафик. Особую актуальность вопросы защиты IGMPv2 приобретают на L2+ устройствах – коммутаторах, поддерживающих функции уровня 2 и расширенные возможности уровня 3, такие как IGMP snooping. IGMP snooping позволяет коммутатору анализировать IGMP-сообщения и оптимизировать рассылку multicast-трафика только на те порты, где есть подписчики, что снижает нагрузку на сеть. Однако само наличие механизма анализа создаёт поверхность для атак: злоумышленник в том же широковещательном домене может отправлять поддельные IGMP-пакеты, заставляя коммутатор исключать легитимных получателей из группы и тем самым нарушая доставку данных.

Проблема защиты IGMPv2 на L2+ устройствах становится особенно важной в корпоративных и провайдерских сетях, где multicast-сервисы играют критическую роль, а безопасность должна обеспечиваться без существенного усложнения конфигурации и потери производительности. Несмотря на наличие версии IGMPv3 с поддержкой фильтрации multicast-источников, значительная часть оборудования до сих пор эксплуатируется с поддержкой IGMPv2, а многие приложения ориентированы именно на эту версию протокола. Поэтому исследование уязвимостей и разработка методов защиты актуальны как для теоретического изучения, так и для практического применения в реальных условиях, что подтверждается современными разработками в области передачи multicast-трафика [2] и обзорами атак на канальном уровне [3].

Объект исследования: сетевые инфраструктуры, использующие multicast-трафик и L2+

коммутаторы с поддержкой IGMP snooping.

Предмет исследования: методы защиты от атак, основанных на подделке управляющих сообщений IGMPv2, включая подмену IGMP Leave и IGMP Report.

Цель исследования: анализ уязвимостей протокола IGMPv2 на L2+ устройствах, экспериментальная демонстрация атаки и разработка рекомендаций по обеспечению безопасности multicast-трафика.

Теоретические основы IGMPv2 и IGMP snooping

RFC 2236 (IGMPv2)

Стандарт RFC 2236 [1] определяет версию 2 протокола IGMP, используемую для управления групповой рассылкой в IPv4-сетях. Он описывает три типа сообщений: Membership Query, Membership Report и Leave Group. Уязвимость протокола заключается в отсутствии механизмов аутентификации и проверки подлинности источника: любой узел в сегменте L2 может отправить поддельное сообщение от имени другого узла, что приводит к несанкционированному изменению состояния multicast-подписок.

RFC 4541 (IGMP Snooping)

Документ RFC 4541 [4] описывает рекомендации по реализации IGMP snooping в коммутаторах. Эта технология позволяет L2-устройствам перехватывать IGMP-пакеты между хостами и маршрутизаторами и на их основе строить таблицы, чтобы multicast-трафик доставлялся только заинтересованным портам. В RFC 4541 также рассматриваются вопросы безопасности, в частности, необходимость защиты от поддельных сообщений, однако конкретные механизмы защиты оставлены на усмотрение производителей. Это приводит к различиям в реализации и потенциальным уязвимостям.

Механизмы защиты на L2+ устройствах

Современные L2+ коммутаторы поддерживают различные настройки управления multicast-трафиком. В руководствах Cisco [5], Eltex [6] и MikroTik [7] описаны статические привязки multicast-групп к портам, параметры IGMP snooping, Immediate-leave и фильтрация групп. IGMPv3 поддерживает фильтрацию по источникам, включая Source-Specific Multicast, но не обеспечивает самостоятельную аутентификацию отправителя IGMP-сообщения [8]. Эффективность перечисленных мер зависит от модели и конфигурации; в данной статье экспериментально проверялась атака поддельным IGMP Leave в сценарии IGMPv2.

Multicast-группы и IGMP-технологии

Multicast-группой называется логическое объединение сетевых узлов, заинтересованных в получении одного и того же потока данных. Трафик, направляемый на групповой адрес, доставляется только тем устройствам, которые явно выразили желание его получать с помощью протокола IGMP. В отличие от широковещательной рассылки, multicast позволяет экономить пропускную способность и ресурсы конечных узлов, так как пакеты копируются только на те порты коммутатора, за которыми есть подписчики. Это достигается благодаря технологии IGMP snooping, реализуемой на L2+ коммутаторах. Коммутатор анализирует IGMP-сообщения, перехватывая их между хостом и маршрутизатором, и на основе этой информации строит таблицу пересылки multicast-трафика. Таким образом, кадры для определённой группы направляются только в порты, где имеются активные получатели, что существенно снижает нагрузку на сеть и повышает её производительность.

Применение IGMP snooping даёт следующие преимущества:

1. Гибкость развёртывания multicast-сервисов — получатели могут находиться в любом месте сети, независимо от физического расположения, и получать необходимый трафик без необходимости статической настройки.
2. Оптимизация трафика — multicast-пакеты не рассылаются во все порты, а доставляются только подписчикам, что экономит полосу пропускания и уменьшает нагрузку на оборудование.
3. Ограничение распространения трафика — IGMP snooping направляет multicast-поток на порты, где зарегистрированы подписчики. Сам по себе этот механизм не аутентифицирует отправителей IGMP-сообщений; для контроля доступа требуются

дополнительные средства защиты.

Диапазоны multicast-адресов

Адресное пространство IPv4 для multicast определено в диапазоне 224.0.0.0/4. Внутри него выделяются несколько поддиапазонов:

1. Локальные адреса используются для протоколов маршрутизации и управления сетью. Пакеты с такими адресами не должны пересылаться за пределы локального сегмента.
2. Глобальные адреса могут использоваться для любых multicast-приложений в масштабах сети или интернета.
3. Административно-ограниченные предназначены для использования внутри домена или организации, аналогично частным IP-адресам. Именно из этого диапазона часто выбираются адреса для корпоративных multicast-сервисов.

Порты коммутатора в контексте IGMP snooping

В зависимости от роли в multicast-рассылке порты L2+ коммутатора можно классифицировать следующим образом:

1. Порты, подключенные к multicast-маршрутизаторам — на них коммутатор ожидает IGMP-запросы и пересылает multicast-трафик от источников. Такие порты могут быть определены статически администратором или динамически обнаружены при получении IGMP-запросов.
2. Порты, подключенные к получателям — на них подключены хосты, отправившие IGMP-отчёты о присоединении к группе. Коммутатор пересылает трафик группы только на эти порты.
3. Порты с включённым IGMP filtering — административно ограничивается максимальное количество групп, к которым может присоединиться узел за портом, или блокируются определённые группы. Это эффективный фактор защиты от атак исчерпания ресурсов.
4. Статические multicast-группы — администратор может вручную привязать multicast-группу к порту, что гарантирует доставку трафика даже при отсутствии IGMP-отчётов и исключает влияние поддельных Leave-сообщений.

Поведение по умолчанию (без IGMP snooping)

Если на коммутаторе не включён IGMP snooping, multicast-трафик обрабатывается как широковещательный: кадры, направленные на групповой MAC-адрес, рассылаются во все порты VLAN, за исключением порта, с которого они пришли. Это приводит к неоправданной загрузке сети и создаёт угрозу перехвата данных — любой узел в том же VLAN может принимать multicast-потoki, даже не подписываясь на них. Включение IGMP snooping переводит коммутатор в режим интеллектуальной фильтрации, что не только повышает эффективность, но и создаёт основу для внедрения политик безопасности.

Атаки на протокол IGMPv2

1. Подделка IGMP Leave. Данная атака заключается в отправке поддельного сообщения о выходе из группы от имени легитимного клиента. Коммутатор с включённым IGMP snooping, получив такой пакет, может исключить порт жертвы из списка получателей multicast-трафика, что приведёт к прекращению доставки потока. Успех атаки зависит от наличия активного IGMP Querier и настроек таймеров. При использовании функции Immediate-leave порт удаляется немедленно, что делает атаку особенно эффективной.
2. Подделка IGMP Report. Злоумышленник может отправлять ложные отчёты о присоединении к группе, заставляя коммутатор пересылать multicast-трафик на свой порт. Это позволяет несанкционированно получать данные, а также создавать нагрузку на сеть, имитируя множество подписчиков. В некоторых случаях можно подменить Report таким образом, чтобы "перехватить" поток, заставив коммутатор исключить других получателей.
3. Атака на IGMP Querier. Если в сети отсутствует легитимный Querier или его роль может быть перехвачена, злоумышленник может начать отправлять свои Query-пакеты, становясь фактически управляющим устройством. Это позволяет манипулировать процессом опроса и, например, преждевременно удалять клиентов из групп. На

большинстве L2+ коммутаторов выбор Queriera осуществляется на основе наименьшего IP-адреса, что создаёт возможность для перехвата роли при наличии доступа к сети.

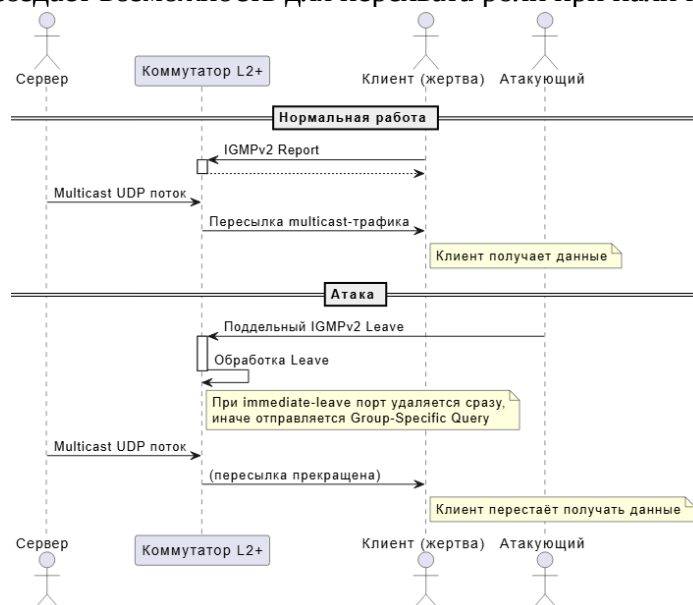


Рис. 1. Схема атаки с поддельным сообщением IGMP Leave

Материалы и методы

Проверка поддельного IGMP Leave на Cisco Catalyst 2960

Гипотеза эксперимента

Если на L2+ коммутаторе с включённым IGMP snooping не применены дополнительные факторы защиты, злоумышленник, находящийся в том же VLAN, может отправить поддельное IGMP Leave-сообщение от имени легитимного клиента и временно или полностью прекратить доставку multicast-трафика этому клиенту.

Условия проведения эксперимента:

Все эксперименты проводились в изолированном лабораторном стенде, исключая влияние фонового трафика. Коммутатор и устройства (сервер, клиент, атакующий) были соединены напрямую патч-кордами, без использования промежуточных коммутаторов или маршрутизаторов. Электропитание оборудования осуществлялось через стабилизаторы напряжения для исключения сбоев, связанных с нестабильностью питания. Дополнительный сетевой трафик отсутствовал, все неиспользуемые порты коммутатора были отключены.

Методика эксперимента:

1. К коммутатору подключаются три ПК: сервер, клиент и атакующий.
2. На коммутаторе включается IGMP snooping, настраивается IGMP Querier и статический mrouter-порт для сервера. Клиент подписывается на группу динамически.
3. Запускается multicast-поток с сервера, клиент подписывается на группу с помощью IGMP-отчёта.
4. На клиенте наблюдалось непрерывное воспроизведение видео, подтверждающее успешную подписку на multicast-группу.
5. Производится захват трафика с помощью Wireshark на ПК атакующего.
6. Атакующий запускает Python-скрипт, отправляющий IGMP Leave-пакет от имени клиента.
7. Сразу после отправки поддельного IGMP Leave-пакета воспроизведение видео на клиенте прервалось, что свидетельствует о нарушении доставки трафика.
8. Анализируется изменение состояния multicast-подписки на коммутаторе и прекращение приёма потока на клиенте.

Порядок эксперимента:

Используется коммутатор Cisco Catalyst 2960 Series с заводскими настройками, на котором предварительно активирован IGMP snooping для VLAN 1, назначен IP-адрес

интерфейсу VLAN 1 для выполнения роли IGMP Querier, а порт сервера статически определён как mrouter-порт (руководство по настройке [5]). ПК сервера имеет IP-адрес 10.10.10.1, клиента – 10.10.10.2, атакующего – 10.10.10.3. Все ПК подключены к портам коммутатора Fa0/11, Fa0/15 и Fa0/17 соответственно.

Перед началом атаки проверяется наличие динамической подписки клиента. Для этого на клиенте запускается скрипт-приёмник multicast, который отправляет IGMPv2 Report и начинает принимать поток. На коммутаторе команда show ip igmp snooping groups отображает группу 239.255.255.250 с портами Fa0/11 и Fa0/15. Захват трафика в Wireshark на атакующем ПК показывает IGMP-отчёты и UDP-пакеты потока.

Листинг 1 – Таблица IGMP-групп на коммутаторе до начала атаки

Vlan	Group	Type	Version	Port List
----	-----	----	-----	-----
1	239.255.255.250	igmp	v2	Fa0/11, Fa0/15

Далее атакующий запускает скрипт igmp_attack_work.py, который отправляет IGMP Leave-пакет от имени клиента.

Сразу после отправки пакета на коммутаторе выполняется повторная проверка таблицы групп. Порт клиента Fa0/15 исчезает из списка получателей, что подтверждает успешную обработку Leave-сообщения.

No.	Time	Source	Destination	Protocol	Length	Info
27471	294.215979675	Cisco_35:57:83	Nearest-Customer-Br...	STP	68	Conf. Root = 32768/10/24:01:c7:35:5...
27472	296.216506093	Cisco_35:57:83	Nearest-Customer-Br...	STP	68	Conf. Root = 32768/10/24:01:c7:35:5...
27473	297.489492599	10.10.10.2	224.0.0.2	IGMPv2	42	Leave Group 239.255.255.250
27474	298.222149100	Cisco_35:57:83	Nearest-Customer-Br...	STP	68	Conf. Root = 32768/10/24:01:c7:35:5...
27475	300.230010447	Cisco_35:57:83	Nearest-Customer-Br...	STP	68	Conf. Root = 32768/10/24:01:c7:35:5...
27476	302.235248360	Cisco_35:57:83	Nearest-Customer-Br...	STP	68	Conf. Root = 32768/10/24:01:c7:35:5...
27477	303.912730131	Cisco_35:57:83	Cisco_35:57:83	LOOP	60	Reply
27478	304.240242947	Cisco_35:57:83	Nearest-Customer-Br...	STP	68	Conf. Root = 32768/10/24:01:c7:35:5...
27479	306.247558761	Cisco_35:57:83	Nearest-Customer-Br...	STP	68	Conf. Root = 32768/10/24:01:c7:35:5...
27480	308.253024463	Cisco_35:57:83	Nearest-Customer-Br...	STP	68	Conf. Root = 32768/10/24:01:c7:35:5...
27481	310.262260146	Cisco_35:57:83	Nearest-Customer-Br...	STP	68	Conf. Root = 32768/10/24:01:c7:35:5...
27482	312.268011193	Cisco_35:57:83	Nearest-Customer-Br...	STP	68	Conf. Root = 32768/10/24:01:c7:35:5...
27483	313.925664884	Cisco_35:57:83	Cisco_35:57:83	LOOP	60	Reply
27484	315.000000000	Cisco_35:57:83	Nearest-Customer-Br...	STP	68	Conf. Root = 32768/10/24:01:c7:35:5...

No.	Time	Source	Destination	Protocol	Length	Info
27473	297.489492599	10.10.10.2	224.0.0.2	IGMPv2	42	Leave Group 239.255.255.250

No.	Time	Source	Destination	Protocol	Length	Info
27473	297.489492599	10.10.10.2	224.0.0.2	IGMPv2	42	Leave Group 239.255.255.250

Рис. 2. Захват пакета IGMPv2 в Wireshark

Листинг 2 – Таблица IGMP-групп после атаки

```
Switch#show ip igmp snooping groups
```

Vlan	Group	Type	Version	Port List
----	-----	----	-----	-----
1	239.255.255.250	igmp	v2	Fa0/11

Switch#

На стороне клиента приём UDP-пакетов, имитирующих видеопоток, прекращается, что свидетельствует о нарушении доставки multicast-трафика. Через некоторое время подписка может восстановиться, однако сам факт успешного временного отключения демонстрирует уязвимость протокола.

В испытанном стенде с IGMP snooping и активным Querier отправка поддельного IGMPv2 Leave приводила к нарушению multicast-связности. IGMPv2 не предусматривает встроенной аутентификации сообщений [1], поэтому узел в сегменте может влиять на состояние подписок. Статические привязки групп и ограничения по портам могут использоваться как меры снижения риска, но их действие проверялось только в указанной конфигурации. IGMPv3 позволяет фильтровать multicast-источники, однако не аутентифицирует отправителя Leave-сообщения; для защиты управления сообщениями нужен отдельный механизм. Испытания IGMPv3 в этой работе не проводились [8].

Валидация факторов защиты

Для эмпирической проверки эффективности предложенных в теоретической части методов защиты был проведён дополнительный эксперимент на том же лабораторном стенде с использованием коммутатора Cisco Catalyst 2960. После успешной демонстрации атаки поддельным IGMP Leave на незащищённой конфигурации была применена и протестирована

статическая привязка multicast-группы.

В тексте приведена команда `ip igmp snooping vlan 1 static 239.255.255.250 interface FastEthernet0/15` для статической привязки порта. В следующем листинге показана запись `type user` для другой группы — 239.255.1.1. Эти адреса различаются, поэтому показанный вывод не подтверждает результат именно приведённой команды; он иллюстрирует статическую запись в таблице IGMP-групп.

Листинг 3 – Таблица IGMP-групп после применения факторов защиты

Building configuration...

[OK]

Switch#show ip igmp snooping groups

Vlan	Group	Type	Version	Port List
1	239.255.1.1	user	v2	Fa0/11, Fa0/15

Авторы сообщают, что при повторной отправке поддельного IGMPv2 Leave порт Fa0/15 остался в таблице и видеопоток не прервался. Это наблюдение относится к показанной Cisco-конфигурации. Различие адресов группы в команде и выводе ограничивает воспроизводимость этого эпизода; из него нельзя заключить о полном предотвращении таких атак во всех конфигурациях.

Статическая привязка рассматривается как вариант сохранения членства порта независимо от динамических сообщений. Её применимость к конкретному multicast-потoku следует проверять на используемой модели и с согласованными адресами группы; универсальная эффективность в этой работе не установлена.

Сопоставление реакции Cisco, Eltex и MikroTik на поддельное IGMP Leave

Описание эксперимента:

Целью эксперимента являлась практическая демонстрация уязвимости протокола IGMPv2 к атаке поддельным Leave-сообщением, а также сравнительный анализ реакции на эту атаку коммутаторов трёх различных производителей: Cisco Systems (модель Catalyst 2960), MikroTik (модель CRS326-24G-2S+RM) и Eltex (модель MES1428). [5–7] Все устройства относятся к классу L2+ и поддерживают функционал IGMP snooping, что позволяет им анализировать IGMP-трафик и оптимизировать multicast-рассылку.

Гипотеза эксперимента:

Предполагалось, что при идентичных базовых настройках реакция на поддельное IGMP Leave-сообщение будет различаться в зависимости от производителя из-за особенностей реализации протокола, используемых таймеров и наличия дополнительных защитных механизмов.

Условия проведения эксперимента:

Все эксперименты проводились в изолированном лабораторном стенде, исключающем влияние фонового трафика. Коммутаторы и устройства (сервер, клиент, атакующий) были соединены напрямую патч-кордами, без использования промежуточных коммутаторов или маршрутизаторов. Электропитание оборудования осуществлялось через стабилизаторы напряжения для исключения сбоев, связанных с нестабильностью питания. Дополнительный сетевой трафик отсутствовал, все неиспользуемые порты коммутатора были отключены.

Методика эксперимента:

Для каждого коммутатора стенд собирался независимо по единой схеме:

1. К коммутатору подключались три устройства: сервер – источник multicast-потока, клиент – легитимный получатель; атакующий – источник поддельных сообщений.
2. На коммутаторе выполнялась минимально необходимая конфигурация: активировался IGMP snooping для VLAN 1, интерфейсу VLAN 1 назначался IP-адрес, включался IGMP Querier, порт сервера статически обозначался как mrouter-порт.
3. На сервере запускался скрипт, генерирующий UDP-пакеты в multicast-группу 239.255.255.250:1234.
4. На клиенте наблюдалось непрерывное воспроизведение видео, подтверждающее

успешную подписку на multicast-группу.

5. На атакующем устройстве запускался Python-скрипт, использующий библиотеку Scapy для отправки IGMPv2 Leave-пакета от имени клиента на адрес всех маршрутизаторов 224.0.0.2.
6. Сразу после отправки поддельного IGMP Leave-пакета воспроизведение видео на клиенте прервалось, что свидетельствует о нарушении доставки трафика.
7. Для каждого коммутатора замерялось время от отправки первого Leave-пакета до исчезновения порта клиента из таблицы IGMP-групп и до фактического прекращения приёма данных клиентом.

Контрольные замеры:

Авторы сообщают о контрольных наблюдениях легитимного Leave и интервалах истечения членства без Leave в пределах 260–300 с. Первичные журналы этих прогонов в статье не представлены. Поэтому заявленное совпадение с реакцией на поддельный Leave рассматривается как авторское наблюдение, а не доказательство отсутствия аномалий или соответствия всем настройкам по умолчанию.

Порядок эксперимента:

Для каждого исследуемого коммутатора собирался идентичный стенд: к устройству подключались три ПК – сервер-источник multicast-потока, клиент-получатель и атакующий. На коммутаторе активировался IGMP snooping для VLAN 1, интерфейсу VLAN 1 назначался IP-адрес 10.10.10.254, включался IGMP Querier, а порт сервера статически определялся как mrouter-порт. Сервер генерировал UDP-пакеты в группу 239.255.255.250:1234, клиент запускал скрипт-приёмник, отправляющий IGMPv2 Report и выводящий полученные данные. Корректность подписки проверялась командой show ip igmp snooping groups. Атакующий с помощью Python-скрипта на базе библиотеки Scapy отправлял IGMPv2 Leave-пакет с подменённым IP-адресом источника на адрес всех маршрутизаторов 224.0.0.2. Для захвата трафика использовался Wireshark, запущенный на атакующем ПК с предварительно настроенным зеркалированием порта клиента. Целью являлась фиксация момента отправки поддельного Leave-пакета и наблюдение за прекращением приёма multicast-трафика на клиенте, а также сравнение времени реакции исследуемых коммутаторов.

Таблица 1 – Время реакции на поддельное сообщение IGMP Leave

Производитель	Модель	Время реакции
Cisco	Catalyst 2960	около 2-3 секунд
Eltex	MES1428	меньше 1 секунды
MikroTik	CRS326	около 10 секунд

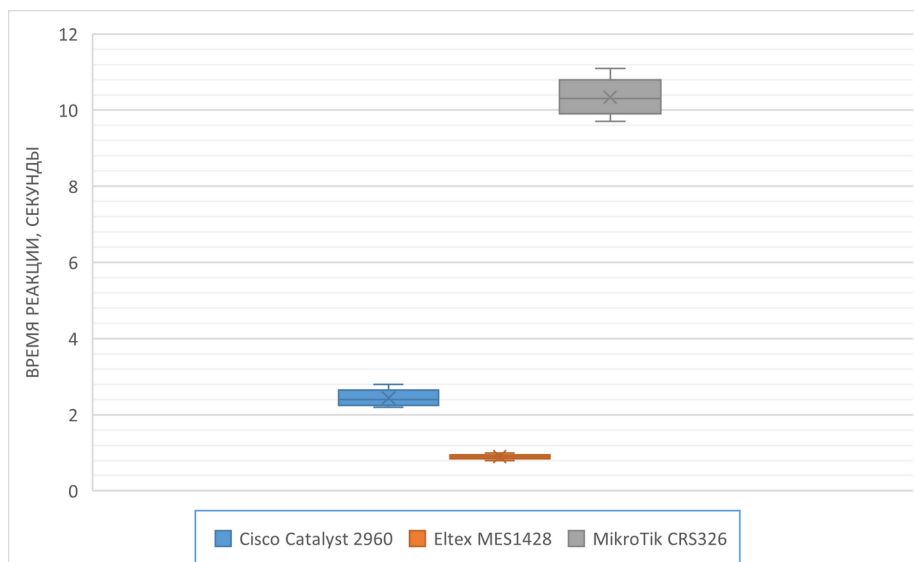


Рис. 3. Авторские наблюдения времени реакции коммутаторов на IGMP Leave

Результаты и обсуждение

Анализ наблюдаемых интервалов реакции

Ниже рассматриваются возможные объяснения различий авторских сводных интервалов. Путь аппаратной и программной обработки, загрузка CPU и фактические значения всех таймеров отдельно не измерялись, поэтому причинная интерпретация остаётся гипотезой.

61. Для Eltex MES1428 авторы указали реакцию менее 1 с. Это значение относится к выбранному стенду. Настройки IGMP snooping рассматриваются в документации [6], но данное наблюдение не устанавливает включение Immediate-leave по умолчанию, роль ASIC или сравнительную уязвимость платформы.
62. Для MikroTik CRS326 указано около 10 с. Настройки IGMP snooping описаны в источнике [7]. Из показанного интервала нельзя определить долю программной обработки, значения таймеров по умолчанию или строгое соответствие конкретной реализации всем рекомендациям RFC 4541.
63. Для Cisco Catalyst 2960 указано около 2–3 с. Документация [5] может использоваться при проверке параметров группы и запросов. В статье не показано отдельное измерение аппаратного ускорения; поэтому оно не считается установленной причиной отличия от других моделей.

Масштабируемость атаки

В работе не проводились нагрузочные испытания с множественными поддельными сообщениями. Поэтому реакцию устройств на интенсивный поток IGMP-пакетов, загрузку CPU и пределы масштабирования по этим результатам оценить нельзя; это требует отдельного контролируемого эксперимента.

Следует отметить, что данное исследование было сфокусировано исключительно на атаке подделкой IGMP Leave, как на наиболее наглядном способе нарушения multicast-связности. Однако, протокол IGMPv2 уязвим и для других векторов, в частности подделки IGMP Report и атаки на IGMP Querier. Проведение экспериментов с этими типами атак требует отдельной методики и выходит за рамки данной работы, но их важность подчёркивает необходимость комплексного подхода к защите.

Зависимость времени реакции от параметров IGMP snooping

В таблице 2 приведён авторский пример изменения last-member-query-interval и last-member-query-count на Cisco Catalyst 2960. Он не является сравнительным анализом всех возможностей регулирования таймеров на трёх платформах. Настройки других моделей и версий следует проверять по соответствующей документации; уникальная гибкость Cisco и фиксированность параметров Eltex в этой работе не установлены.

Таблица 2 – Наблюдаемое время реакции при изменении параметров опроса

last-member-query-interval (миллисекунды)	last-member-query-count (количество)	Время реакции (секунды)
500	2	1,0-1,5
1000	2	2,0-3,0
2000	2	4,0-5,0
1000	3	3,0-4,0
500	3	1,5-2,0

Для приведённых значений в таблице 2 авторы предлагают приближённую зависимость времени реакции от интервала и числа запросов (формула 1). В формуле t — время реакции (с); I — интервал Last Member Query (с); C — число запросов. Поправка 0,5 входит в авторское приближение; его точность за пределами приведённых комбинаций отдельно не оценивалась.

$$t \approx I \times (C + 0.5) \quad (1)$$

В испытаниях на Cisco Catalyst 2960 наблюдаемое время реакции изменялось вместе с настроенными параметрами таймеров. Эти результаты относятся только к Cisco и не подтверждают линейную зависимость на других платформах:

Варианты настройки защиты IGMPv2 для трёх платформ

Ниже представлена таблица, сравнивающая основные команды для конфигурации механизмов защиты IGMPv2 на трёх исследуемых платформах: Cisco Catalyst 2960, Eltex MES1428 и MikroTik CRS326. [5–7]

Таблица 3 – Примеры настройки защитных функций IGMPv2 на коммутаторах

Действие	CISCO	ELTEX	MIKROTIK
Включение IGMP snooping глобально	ip igmp snooping	ip igmp snooping	/interface bridge set [find name=bridge1] igmp-snooping=yes
Включение IGMP snooping для конкретного VLAN	ip igmp snooping vlan 1	ip igmp snooping vlan 1	Настраивается через bridge VLAN; snooping работает для всех VLAN, включённых в bridge
Настройка IGMP Querier	ip igmp snooping querier vlan 1	ip igmp snooping querier vlan 1	/interface bridge set [find] igmp-querier=yes
Назначение IP-адреса интерфейсу VLAN для Querier	interface vlan 1 ip address 10.10.10.254 255.255.255.0 no shutdown	interface vlan 1 ip address 10.10.10.254 255.255.255.0	/interface vlan add interface=bridge1 name=vlan1 vlan-id=1 /ip address add address=10.10.10.254/24 interface=vlan1
Включение Immediate-Leave	ip igmp snooping vlan 1 immediate-leave	ip igmp snooping vlan 1 immediate-leave	/interface bridge set [find] igmp-fast-leave=yes
Статическая привязка multicast-группы к порту	ip igmp snooping vlan 1 static 239.255.255.250 interface FastEthernet0/15	ip igmp snooping vlan 1 static 239.255.255.250 interface ethernet 1/0/15	/interface bridge mdb add bridge=bridge1 group=239.255.255.250 interface=ether1

Действие	CISCO	ELTEX	MIKROTIK
Ограничение максимального количества групп на порт	interface FastEthernet0/15 ip igmp limit 5	interface ethernet 1/0/15 ip igmp max-groups 5	/interface bridge port set [find interface=ether1] igmp-group-limit=5
Фильтрация IGMP-пакета с помощью ACL	access-list 10 deny 239.255.255.250 access-list 10 permit any interface FastEthernet0/15 ip igmp access-group 10	access-list 10 deny 239.255.255.250 access-list 10 permit any interface ethernet 1/0/15 ip igmp access-group 10	/ip firewall filter add chain=forward action=drop protocol=igmp dst- address=239.255.255.250 in-interface=ether1
Настройка таймера Last Member Query Interval	ip igmp snooping vlan 1 last-member-query- interval 500	ip igmp snooping vlan 1 last-member-query- interval 500	/interface bridge set [find] igmp-last- member-query-interval=500ms
Настройка количества Last Member Query Count	ip igmp snooping vlan 1 last-member-query- count 2	ip igmp snooping vlan 1 last-member-query- count 2	igmp-last-member-query-interval
Настройка Robustness Variable	ip igmp snooping vlan 1 robustness-variable 3	ip igmp snooping vlan 1 robustness-variable 3	/interface bridge set [find] igmp- robustness=3
Сохранение конфигурации	write memory или copy running-config startup-config	write startup-config	/export file=config

Таблица 3 содержит приведённые авторами варианты настройки для планирования защиты multicast-доставки. Синтаксис и применимость команд необходимо сверять с документацией конкретной модели, версии ПО и операционной системы коммутатора. Совокупная эффективность перечисленных настроек на всех трёх платформах в работе не проверялась. Для MikroTik в таблице использован синтаксис RouterOS, тогда как источник [7] описывает SwOS. Возможность применения отдельных команд и полнота их синтаксиса по представленным материалам не подтверждены.

Заключение

В статье описан лабораторный эпизод с поддельным IGMPv2 Leave-сообщением на Cisco Catalyst 2960 и приведены наблюдения времени реакции для Cisco, Eltex и MikroTik. Выбранные сценарии и таймеры демонстрируют риск изменения членства порта, но не устанавливают одинаковую уязвимость всех L2+ коммутаторов. Статические записи и настройки запросов рассмотрены как варианты снижения риска; выводы ограничены

представленными конфигурациями и иллюстрациями.

В качестве направления дальнейшей работы можно проверить фильтрацию multicast-источников, предусмотренную IGMPv3 [8]. Сам IGMPv3 не добавляет аутентификацию участников; защита сообщений требует отдельного механизма, например IPsec в соответствующем окружении. Экспериментальная проверка IGMPv3 в данной работе не проводилась.

Вместе с тем важно подчеркнуть, что статическая привязка multicast-групп, будучи высокоэффективным защитным механизмом, обладает существенными эксплуатационными недостатками. Ручное конфигурирование каждой группы лишает сеть гибкости динамического управления подписками, что критично в условиях часто меняющегося состава получателей. Административные издержки на поддержание статических записей в крупных инфраструктурах могут стать неприемлемыми.

Библиографический список

1. Fenner W. Internet Group Management Protocol, Version 2 : RFC 2236. — IETF, 1997. — URL: <https://datatracker.ietf.org/doc/html/rfc2236> (дата обращения: 15.02.2026).
2. Способ и устройство передачи трафика с групповой адресацией с множеством линий связи : пат. 2804753 Российская Федерация, МПК H04W 4/06, H04W 72/04 / М. Гань, Д. Лян, И. Ли, Ю. Го, Ю. Ли, Ц. Юй, С. Ян ; патентообладатель Хуавэй Текнолоджиз Ко., Лтд. — № 2022133288 ; заявл. 04.06.2021 ; опубл. 05.10.2023. — 30 с. : ил.
3. Обзор сетевых атак и методов их предотвращения на канальном уровне / Казанский национальный исследовательский технический университет имени А. Н. Туполева — КАИ. — Казань, 2024. — 6 с.
4. Christensen M., Kimball K., Solensky F. Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches : RFC 4541. — IETF, 2006. — URL: <https://datatracker.ietf.org/doc/html/rfc4541> (дата обращения: 15.02.2026).
5. Cisco Systems. Configuring IGMP Snooping for Cisco Catalyst 2960 Series Switches [Электронный ресурс]. — URL: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/12-2_55_se/configuration/guide/scg_2960/swigmp.html (дата обращения: 16.02.2026).
6. Eltex. Ethernet Switches MES14xx, MES24xx : Operation Manual, Firmware Version 10.1.8.2 [Электронный ресурс]. — URL: https://eltexalatau.kz/upload/iblock/60f/mes14xx_-mes24xx_user-manual_10.2.1.1.pdf (дата обращения: 10.12.2025).
7. MikroTik. CRS3xx and CSS3xx Series Manual [Электронный ресурс]. — URL: <https://help.mikrotik.com/docs/spaces/SWOS/pages/76415036/CRS3xx+and+CSS3xx+series+Manual> (дата обращения: 10.12.2025).
8. Cain B., Deering S., Kouvelas I., Fenner B., Thyagarajan A. Internet Group Management Protocol, Version 3 : RFC 3376. — IETF, 2002. — URL: <https://datatracker.ietf.org/doc/html/rfc3376>.

References

1. Fenner, W. (1997). *Internet Group Management Protocol, Version 2 (RFC 2236)*. Internet Engineering Task Force. <https://datatracker.ietf.org/doc/html/rfc2236>
2. Gan, M., Liang, D., Li, Y., Guo, Y., Li, Y., Yu, J., & Yang, S. (2023). *Sposob i ustroistvo peredachi trafika s gruppovoi adresatsiei s mnozhestvom linii svyazi [Method and device for transmitting multicast traffic over multiple communication lines] (Patent RU 2804753 C1)*. Huawei Technologies Co., Ltd.
3. Kazanskii natsionalnyi issledovatel'skii tekhnicheskii universitet imeni A. N. Tupoleva—KAI. (2024). *Obzor setevykh atak i metodov ikh predotvrashcheniya na kanalnom urovne [Overview of network attacks and methods of preventing them at the data link layer]*.
4. Christensen, M., Kimball, K., & Solensky, F. (2006). *Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches (RFC 4541)*. Internet Engineering Task Force. <https://datatracker.ietf.org/doc/html/rfc4541>

5. Cisco Systems. (n.d.). *Configuring IGMP Snooping for Cisco Catalyst 2960 Series Switches*. https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/12-2_55_se/configuration/guide/scg_2960/swigmp.html
6. Eltex. (n.d.). *Ethernet Switches MES14xx, MES24xx: Operation Manual, Firmware Version 10.1.8.2*. https://eltexalatau.kz/upload/iblock/60f/mes14xx_-mes24xx_user-manual_10.2.1.1.pdf
7. MikroTik. (n.d.). *CRS3xx and CSS3xx Series Manual*. <https://help.mikrotik.com/docs/spaces/SWOS/pages/76415036/CRS3xx+and+CSS3xx+series+Manual>
8. Cain, B., Deering, S., Kouvelas, I., Fenner, B., & Thyagarajan, A. (2002). *Internet Group Management Protocol, Version 3 (RFC 3376)*. Internet Engineering Task Force. <https://datatracker.ietf.org/doc/html/rfc3376>

Информация об авторах

Кязымов Адалат Адалатович — студент факультета комплексной безопасности ТЭК ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И. М. Губкина», Москва, Россия; e-mail: adalat.kiazymov@mail.ru.

Терешонок Артём Алексеевич — студент факультета комплексной безопасности ТЭК ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И. М. Губкина», Москва, Россия; e-mail: kr3nver@yandex.ru.

EXPERIMENTAL ANALYSIS OF IGMPV2 VULNERABILITIES AND COMPARATIVE EVALUATION OF PROTECTION METHODS ON L2+ SWITCHES FROM DIFFERENT VENDORS

Kyazimov A. A.¹, Tereshonok A. A.¹

¹ Gubkin Russian State University of Oil and Gas (National Research University), Moscow, Russia

Abstract. This paper describes a laboratory example involving a spoofed IGMP Leave message and discusses ways to protect multicast group membership on Cisco Catalyst 2960, Eltex MES1428, and MikroTik CRS326 switches. It outlines IGMPv2 and IGMP snooping, which maintain subscriber information and direct multicast traffic to selected ports. The article reports approximate client-port removal intervals of two to three seconds for Cisco, less than one second for Eltex, and about ten seconds for MikroTik. These observations concern the stated models and test settings. The main attack and static-entry example concerns the Cisco configuration. Static multicast binding, group-count limits, IGMP access lists, and Last Member Query Interval and Count settings are considered as possible controls. Reported timer combinations illustrate the trade-off between faster membership removal and tolerance of false messages. The illustrated static command and displayed group table contain different multicast addresses, so the displayed result cannot verify that exact command. The authors report uninterrupted delivery during one repeated attempt, but this does not establish universal protection. Operational limitations of static entries and IGMPv3 are discussed rather than independently tested across all platforms. The results support local configuration checks and distinguish observed behavior from proposed protective settings.

Keywords: IGMPv2, IGMP snooping, multicast, L2+ switches, network security, attack, protection.

Information about the authors

Kyazimov Adalat Adalatovich — student, Faculty of Integrated Security of the Fuel and Energy Complex, Gubkin Russian State University of Oil and Gas (National Research University), Moscow, Russia; e-mail: adalat.kiazymov@mail.ru.

Tereshonok Artem Alekseevich — student, Faculty of Integrated Security of the Fuel and Energy Complex, Gubkin Russian State University of Oil and Gas (National Research University), Moscow, Russia; e-mail: kr3nver@yandex.ru.