ПРОФЕССИОНАЛИТЕТ, 2025, № 2 (006)

УДК *004.056.53*

Е. А. Еремина [1]***, А. Н. Простова*** [1]

[1]*ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И.М. Губкина», г. Москва, Российская Федерация*

ВЛИЯНИЕ АТАКИ MAC-FLOODING НА КОММУТАТОРЫ L2 В ГИБРИДНОЙ СЕТЕВОЙ ИНФРАСТРУКТУРЕ

Аннотация: *Проведенное исследование выявляет критическую уязвимость L3-устройств в гибридных сетях при атаках на канальном уровне. Экспериментально показано, классическая атака MAC-flooding, направленная на переполнение CAM-таблиц коммутаторов доступа, приводит не только к нарушению конфиденциальности трафика на L2-уровне, но и вызывает каскадный рост нагрузки на маршрутизаторы (L3) из-за массовой генерации unknown unicast-трафика. Данный трафик перенаправляется на маршрутизатор, приводя к критической нагрузке на его процессор, увеличении времени отклика и возможному отказу в обслуживании для всей сетевой инфраструктуры.*

В работе проведено сравнительное тестирование стандартных механизмов защиты (Port Security, Storm Control) на оборудовании различных производителей в условиях смоделированной атаки. Эксперименты проводились на стенде с использованием оборудования Cisco, Mikrotik и Eltex, атака генерировалась средствами Kali Linux. Результаты демонстрируют, что активация Port Security в режиме shutdown на портах доступа является наиболее эффективным способом блокировки атаки в источнике. Для обеспечения комплексной устойчивости гибридной сети эту меру необходимо дополнять ограничением широковещательного трафика на уровне маршрутизатора.

Полученные данные имеют важное прикладное значение для обеспечения отказоустойчивости и безопасности современных гибридных сетевых инфраструктур, объединяющих оборудование различных вендоров, и позволяют сформулировать практические рекомендации по настройке безопасности для сетей, объединяющих оборудование различных производителей, с целью предотвращения эскалации L2-атак на L3-уровень.

Ключевые слова: *MAC-flooding, сетевая безопасность, L3 маршрутизатор, L2 коммутатор, CAM-таблица, unknown unicast, Port Security.*

Введение

В современном мире в информационной среде все более активно используются L3 устройства, работающие с IP-адресами и имеющие функцию маршрутизации и соединения различных VLAN. L3 коммутатор соединяет в себе функции L2 коммутатора и маршрутизатора, то есть может выполнять все функции обычного коммутатора (L2), но также обладает «интеллектуальными» функциями маршрутизатора, которые позволяют эффективно передавать данные между различными сетями без необходимости использования внешнего маршрутизатора [1]. Такая интеграция создает новые угрозы информационной безопасности.

Особенностью современных вызовов информационной безопасности является приобретение классическими атаками на канальном уровне модели новых качеств. Основная проблема заключается в недооценке данной эволюции.

Цель исследования: разработка эффективного метода защиты от атаки MAC-flooding на L3 устройства.

Объект исследования: защищенность гибридной сетевой инфраструктуры, включающей L3-устройства (маршрутизаторы), от атак на канальном уровне.

Предмет исследования: механизм влияния атаки MAC-flooding, проводимой на L2-коммутаторах доступа, на производительность и отказоустойчивость L3-маршрутизаторов, а также сравнительная эффективность методов защиты.

На классическом L2 коммутаторе цель атаки: переполнение CAM-таблицы с последующим переходом устройства в режим хаба для перехвата трафика (нарушение конфиденциальности) [2].

Материалы и методы

Анализ показывает, что атака MAC-flooding была и остается актуальной угрозой для L3-устройств, несмотря на наличие базовых механизмов защиты. В 2015 году в фундаментальном исследовании Florent Gontharet «Man-in-The-Middle Attacks & Countermeasures Analysis»

(Университет Абертей Данди) [3] описана базовая уязвимость коммутатора: атака успешно реализуема с помощью macof из dsniff, приводит к переполнению CAM-таблицы виртуального коммутатора Cisco и требует защиты с мониторингом MAC-адресов.

В 2018 году исследование Simran Thakur et al.: «Three tier architecture with enhanced security at layer 2 And layer 3» (IARJSET, CETE-2018) [4] пришло к следующим выводам: атака возможна из-за динамического изучения адресов на L2/L3-свитчах трехуровневой архитектуры, приводит к DoS и перехвату трафика флудом уникальных MAC; протестировано в GNS3 на Cisco-оборудовании.

В 2023 году Скоробогатова С.Ю. и др. «Методика прогнозирования воздействия компьютерных атак на элементы программно-конфигурируемой сети» [5] выявили успешность атаки как элемента многоуровневого DoS в SDN-инфраструктурах с L3-элементами, с нарушением работы критических сетевых компонентов.

Руководство Cisco «Configure DHCP Snooping» (2018) [6] подтвердило эффективность port security и DHCP Snooping для L3-устройств против MAC-flooding в связке с DAI.

Однако проведенный анализ литературы показал, что большинство исследований на тему атаки MAC-flooding сосредоточено либо на теоретическом описании угрозы, либо на инструкциях по настройке отдельных защитных механизмов, также основное внимание уделено атакам на атаки 2 уровня модели OSI (L2).

Тип исследования: анализ уязвимости с элементами экспериментального исследования в лабораторной среде.

Характеристика среды исследования: лабораторная сетевая инфраструктура, включающая коммутаторы L2 различных производителей, L3 маршрутизатор Cisco 1941, а также три конечных узла. Один из конечных узлов на базе ОС Kali Linux использовался в качестве источника атаки, второй узел на базе ОС Альт Linux использовался как пользователь сети, третий узел применялся для мониторинга сетевого трафика и фиксации аномалий.

Процедура проведения эксперимента:

- Развертывание и настройка базовой тестовой сети.
- Определение базовых показателей и ролей узлов.
- Проведение атаки MAC-flooding.
- Мониторинг и анализ последствий атаки.
- Тестирование механизмов защиты.
- Сравнительный анализ и формирование выводов.

Методы обработки данных: анализ успешности атаки, сравнение эффективности методов защиты, качественный анализ эффективности защитных мер.

При атаке MAC-flooding злоумышленник отправляет в сеть большое количество пакетов с поддельными или случайными MAC-адресами источников. Это приводит к быстрому заполнению таблицы MAC-адресов коммутатора. Когда таблица достигает своей емкости, коммутатор больше не может сопоставлять MAC-адреса с определенными портами и переходит в режим fail-open, в котором он начинает перекачивать входящий трафик через все порты. Это позволяет злоумышленнику перехватывать трафик, так как после атаки коммутатор транслирует трафик на все порты.

Port Security – это функция коммутаторов Cisco и подобных (например, Eltex), которая контролирует доступ к порту на основе MAC-адресов. Она позволяет привязать к порту только определенные MAC-адреса и блокировать неавторизованные устройства.

На оборудовании Mikrotik аналогичная функциональность обеспечивается параметром learn-limit для портов моста, который выполняет ту же задачу: блокирует изучение новых MAC-адресов сверх заданного предела.

Эксперимент был ориентирован на анализ последствий переполнения CAM-таблицы коммутаторов доступа (Cisco Catalyst 2960, Mikrotik CRS326, Eltex MES1428) и оценку эффективности встроенных механизмов защиты при воздействии высокоинтенсивного потока кадров с поддельными MAC-адресами.

Эксперимент был проведен с различными устройствами L2, L3 уровня и PC с операционной системой Linux. На рисунке 1 представлена используемая топология сети.

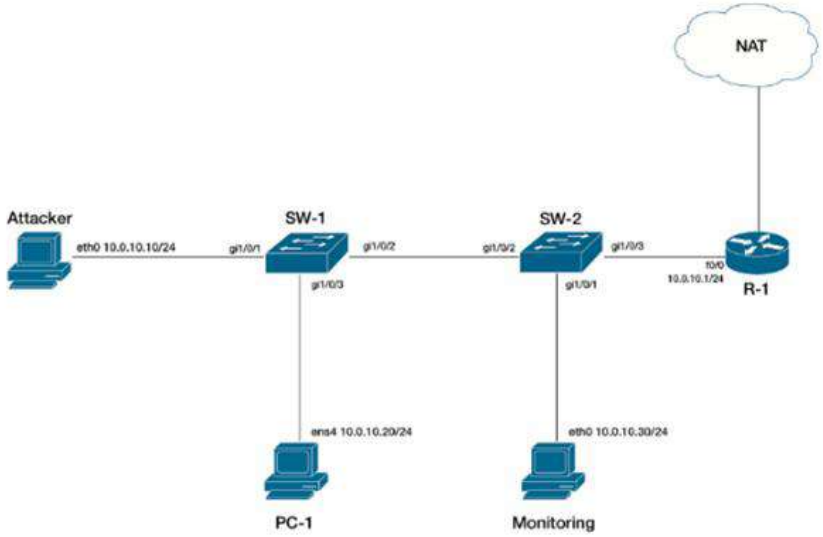

Рис. 1. Топология сети для эксперимента

Подготовка оборудования:

- коммутаторы: Cisco Catalyst 2960 (версия 15.0(2)SE11), Cisco Catalyst 3550 (версия 12.2(55)SE12), Mikrotik Cloud Router Switch CRS326-24G-2S+RM (версия 15.2(4)M7), Eltex MES1428 (версия 10.4.2.1);
- маршрутизатор: Cisco 1941 (версия 15.2(4)M7);
- ПК №1 (атакующий): Kali Linux с интерфейсом ens0;
- ПК №2 (жертва): Alt Linux с интерфейсом ens4;
- ПК №3 (мониторинг): Kali Linux с интерфейсом ens0.

Конфигурация сетевых узлов осуществлялась следующим образом:

– На атакующем узле (Kali Linux) выполнена базовая настройка сетевого интерфейса eth0. Был назначен статический IP-адрес 10.0.10.10/24; активирован интерфейс; добавлен маршрут по умолчанию через шлюз 10.0.10.1.

– На пользовательском узле (Alt Linux) установлено имя хоста (Eremina-ALT); назначен статический IP-адрес 10.0.10.20/24 на интерфейс ens4; указан DNS сервер 1.1.1.1; добавлен маршрут по умолчанию через шлюз 10.0.10.1 для проверки доступности шлюза.

– На узле мониторинга, который нужен для захвата и анализа трафика в ходе эксперимента, назначен статический IP-адрес 10.0.10.30/24 на интерфейс eth0; также указан DNS-сервер 1.1.1.1 и добавлен маршрут по умолчанию через шлюз 10.0.10.1.

– На коммутаторе доступа Eremina-SW1 (Cisco Catalyst 2960) была выполнена следующая конфигурация портов: порт GigabitEthernet0/1 настроен как access для атакующего узла; порт GigabitEthernet0/2 настроен как access для узла-пользователя. Также оба порта помещены в VLAN 1 (нативный VLAN); активирован spanning-tree portfast для ускорения перехода портов в активное состояние. Коммутатор обеспечивает канальное соединение узлов внутри одного широковещательного домена [7]. См. рис. 2.

```
Switch(config)#hostname Eremina-SW1
Eremina-SW1(config)#no ip domain-lookup
Eremina-SW1(config)#spanning-tree mode rapid-pvst
Eremina-SW1(config)#interface gi0/0
Eremina-SW1(config-if)#description Kali
Eremina-SW1(config-if)#switchport mode access
Eremina-SW1(config-if)#switchport access vlan 1
Eremina-SW1(config-if)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
 host. Connecting hubs, concentrators, switches, bridges, etc... to this
 interface  when portfast is enabled, can cause temporary bridging loops.
 Use with CAUTION

%Portfast has been configured on GigabitEthernet0/0 but will only
 have effect when the interface is in a non-trunking mode.
Eremina-SW1(config-if)#interface gi0/2
Eremina-SW1(config-if)#description ALT-user
Eremina-SW1(config-if)#switchport mode access
Eremina-SW1(config-if)#switchport access vlan 1
Eremina-SW1(config-if)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
 host. Connecting hubs, concentrators, switches, bridges, etc... to this
 interface  when portfast is enabled, can cause temporary bridging loops.
 Use with CAUTION

%Portfast has been configured on GigabitEthernet0/2 but will only
 have effect when the interface is in a non-trunking mode.
Eremina-SW1(config-if)#no shutdown
exitina-SW1(config-if)#
Eremina-SW1(config)#
```

Рис. 2. Конфигурация портов коммутатора Cisco Catalyst 2960 (Eremina-SW1)

Коммутатор доступа Eremina-SW2 был настроен аналогично. Порт GigabitEthernet0/0 настроен как access для узла мониторинга; порт GigabitEthernet0/1 предназначен для uplink-соединения; все порты размещены в VLAN 1. Второй коммутатор необходим для подключения узла мониторинга к зеркальному (SPAN) порту без влияния на основной трафик атаки между коммутатором-жертвой и маршрутизатором.

На маршрутизаторе Eremina-R1 была выполнена следующая конфигурация: интерфейс FastEthernet0/0 настроен как внутренний с адресом 10.0.10.1/24; интерфейс FastEthernet0/1 настроен как внешний с получением адреса через DHCP; настроен NAT для трансляции адресов сети 10.0.10.0/24; а также добавлен статический маршрут по умолчанию через внешний интерфейс.

Все конечные узлы и маршрутизатор были размещены в одном широковещательном домене VLAN. Маршрутизатор выполнял функции шлюза по умолчанию для всех узлов и обеспечивал выход во внешнюю сеть через механизм NAT. Была проверена связность устройств, в результате выводится динамическая таблица MAC-адресов, содержащая всего 5 записей, что соответствует нормальному состоянию сети. См. рис. 3.

```
Eremina-SW1#show mac address-table dynamic
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    0c2d.2325.0001    DYNAMIC     Gi0/1
   1    0c2d.245d.0000    DYNAMIC     Gi0/2
   1    0cc6.dc13.0000    DYNAMIC     Gi0/2
   1    0cfe.f737.0000    DYNAMIC     Gi0/1
   1    c201.23e3.0000    DYNAMIC     Gi0/1
-------------------------------------------
Total Mac Addresses for this criterion: 5
```

Рис. 3. CAM-таблица коммутатора в штатном режиме, содержащая 5 записей

На следующем этапе с узла-нарушителя была инициирована атака с помощью команды: *macof –I eth0*. В процессе атаки фиксировались изменения в работе коммутаторов, рост количества динамических MAC-адресов, увеличение числа неизвестных unicast-кадров, а также рост нагрузки на плоскость управления устройств. См. рис. 4.

```
Eremina-SW1#show mac address-table dynamic
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    3a7f.9c21.a4d8    DYNAMIC     Gi0/0
   1    b6c2.0e91.7f33    DYNAMIC     Gi0/0
   1    5d11.84a0.c9ef    DYNAMIC     Gi0/0
   1    9e3a.6f18.22b7    DYNAMIC     Gi0/0
   1    0001.ff49.bff9    DYNAMIC     Gi0/0
   1    0018.bd4a.c66f    DYNAMIC     Gi0/0
   1    0022.4950.02f7    DYNAMIC     Gi0/0
   1    002f.c02e.090e    DYNAMIC     Gi0/0
   1    003a.5c36.f671    DYNAMIC     Gi0/0
   1    003d.e509.6f35    DYNAMIC     Gi0/0
   1    0004.b278.e74f    DYNAMIC     Gi0/0
   1    0046.bf4b.2278    DYNAMIC     Gi0/0
   1    004d.2a10.bf13    DYNAMIC     Gi0/0
   1    0010.bd75.684d    DYNAMIC     Gi0/0
   1    0052.9d7a.7733    DYNAMIC     Gi0/0
   1    0013.d278.426b    DYNAMIC     Gi0/0
--More--
```

Рис. 4. CAM-таблица во время атаки MAC-flooding

В ходе атаки MAC-flooding в CAM-таблице коммутатора фиксировались многочисленные динамические MAC-адреса, ассоциированные с одним портом доступа. Данные адреса носили случайный характер и постоянно изменялись, что указывает на искусственную генерацию MAC-адресов узлом-нарушителем. Количество динамических MAC-записей в VLAN 1 достигло 21 154, что подтверждает успешное проведение атаки. См. рис. 5.

```
Eremina-SW1#show mac address-table count

Mac Entries for Vlan 1:
------------------------
Dynamic Address Count   : 21154
Static Address Count    : 0
Total Mac Addresses     : 21154

Total Mac Address Space Available: 68133102
```

Рис. 5. Подтверждение переполнения CAM-таблицы: 21154 записи в VLAN 1

В ходе атаки MAC-flooding на мониторинговом узле, подключенном к зеркальному порту коммутатора, фиксировалось поступление Ethernet-кадров, адресованных на MAC-адреса, не принадлежащие данному узлу. Анализ захваченных пакетов показал наличие случайных MAC- и IP-адресов назначения, что свидетельствует о том, что все unknown unicast-кадры широковещательно рассылаются на все порты VLAN, в том числе и на порт мониторинга. См. рис. 6.

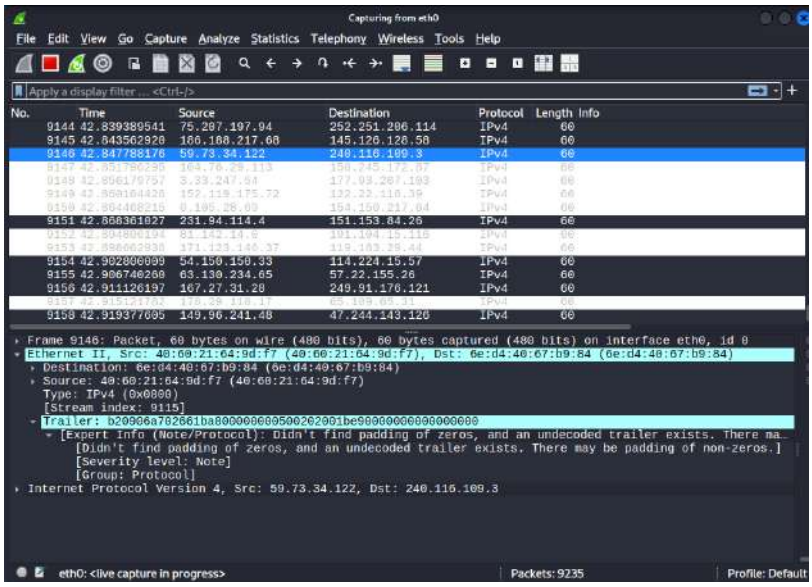

Рис. 6. Анализ трафика в Wireshark: кадры unknown unicast со случайными MAC-адресами

На данном этапе эксперимента на коммутаторе Eremina-SW1 была активирована и поэтапно протестирована функция Port Security на порту GigabitEthernet0/0, к которому подключен атакующий узел. Тестирование проводилось в два этапа: сначала в режиме Restrict, затем в режиме Shutdown. См. рис. 7-10.

```
enable
conf t
interface GigabitEthernet0/0
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address sticky
switchport port-security violation restrict
end
```

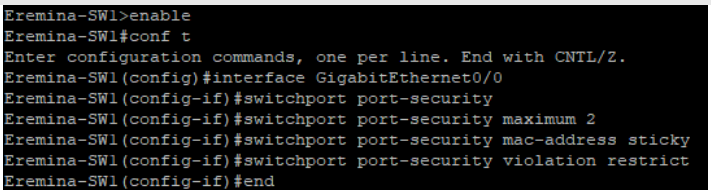

Рис. 7. Настройка Port Security в режиме Restrict с лимитом 2 MAC-адреса

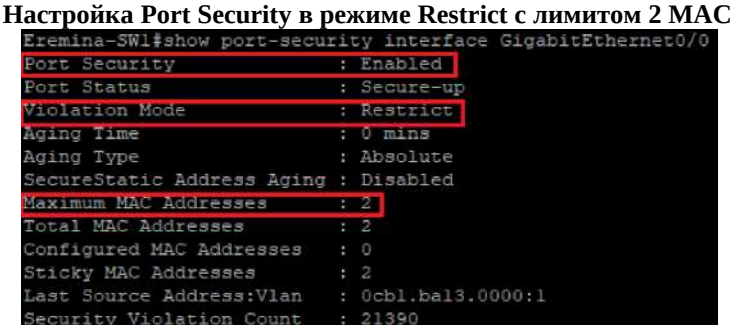

Рис. 8. Port Security в режиме Restrict: 21390 нарушений, порт активен

На рисунке 8 видно, что на интерфейсе gi0/0 настроен Port Security с лимитом в 2 MAC-адреса, используется режим Restrict, и зафиксировано более 21 тысячи нарушений.

```
interface gi0/0
switchport port-security
switchport port-security maximum 2
switchport port-security violation shutdown
switchport port-security mac-address sticky
```

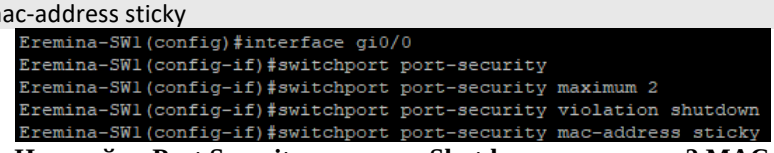

Рис. 9. Настройка Port Security в режиме Shutdown с лимитом 2 MAC-адреса

Рис. 10. Результат срабатывания Port Security: порт в состоянии secure-shutdown

На рисунке 10 видно, что на интерфейсе Gi0/0 настроен Port Security с лимитом в 1 MAC-адрес в строгом режиме Shutdown. В результате одного нарушения безопасности порт был переведен в заблокированное состояние (secure-shutdown).

В захвате трафика отсутствуют кадры с поддельными MAC-адресами и случайными IP.

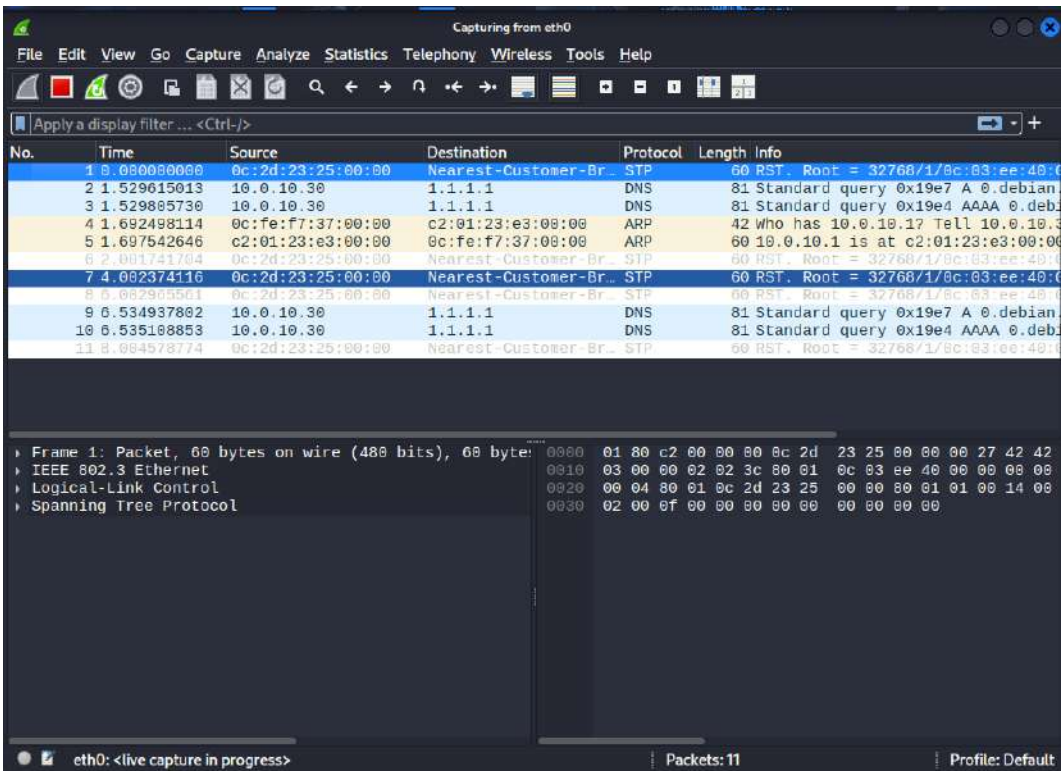

Рис. 11. Мониторинг Wireshark после активации Port Security, прекращение флуда

Режим Shutdown функции Port Security обеспечил эффективную и мгновенную изоляцию источника атаки, что позволило сети вернуться к штатному режиму работы без снижения производительности.

Для сравнения поведения оборудования различных производителей атака MAC-flooding также была последовательно проведена на коммутаторах доступа Mikrotik Cloud Router Switch CRS326-24G-2S+RM, Eltex MES1428, которые были интегрированы в ту же лабораторную топологию на месте коммутатора Eremina-SW1.

Базовая настройка Mikrotik CRS326 включала создание моста bridge1 с включением портов ether1-ether4, назначение IP-адреса управления и проверку штатного заполнения таблицы MAC-адресов. См. рис. 12.

```
[admin@MikroTik] > /system identity set name=Eremina-SW1
[admin@Eremina-SW1] > /interface bridge add name=bridge1 protocol-mode=rstp
[admin@Eremina-SW1] > /interface bridge port add bridge=bridge1 interface=ether1
[admin@Eremina-SW1] > /interface bridge port add bridge=bridge1 interface=ether2
[admin@Eremina-SW1] > /interface bridge port add bridge=bridge1 interface=ether3
[admin@Eremina-SW1] > /interface bridge port add bridge=bridge1 interface=ether4
[admin@Eremina-SW1] > /interface bridge set bridge1 vlan-filtering=no
[admin@Eremina-SW1] > /ip address add address=10.0.10.2/24 interface=bridge1
[admin@Eremina-SW1] > /ip route add gateway=10.0.10.1
[admin@Eremina-SW1] > /interface ethernet set ether1 comment="Kali-attacker"
[admin@Eremina-SW1] > /interface ethernet set ether2 comment="ALT-user"
[admin@Eremina-SW1] > /interface ethernet set ether3 comment="Uplink-to-SW2"
[admin@Eremina-SW1] > /interface ethernet set ether4 comment="Monitoring"
[admin@Eremina-SW1] > /interface bridge host print
Flags: X - disabled, I - invalid, D - dynamic, L - local, E - external
#       MAC-ADDRESS       VID  ON-INTERFACE   BRIDGE    AGE
0   DL  0C:3A:5D:39:00:00       ether1   bridge1
1   DL  0C:3A:5D:39:00:01       ether2   bridge1
2   DL  0C:3A:5D:39:00:02       ether3   bridge1
3   DL  0C:3A:5D:39:00:03       ether4   bridge1
[admin@Eremina-SW1] >
```

Рис. 12. Настройка коммутатора Mikrotik CRS326

После проведения атаки общее количество записей в таблице моста составило 9051, таблица MAC-адресов с порта ether1 наглядно демонстрирует их случайный характер и высокую интенсивность поступления, что привело к исчерпанию ресурсов устройства. См. рис. 13.

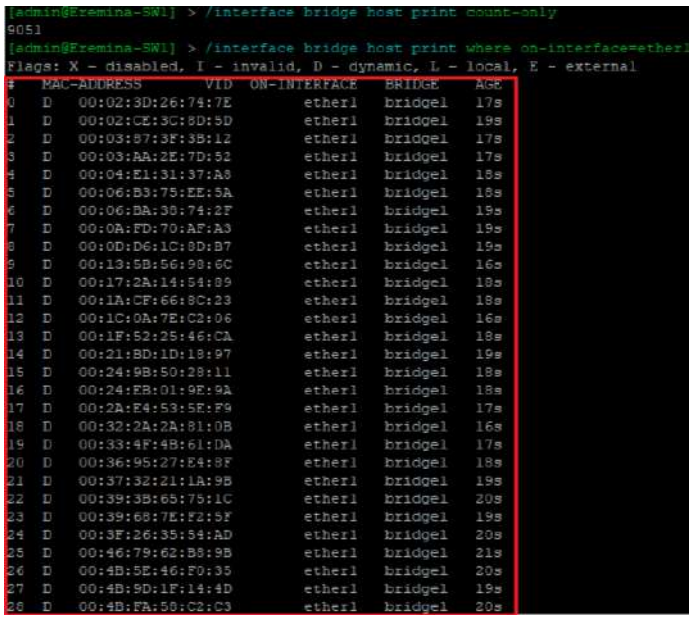

Рис. 13. Результат атаки на Mikrotik: 9051 запись в таблице моста

При попытке использования IP Firewall атака продолжилась, так как MAC-flooding действует на уровне L2 до обработки правил межсетевого экрана L3.

Эффективным механизмом защиты на коммутатор Mikrotik оказалось ограничение числа используемых MAC-адресов на порту с помощью параметра learn-limit. После установки learn-limit=2 на порт ether1 общее количество записей в таблице моста сократилось до 6, что подтверждает блокировку фреймов с поддельными MAC-адресами и остановку атаки. См. рис. 14.

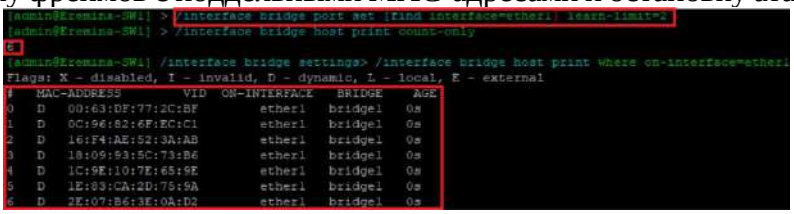

Рис. 14. Таблица MAC-адресов после защиты learn-limit=2 с 6 записями

Далее в работе исследуется поведение коммутатора Eltex MES1428 в условиях атаки MAC-flooding, а также тестируются доступные на данном оборудовании контрмеры.

До атаки таблица MAC-адресов содержит 4 динамические записи, ошибки на портах отсутствуют, загрузка CPU составляет 3%. Это демонстрирует нормальную работу устройства. См. рис. 15.

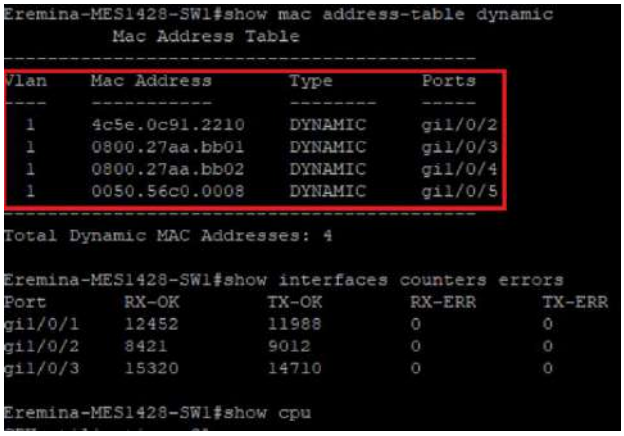

Рис. 15. Eltex MES1428 в штатном режиме: 4 MAC-записи, CPU 3%

После проведения атаки количество MAC-адресов достигло 5089, система зафиксировала критические события: переполнение таблицы MAC, чрезмерный unknown unicast-трафик. Загрузка CPU выросла до 38%. См. рис. 16.

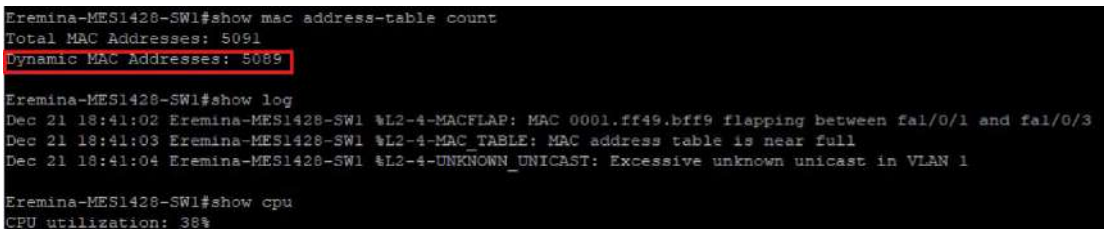

Рис. 16. Последствия атаки на Eltex: 5089 MAC-записей, CPU 38%

Для противодействия атаке на коммутаторе Eltex были последовательно протестированы два механизма: Storm Control (ограничение широковещательного и неизвестного unicast-трафика на уровне 1%) показал себя как сдерживающая, но не предотвращающая мера. При включенном Storm Control количество MAC-записей в CAM-таблице выросло с 4 до 5089 (рис. 15, 16), а загрузка CPU сохранялась на уровне 38%, что указывает на высокую нагрузку из-за обработки огромного числа кадров. Это подтверждает, что Storm Control ограничивает лишь последствия атаки (широковещательный шторм), но не влияет на процесс изучения поддельных MAC-адресов. CAM-таблица продолжает переполняться, нагрузка на CPU остаётся высокой, и часть аномального трафика всё же достигает вышестоящих устройств. Port Security с лимитом в 2 MAC-адреса и реакцией shutdown обеспечил полную нейтрализацию угрозы, переведя порт атакующего в состояние secure-shutdown после первого же нарушения и очистив таблицу MAC-адресов до штатного размера. См. рис. 17, 18, 19.

```
configure
interface fa1/0/1
storm-control broadcast level 1
storm-control unknown-unicast level 1
exit
exit
```

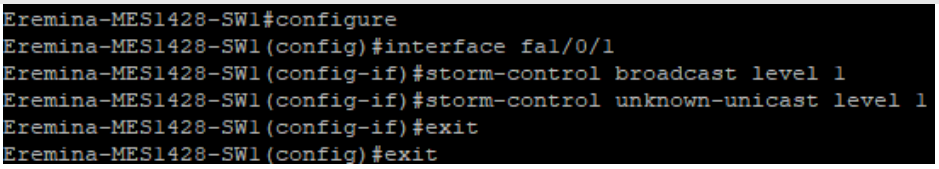

Рис. 17. Конфигурация Storm Control на Eltex

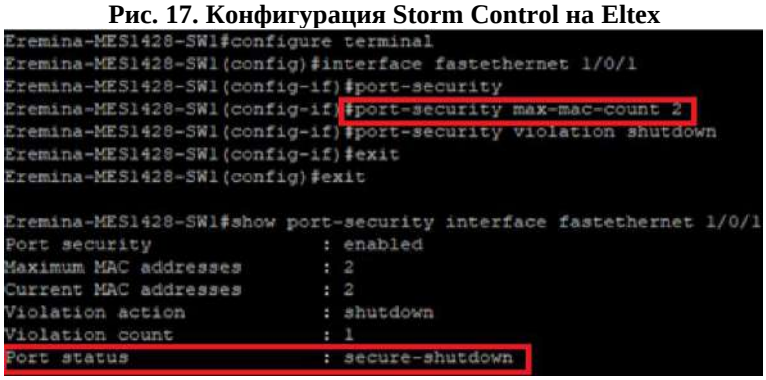

Рис. 18. Настройка Port Security на Eltex с лимитом 2 MAC-адреса

Рис. 19. Результат Port Security на Eltex: таблица MAC-адресов очищена (4 динамические записи)

Результаты

В ходе экспериментального исследования подтверждены переполнение CAM-таблицы и рост нагрузки CPU на коммутаторах доступа. Отдельные метрики L3-маршрутизатора, включая CPU, задержку, потери и ARP-нагрузку, не измерялись, поэтому влияние на L3 в данной работе не оценивается.

На оборудовании Cisco после включения механизма Port Security в режиме Restrict было зафиксировано прекращение распространения flood-трафика за пределы порта доступа, стабилизация CAM-таблиц и отсутствие деградации сетевой связности для легитимных узлов. При этом узел-нарушитель продолжал генерировать кадры с поддельными MAC-адресами, которые отбрасывались коммутатором на уровне порта доступа.

В результате фиксировался значительный рост количества событий нарушения безопасности и увеличение нагрузки на CPU коммутатора. При переводе механизма Port Security в режим Shutdown порт доступа автоматически переводился в состояние err-disabled при первом нарушении, что приводило к полному прекращению приема трафика с узла-нарушителя, что согласуется с общепринятыми практиками защиты на основе Port Security, подробно описанными в работе Protecting Against MAC Flooding Attack [8].

Сравнительный анализ показал, что принцип ограничения числа изучаемых MAC-адресов на порту является универсальной и эффективной контрмерой, успешно реализованной у различных производителей. На коммутаторе Eltex функция Port Security с идентичными параметрами также остановила атаку; на коммутаторе Mikrotik роль аналогичного механизма защиты выполняет параметр learn-limit.

Таким образом, в ходе тестирования на оборудовании различных производителей были получены следующие результаты:

- Cisco Catalyst 2960: Port Security в режиме Shutdown эффективно заблокировал порт после первого нарушения, что подтверждено переводом порта в состояние secure-shutdown;
- Mikrotik CRS326: использование параметра learn-limit=2 на порте ether1 позволило ограничить количество изучаемых MAC-адресов и остановить атаку, сократив количество записей в таблице моста до штатного уровня;
- Eltex MES1428: Port Security с лимитом в 2 MAC-адреса и реакцией Shutdown также обеспечил полную нейтрализацию угрозы, переведя порт в состояние secure-shutdown после первого нарушения.

Для оборудования Mikrotik, помимо параметра learn-limit, может использоваться Bridge Filter – штатный инструмент L2-фильтрации. Для блокировки поддельных ARP-пакетов при MAC-flooding атаке можно добавить правило: /interface bridge filter add chain=forward mac-protocol=arp action=drop. Однако в ходе эксперимента learn-limit показал себя как более простое и эффективное решение именно для предотвращения переполнения CAM-таблицы, так как Bridge Filter фильтрует трафик, но не предотвращает само заполнение таблицы MAC-адресов. Bridge Filter может использоваться как дополнительная мера, например, для борьбы с ARP-спуфингом, но не заменяет защиту от переполнения CAM-таблицы.

Для наглядной оценки эффективности механизма Port Security при противодействии MAC-flooding в таблице 1 представлен сравнительный анализ двух основных режимов реакции на нарушение.

Таблица 1 – Сравнительный анализ режимов реакции Port Security на атаку MAC-flooding

Критерий оценки	Режим restrict	Режим shutdown
Принцип действия	Отбрасывание кадров с неразрешенных MAC-адресов. Порт остается активным	Немедленное отключение порта (перевод в состояние err-disabled)
Влияние на атакующий трафик	Трафик блокируется, но атака продолжается	Атака полностью останавливается после первого нарушения
Нагрузка на CPU коммутатора	Высокая	Отсутствует
Рекомендуемый сценарий применения	Сети, где важен мониторинг атак без остановки обслуживания	Сети, где приоритетом является мгновенная нейтрализация угрозы.

Заключение

Исследование подтвердило:

- успешная атака MAC-flooding приводит к полному переполнению CAM-таблицы коммутатора, что вызывает переход устройства в режим hub и массовую рассылку unknown

unicast-трафика по всем портам VLAN, нарушая доступность сети и создавая угрозу перехвата трафика;

- встроенная функция Port Security (а также ее аналоги) доказала свою результативность на оборудовании различных производителей (Cisco, Mikrotik, Eltex), однако ее режимы демонстрируют различный баланс между безопасностью и эксплуатационными издержками;
- для оборудования Mikrotik эффективным механизмом защиты оказалось ограничение числа MAC-адресов на порту (learn-limit), что также позволяет предотвратить атаку без полного отключения порта.

Это демонстрирует необходимость выбора режима защиты, основанного на приоритетах конкретной сети: максимальная автоматическая защита (Shutdown) или сохранение подключения с мониторингом событий (Restrict, learn-limit).

Атака MAC-flooding остаётся серьёзной угрозой для сетей уровня доступа и может нарушить стабильность L2-инфраструктуры. В ходе исследования были экспериментально проанализированы механизм ее воздействия и дана сравнительная оценка стандартных контрмер на оборудовании различных производителей.

Практические рекомендации:

- включение функции Port Security (или аналогов, таких как learn-limit на Mikrotik) на всех пользовательских портах доступа является обязательной базовой мерой;
- для портов общего пользования рекомендуется режим Restrict с ведением лога событий;
- реализация функций DHCP Snooping и Dynamic ARP Inspection (DAI) в связке с Port Security для комплексного противодействия атакам на канальном уровне;
- настройка систем мониторинга (SNMP, Syslog) для отслеживания событий безопасности портов и статистики unknown unicast-трафика для оперативного выявления инцидентов.

Библиографический список

1. Уровни OSI: простое объяснение и отличия коммутаторов L1, L2 и L3 : [сайт]. – Москва, 2024. – URL: https://servergate.ru/articles/otlichiya-kommutatorov-l1-l2-i-l3/ (дата обращения: 05.11.2025). – Текст: электронный.
2. Что такое MAC Flooding? Как его предотвратить? : [сайт] / Alexhost. – 2024. – URL: https://alexhost.com/ru/faq/what-is-mac-flooding-how-to-prevent-it/ (дата обращения: 20.11.2025).– Текст: электронный.
3. Gontharet, F. Man-in-The-Middle Attacks & Countermeasures Analysis [Электронный ресурс]. – Dundee : University of Abertay Dundee, 2015. – 66 с. – URL: https://www.researchgate.net/publication/340720434_Man-in-The-Middle_Attacks_Countermeasures_Analysis (дата обращения: 10.12.2025). – Текст: электронный.
4. Thakur, S. Three tier architecture with enhanced security at layer 2 And layer 3 [Электронный ресурс] / S. Thakur, A. Khan, J. Dave, S. Kaulgud // International Advanced Research Journal in Science, Engineering and Technology. – 2018. – Vol. 5, Special Issue 3. – С. 13-18. – URL: https://clck.ru/3Qy9Ak (дата обращения: 10.12.2025). – Текст: электронный.
5. Скоробогатов, С. Ю. Методика прогнозирования воздействия компьютерных атак на элементы программно-конфигурируемой сети [Электронный ресурс] / С. Ю. Скоробогатов, И. М. Жданова, А. В. Кузнецов, А. А. Осипенко, Р. Р. Хабушев // Известия Тульского государственного университета. Технические науки. – 2023. – Вып. 2. – С. 269–274. – DOI: 10.24412/2071-6168-2023-2-269-274. – URL: https://cyberleninka.ru/article/n/metodika-prognozirovaniya-vozdeystviya-kompyuternyh-atak-na-elementy-programmno-konfiguriruemoy-seti (дата обращения: 11.12.2025). – Текст: электронный.
6. Configure Dynamic Host Configuration Protocol (DHCP) Snooping on a Switch through the Command Line Interface (CLI) : [сайт] / Cisco. – 2018. – URL: https://www.cisco.com/c/en/us/support/docs/smb/switches/cisco-small-business-300-series-

managed-switches/smb5515-configure-dynamic-host-configuration-protocol-dhcp-snooping.html (дата обращения: 20.12.2025). – Текст: электронный.
7. Уймин, А. Г. Компьютерные сети. L2-технологии : практикум для СПО / А. Г. Уймин. – Саратов, Москва : Профобразование, Ай Пи Ар Медиа, 2024. – 190 с. – ISBN 978-5-4497-2559-2, 978-5-4488-1745-8. – Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. – URL: https://www.iprbookshop.ru/135231.html (дата обращения: 15.11.2025). – Режим доступа: для авторизир. пользователей. – Текст: электронный.
8. Защита от атаки с переполнением MAC-адреса : [сайт] / R. Brezular. – 2024. – URL: https://brezular.com/2024/01/03/protecting-against-mac-flooding-attack/ (дата обращения: 09.12.2025). – Текст: электронный.

References

1. ServerGate. (2024). OSI Layers: A Simple Explanation and Differences Between L1, L2, and L3 Switches. ServerGate. Retrieved November 5, 2025, from https://servergate.ru/articles/otlichiya-kommutatorov-l1-l2-i-l3/ (accessed: 05.11.2025).
2. Alexhost. (2024). What is MAC Flooding? How to prevent it? Alexhost. Retrieved November 20, 2025, from https://alexhost.com/ru/faq/what-is-mac-flooding-how-to-prevent-it/ (accessed: 20.11.2025).
3. Gontharet, F. (2015). Man-in-The-Middle Attacks & Countermeasures Analysis [Master's thesis, University of Abertay Dundee]. ResearchGate. Retrieved December 10, 2025, from https://www.researchgate.net/publication/340720434_Man-in-The-Middle_Attacks_Countermeasures_Analysis (accessed: 10.12.2025).
4. Thakur, S., Khan, A., Dave, J., & Kaulgud, S. (2018). Three tier architecture with enhanced security at layer 2 and layer 3. International Advanced Research Journal in Science, Engineering and Technology, 5(Special Issue 3), 13–18. Retrieved December 10, 2025, from https://clck.ru/3Qy9Ak (accessed: 10.12.2025).
5. Skorobogatov, S. Yu., Zhdanova, I. M., Kuznetsov, A. V., Osipenko, A. A., & Khabushev, R. R. (2023). A methodology for predicting the impact of cyberattacks on software-defined network elements. Bulletin of the Tula State University. Technical Sciences, (2), 269–274. https://cyberleninka.ru/article/n/metodika-prognozirovaniya-vozdeystviya-kompyuternyh-atak-na-elementy-programmno-konfiguriruemoy-seti (accessed: 11.12.2025).
6. Cisco. (2018). Configure Dynamic Host Configuration Protocol (DHCP) Snooping on a Switch through the Command Line Interface (CLI). Cisco Support. Retrieved December 20, 2025, from https://www.cisco.com/c/en/us/support/docs/smb/switches/cisco-small-business-300-series-managed-switches/smb5515-configure-dynamic-host-configuration-protocol-dhcp-snooping.html (accessed: 20.12.2025).
7. Uymin, A. G. (2024). Computer Networks. L2 Technologies: A Practical Guide for Secondary Vocational Education. Profobrazovanie; IPR MEDIA. Retrieved November 15, 2025, from https://www.iprbookshop.ru/135231.html (accessed: 15.11.2025).
8. Brezular, R. (2024, January 3). Protection against MAC flooding attack. Brezular.com. Retrieved December 9, 2025, from https://brezular.com/2024/01/03/protecting-against-mac-flooding-attack/ (accessed: 09.12.2025).

Информация об авторах

Еремина Елизавета Алексеевна – студент ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И.М. Губкина», г. Москва, e-mail: elizavetaeremina2@gmail.com

Простова Алиса Никитична – студент ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И.М. Губкина», г. Москва, e-mail: prostrova2005@bk.ru

IMPACT OF MAC-FLOODING ATTACKS ON L2 SWITCHES IN A HYBRID NETWORK INFRASTRUCTURE

Eremina E. A.[1], Prostova A. N.[1]

[1]National University of Oil and Gas «Gubkin University»

Abstract. The conducted research reveals the critical vulnerability of L3 devices in hybrid networks during attacks at the channel level. It has been experimentally shown that a classic MAC flooding attack aimed at overflowing the CAM tables of access switches leads not only to a violation of the confidentiality of traffic at the L2 level, but also causes a cascading increase in load on routers (L3) due to the massive generation of unknown unicast traffic. This traffic is redirected to the router, leading to a critical load on its processor, increased response time, and a possible denial of service for the entire network infrastructure.

The paper provides comparative testing of standard protection mechanisms (Port Security, Storm Control) on equipment from various manufacturers under simulated attack conditions. Experiments were conducted on the stand using Cisco, Mikrotik, and Eltex equipment, and the attack was generated using Kali Linux tools. The results demonstrate that activating Port Security in shutdown mode on access ports is the most effective way to block an attack at the source. To ensure the integrated stability of a hybrid network, this measure must be complemented by limiting broadcast traffic at the router level.

The data obtained is of great practical importance for ensuring the fault tolerance and security of modern hybrid network infrastructures combining equipment from various vendors, and allows us to formulate practical recommendations for configuring security for networks combining equipment from various manufacturers in order to prevent the escalation of L2 attacks to the L3 layer.

Keywords: *MAC-flooding, network security, L3 router, L2 switch, CAM table, unknown unicast, Port Security.*

Information about the authors

Eremina Elizaveta Alekseevna – student Gubkin Russian State University of Oil and Gas (National Research University), Moscow, e-mail: elizavetaeremina2@gmail.com

Prostova Alisa Nikitichna – student Gubkin Russian State University of Oil and Gas (National Research University), Moscow, e-mail: prostrova2005@bk.ru