ПРОФЕССИОНАЛИТЕТ, 2025, № 3 (007)

УДК *004.056*

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

ВОПРОСЫ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ОТ АТАКИ CAM TABLE OVERFLOW НА L2 УСТРОЙСТВАХ

Аннотация. В современных локальных сетях атака CAM Table Overflow представляет критическую угрозу безопасности уровня L2, приводящую к переполнению таблицы MAC-адресов коммутатора потоком фейковых адресов. Успешная реализация атаки переводит устройство в режим широковещательной рассылки (flooding), что позволяет злоумышленнику перехватывать конфиденциальный трафик и вызывает критическую нагрузку на ресурсы оборудования (CPU до 85%, RAM до 75%), нарушая доступность сетевых услуг. Целью работы стал сравнительный анализ методов нейтрализации данной угрозы: Port Security, Storm Control и DHCP Snooping. Методология исследования включала моделирование атаки с помощью утилиты macof и оценку эффективности защитных механизмов на оборудовании вендоров Cisco, Eltex и MikroTik. Критериями выбора служили скорость реакции, точность блокировки и влияние на трафик. Результаты экспериментов подтвердили превосходство технологии Port Security. При активации данного механизма коммутатор мгновенно (за 2–5 секунд) блокирует порт нарушителя в режиме secure-shutdown, ограничивая таблицу двумя записями вместо 8124. Нагрузка на процессор снижается до 10%, а оперативная память разгружается до 35%, при этом работа легитимных узлов не прерывается. В отличие от аналогов, Port Security обеспечивает прямую защиту от причины атаки, а не только смягчает её последствия. Сделан вывод, что внедрение Port Security является наиболее универсальным и надежным решением для защиты коммутаторов L2+ от переполнения CAM-таблиц. Рекомендовано использовать данный механизм как базовый

Ключевые слова: CAM таблица, MAC адрес, L2 устройства, защита коммутаторов, Port Security, перехват трафика.

Введение

В современных сетях передачи данных коммутаторы L2 являются критически важным элементом инфраструктуры сети. Атака CAM table overflow — переполнение таблицы MAC-адресов коммутатора — представляет серьезную угрозу безопасности, позволяя злоумышленнику перехватывать трафик и нарушать функционирование сети. Несмотря на известность атаки, многие сетевые администраторы не уделяют достаточного внимания настройке механизмов защиты.

Цель работы: провести сравнительную оценку защиты от атаки CAM table overflow и экспериментально подтвердить эффективность выбранного метода на оборудовании различных вендоров.

Задачи исследования:

- проанализировать механизм атаки CAM table overflow;
- исследовать существующие методы защиты и выбрать наиболее эффективный;
- реализовать конфигурации выбранного метода защиты на коммутаторах Cisco, Eltex, MikroTik;
- провести анализ влияния атаки и метода защиты на ресурсы устройства и сетевую задержку
- экспериментально доказать эффективность защиты;

Литературный обзор

С точки зрения IEEE(стандарт спецификации), CAM-Table overflow — это атака, эксплуатирующее стандартное поведение коммутатора, описываемое IEEE 802.3. RFC 2863 хоть и не определяет MAC-адреса напрямую, описывает стандартизацию управления интерфейсами, их обслуживание и свойства.

Современные коммутаторы работает следующим образом. получает данные от обращающихся к нему устройств и постепенно заполняет CAM-таблицу (таблицу коммутации) их

MAC-адресами. При последующих обращениях коммутатор считывает адрес устройства-отправителя, анализирует таблицу коммутации и определяет по ней, на какое устройство нужно переслать данные [1]. Прочие компьютеры при этом не «знают» о факте передачи информации, поскольку она не имеет к ним отношения.

В статье [2] описан смысл атаки MAC-flooding, так как обе атаки используют схожие механизмы переполнения таблицы MAC-адресов в коммутаторах. Она помогает глубже понять методы реализации атаки, а также существующие подходы к защите и обнаружению, что важно для критического анализа в публикации.

Статья [7] помогла подробно понять механизм атаки CAM Table Overflow и принципы её реализации в локальных сетях. Полученные сведения использованы при описании теоретической части работы и объяснении уязвимости коммутаторов второго уровня.

Анализ темы

Как именно происходит атаки с переполнением CAM-таблицы? Злоумышленник использует специализированное программное обеспечение, которое генерирует и передает в сеть непрерывный поток Ethernet-кадров, содержащих случайно сгенерированные MAC-адреса. Данные кадры поступают на один из портов целевого коммутатора, который в соответствии со стандартной логикой работы начинает добавлять эти фиктивные адреса в свою CAM-таблицу [2].

По мере заполнения таблицы до ее максимальной емкости коммутатор либо прекращает добавление новых записей, либо начинает вытеснять ранее зарегистрированные легитимные записи. Это нарушает нормальный процесс коммутации - при поступлении кадров на адреса, отсутствующие в переполненной таблице, коммутатор переходит в режим широковещательной рассылки, дублируя трафик на все порты, принадлежащие соответствующей VLAN [2].

Возникающая уязвимость позволяет злоумышленнику, находящемуся в том же широковещательном домене, осуществлять перехват всего сетевого трафика, включая передачу конфиденциальной информации, учетных данных пользователей и других критически важных данных.

Для предотвращения атаки CAM-table overflow существует 3 основных метода защиты:

1. Port Security

Port-Security – механизм обеспечения безопасности и контроля доступа, основанный на контроле изучаемых MAC-адресов. Может использоваться как дополнение существующей аутентификации 802.1x и аутентификации MAC. Port-security контролирует доступ неавторизованных устройств к сети, проверяя MAC-адрес источника принятого кадра и доступ к неавторизованным устройствам, проверяя MAC-адрес назначения отправленного кадра [3].

2. Storm-control

Storm control (контроль шторма) – это сетевая функция, которая предотвращает перегрузку сети из-за чрезмерного широковещательного, многоадресного или неизвестного одноадресного трафика. Функция storm-control задаёт максимальное количество передаваемых пакетов в секунду, тем самым отбрасывая ненужные пакеты при превышении данного значения [6].

3. DHCP Snooping

DHCP Snooping – это механизм безопасности на коммутаторах, который защищает от атак через подмену DHCP-сервера и косвенно помогает предотвращать CAM table overflow. Принцип работы основан на разделении портов на доверенные (для подключения легитимных DHCP-серверов) и недоверенные (для пользовательских устройств). На недоверенных портах блокируются все DHCP-ответы, что предотвращает подключение фальшивых серверов. Одновременно механизм автоматически создает и поддерживает базу данных соответствий IP-MAC-адресов, полученных через легитимные DHCP-транзакции [4].

Для корректного сравнения методов необходимо разграничить уровни их воздействия на архитектуру коммутатора. Атака CAM Table Overflow эксплуатирует уязвимость плоскости данных (Data Plane), перегружая таблицу коммутации.

Port Security является мерой защиты именно плоскости данных (Data Plane protection),

так как контролирует входящий трафик на уровне порта и предотвращает запись нелегитимных MAC-адресов в аппаратную таблицу. Это прямой метод нейтрализации вектора атаки.

Storm Control также относится к защите плоскости данных, но работает реактивно: он не предотвращает заполнение таблицы, а лишь ограничивает интенсивность широковещательного трафика (последствие атаки), когда таблица уже переполнена и коммутатор перешел в режим flooding.

DHCP Snooping функционирует преимущественно в плоскости управления (Control Plane), фильтруя служебные протоколы. Сам по себе он не защищает от прямого заполнения CAM-таблицы фейковыми MAC-адресами. Его эффективность против данной атаки раскрывается только в комплексе с технологиями Dynamic ARP Inspection (DAI) и IP Source Guard (IPSG). В такой связке DHCP Snooping формирует доверенную базу соответствий (binding table IP-MAC-порт), которую используют DAI и IPSG для блокировки пакетов с подмененными адресами на уровне портов, тем самым косвенно предотвращая переполнение. Сравним данные методы для выяснения самого эффективного в контексте защиты от атаки переполнения CAM таблицы:

Таблица 1. Сравнительная характеристика методов защиты

Критерий	Port Security	Storm Control	DHCP Snooping (в связке с DAI/IPSG)
Основная функция	Защита от переполнения CAM-таблицы	Борьба с широковещательными штормами	Защита от подмены DHCP-сервера
Эффективность против CAM table overflow	Прямая и полная защита	Косвенная защита (борьба с последствиями)	Косвенная защита (предотвращение атак через DHCP)
Уровень защиты	Data Plane (прямая защита порта)	Data Plane (ограничение трафика)	Control Plane + Data Plane (комплексная фильтрация)
Принцип работы	Ограничение MAC-адресов на порту, блокировка при нарушении	Ограничение трафика по типам (broadcast/unicast/multicast)	Фильтрация DHCP-сообщений, создание базы доверенных клиентов
Реакция на атаку	Мгновенная блокировка порта	Подавление превышающего трафика	Блокировка неавторизованных DHCP-серверов
Влияние на работу сети	Локальное (только на атакованном порту)	Общее (защищает всю подсеть)	Общее (защищает всю подсеть)
Простота настройки	Простая конфигурация	Требует тонкой настройки порогов	Сложная настройка, требует интеграции с другими механизмами
Преимущества	Наиболее эффективен против целевой атаки, простая настройка, минимальные ложные срабатывания	Защита от последствий атаки, контроль широковещательного трафика	Дополнительная защита сети, создание базы доверенных клиентов
Недостатки	Требует точной настройки лимитов MAC-адресов	Не предотвращает атаку, только смягчает последствия	Не защищает напрямую от CAM table overflow, сложная настройка

Таким образом, Port Security является наиболее эффективным самодостаточным методом защиты непосредственно от вектора атаки CAM Table Overflow, обеспечивая превентивную блокировку на уровне порта (Data Plane). В то время как Storm Control лишь смягчает последствия атаки, а DHCP Snooping требует развертывания дополнительного комплекса мер (DAI, IPSG) для достижения сопоставимого уровня защиты. Учитывая критерии простоты внедрения и прямой направленности действия, для целей данного исследования выбран метод Port Security.

Материалы и методы (ход исследования)

Перейдем к практической реализации на оборудованиях различных вендоров:

```
enable
configure terminal
switchport port-security
interface fastethernet 0/1
```

```
switchport port-security
switchport port-security maximum 2
switchport port-security violation shutdown
switchport port-security mac-addres sticky
end
```

```
Mac Entries for Vlan 30:
---------------------------
Dynamic Address Count  : 0
Static  Address Count  : 0
Total Mac Addresses    : 0

Total Mac Address Space Available: 8043

Switch#
Switch#
Switch#enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#switchport port-security
Switch(config)#interface fastethernet 0/1
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security maximum 2
Switch(config-if)#switchport port-security violation shutdown
Switch(config-if)#switchport port-security mac-addres sticky
Switch(config-if)#end
Switch#
```

Рис. 1. Конфигурация Port-Security на Cisco

```
configure terminal
interface fastEthernet0/1
switchport port-security mode max-addresses
switchport port-security mac-limit 3
switchport port-security action shutdown
switchport port-security enable
exit
exit
copy running-config startup-config
```

```
console#configure terminal
console(config)#interface Fastethernet0/1
console(config-if)#switchport port-security mode max-addresses
console(config-if)#switchport port-security mac-limit 3
console(config-if)#switchport port-security action shutdown
console(config-if)#switchport port-security enable
console(config-if)#exit
console(config)#exit
console#copy running-config startup-config
Building configuration ...
[OK]
console#
```

Рис.2. Конфигурация Port-Security на Eltex

```
/interface ethernet switch rule
add ports=ether1 learn-limit=2 learning=disabled action=drop disabled=no
```

```
switch:
[admin@MikroTik] /interface ethernet switch rule> /
[admin@MikroTik] > interface ethernet switch rule
[admin@MikroTik] /interface ethernet switch rule> add ports=ether1 learn-limit=2 learning=disabled
  \ action=drop disabled=no
[admin@MikroTik] /interface ethernet switch rule> /
```

Рис. 3. Конфигурация Port-Security на MikroTik

Далее проведем эксперимент, где проведем атаку CAM-table overflow на коммутатор с базовыми настройками, настроим на коммутаторе port-security и убедимся в эффективности работы port-security.

Топология сети:

Рис. 4. Топология экспериментальной сети

Подключаем компьютер пользователя и злоумышленника к коммутатору, и проводим базовую настройку коммутатора, следующими командами:

```
Switch> enable
Switch# configure terminal
Switch(config)# hostname CAM-TEST-SWITCH
Switch(config)# no ip domain-lookup
Switch(config)# interface range fastethernet 0/1-2
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 1
Switch(config-if-range)# no shutdown
Switch(config-if-range)# exit
```

Мы установили компьютеры в один VLAN, чтобы эксперимент не вывел из строя коммутатор. Далее установили компьютерам статические ip адреса и проверили CAM-таблицу

```
Switch#show mac address-table count

Mac Entries for Vlan 1:
---------------------------
Dynamic Address Count  : 2
Static  Address Count  : 0
Total Mac Addresses    : 2

Mac Entries for Vlan 3:
---------------------------
Dynamic Address Count  : 0
Static  Address Count  : 0
Total Mac Addresses    : 0

Mac Entries for Vlan 10:
---------------------------
Dynamic Address Count  : 0
Static  Address Count  : 0
Total Mac Addresses    : 0
```

Рис.5. CAM-таблица до атаки

На компьютере злоумышленника используя команду

sudo macof -i eth0 -n 15000

проводим атаку на коммутатор без включенной защиты port-security. Смотрим количество mac адресов и убеждаемся в переполнении

```
Switch#show mac address-table dynamic | count
% Incomplete command.

Switch#show mac address-table count

Mac Entries for Vlan 1:
---------------------------
Dynamic Address Count   : 8124
Static  Address Count   : 0
Total Mac Addresses     : 8124

Mac Entries for Vlan 3:
---------------------------
Dynamic Address Count   : 0
Static  Address Count   : 0
Total Mac Addresses     : 0

Mac Entries for Vlan 10:
---------------------------
Dynamic Address Count   : 0
Static  Address Count   : 0
Total Mac Addresses     : 0
```

Рис. 6. CAM-таблица после атаки

```
4    102c.2206.60ab    DYNAMIC     Fa1/0/29
4    102e.b058.eda4    DYNAMIC     Fa1/0/29
4    102e.ea16.d70b    DYNAMIC     Fa1/0/29
4    1032.4973.92fa    DYNAMIC     Fa1/0/29
4    1035.ad03.ad4e    DYNAMIC     Fa1/0/29
4    1037.8c62.1536    DYNAMIC     Fa1/0/29
4    1037.d535.8552    DYNAMIC     Fa1/0/29
4    1038.0031.5554    DYNAMIC     Fa1/0/29
4    103c.3b7c.76e7    DYNAMIC     Fa1/0/29
4    1045.d26c.25d7    DYNAMIC     Fa1/0/29
4    104a.425a.e135    DYNAMIC     Fa1/0/29
4    104f.9e4e.b160    DYNAMIC     Fa1/0/29
4    1054.4474.9961    DYNAMIC     Fa1/0/29
4    1055.c418.a4b4    DYNAMIC     Fa1/0/29
4    1056.c35c.01d5    DYNAMIC     Fa1/0/29
4    105f.3614.2f5b    DYNAMIC     Fa1/0/29
4    1062.6336.daa4    DYNAMIC     Fa1/0/29
4    1062.af62.b3df    DYNAMIC     Fa1/0/29
4    106d.a55b.eaef    DYNAMIC     Fa1/0/29
4    1071.6823.e21a    DYNAMIC     Fa1/0/29
4    1074.c256.3d48    DYNAMIC     Fa1/0/29
4    1076.ca35.61ad    DYNAMIC     Fa1/0/29
4    107d.ec7b.5235    DYNAMIC     Fa1/0/29
4    107e.342f.31
```

Рис. 7. Содержимое CAM-таблица после атаки

Обсуждение

Приведем результаты мониторинга в таблицу:

Таблица 2. Результаты мониторинга

Время	Количество адресов	Состояние	CPU (%)	RAM (%)
0 сек	2	Начало атаки	5	30
10 сек	2458	Активное заполнение	45	55
20 сек	8124	Таблица переполнена	85	75
30 сек	8124	Режим flooding	85-90	75

Как можно заметить, трафик между коммутатором и пользователем становится доступен

для перехвата. Переходим к настройке Port-Security. На коммутаторе вводим команды

```
Switch# configure terminal
Switch(config)# interface fastethernet 0/1
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 2
Switch(config-if)# switchport port-security violation shutdown
Switch(config-if)# switchport port-security mac-address sticky
Switch(config-if)# end
```

Таким образом проведена конфигурация port-security (на других коммутаторах аналогично вводятся свои команды, приведенные выше). Проводим атаку уже известной командой.

sudo macof -i eth0 -n 15000

Убеждаемся в работе метода защиты:

```
Mac Entries for Vlan 30:
---------------------------
Dynamic Address Count  : 0
Static  Address Count  : 0
Total Mac Addresses    : 0

Total Mac Address Space Available: 8043

Switch#show mac address-table count

Mac Entries for Vlan 1:
---------------------------
Dynamic Address Count  : 2
Static  Address Count  : 0
Total Mac Addresses    : 2

Mac Entries for Vlan 3:
---------------------------
Dynamic Address Count  : 0
Static  Address Count  : 0
Total Mac Addresses    : 0

Mac Entries for Vlan 10:
```

Рис. 8. CAM-таблица после атаки

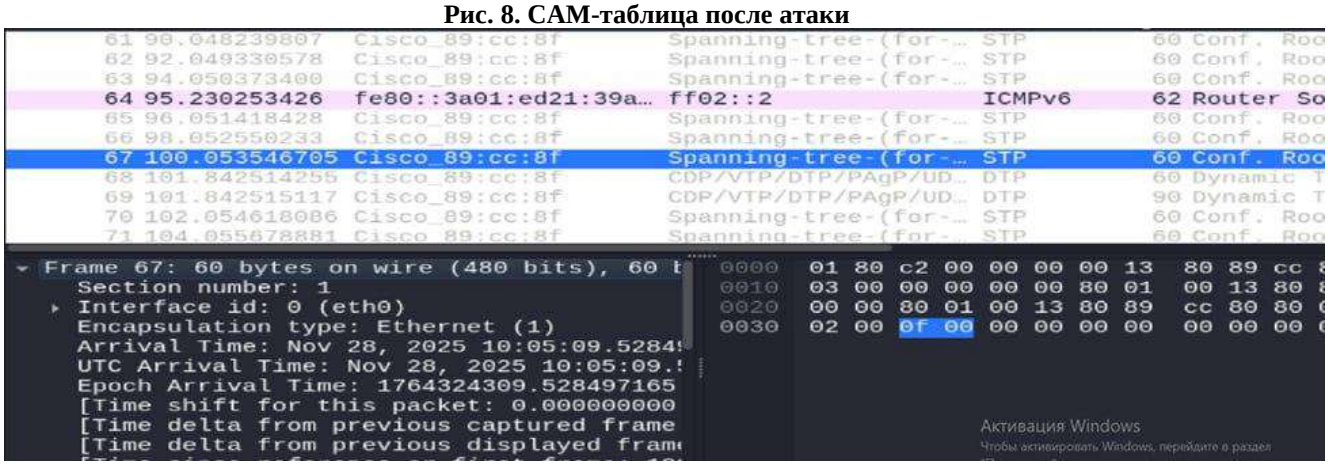

Рис. 9. Wireshark блокировка компьютера атакующего

Подведем анализ эффективности защиты в виде таблицы

Таблица 3. Эффективности защиты

Параметр	Без защиты	С Port Security
Заполнение CAM- таблицы	8124 записей	2 записи
Время реакции	20-30 секунд	2-5 секунд
Состояние порта	Active (flooding)	Secure-shutdown
Возможность перехвата	Да	Нет

Влияние на легитный трафик	Прерывается	Не прерывается
Средняя задержка (Latency)	145 мс (потери 40%)	1.2 мс (стабильно)
Нагрузка на CPU	85-95%	5-10%
Нагрузка на RAM	75%	30-35%

Эксперимент моделировал условия предельной нагрузки (stress-test), при которых утилизация CPU достигала 90%, а таблица MAC-адресов была переполнена на 100%. В таких нестандартных условиях коммутатор переходил в аварийный режим работы (flooding), что привело к критической деградации сервиса. Применение Port Security позволило исключить работу устройства в стрессовом режиме, поддерживая утилизацию ресурсов в пределах штатных значений (<10%) даже при интенсивной внешней атаке

Дополнительно была проведена оценка влияния механизмов защиты на сетевую задержку (latency). В режиме атаки без защиты средняя задержка возросла с 1 мс до 150 мс с потерей 40% пакетов. При активации Port Security после кратковременного прерывания (2 сек) задержка стабилизировалась на уровне 1.2 мс, что подтверждает минимальное влияние механизма защиты на производительность легитимного трафика.

Заключение

В ходе нашего исследования мы разобрали существующие методы защиты от атаки CAM-table overflow, а также на практике убедились в эффективности метода port-security. Было установлено, что данный метод защиты является универсальным решением от атаки, который не только предотвращает утечку трафика, но и не даёт злоумышленнику нагрузить устройство ненужными данными, в следствие чего идет большая нагрузка на оперативную память и процессор, а также вызывает задержку передачи трафика вплоть до 145 мс и потери пакетов (40%).

Эксперимент подтвердил, что Port Security является надежным и эффективным механизмом защиты коммутаторов L2 от атак переполнения CAM-таблицы. Коммутаторы, настроенные приведенным методом, будут защищены от возможных атак, направленных на переполнение таблицы адресов, и будут продолжать выполнение своих функций.

Библиографический список

1. Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы : учебник для вузов / В. Г. Олифер, Н. А. Олифер. — 5-е изд., юбил. – Санкт-Петербург : Питер, 2021. – 1008 с. : ил. – (Серия «Учебник для вузов»). – ISBN 978-5-4461-1584-0.
2. АТАКА CAM-TABLE OVERFLOW. МЕТОДЫ ЗАЩИТЫ [Электронный ресурс] // Security.Lab – URL: https://cyberleninka.ru/article/n/ataka-cam-table-overflow-metody-zaschity (дата обращения: 11.11.2025).
3. Настройка Port Security на коммутаторах SNR / [Электронный ресурс] // Документация NAG: [сайт]. – URL: https://nag.wiki/pages/viewpage.action?pageId=25107728(дата обращения 11.11.2025)
4. Уймин, А. Г. Компьютерные сети. L2-технологии: Практикум / А. Г. Уймин. – Москва: Ай Пи Ар Медиа, 2024. - 191 с. – ISBN 978-5-4497-2539-4. EDN AXDYGY
5. Cisco Catalyst 2960 Series Switches Configuration Guide [Электронный ресурс] // Cisco Systems. – 2023. URL: https://www.cisco.com/c/en/us/support/switches/catalyst-2960-series switches/products-installation-and-configuration-guides-list.html.
6. Основы сетевой безопасности: защита коммутаторов L2 [Электронный ресурс] // Habr: статья. – 2020. – URL: https://habr.com/ru/articles/502480/ (дата обращения: 11.01.2025).
7. Трещев И.А. «О реализации атак типа MAC-FLOOD» / статья (eLIBRARY / научная публикация). // 2022. URL: https://elibrary.ru/item.asp?id=49992198 (дата обращения 11.11.2025).
8. Настройка Port Security на коммутаторах Eltex MES1400/MES2400 // База знаний Eltex [Электронный ресурс] // Документация. – URL: https://eltexcm.ru/baza-znanij/ethernet-kommutatory-mes/mes14xx24xx3400-xx37xx/interfejsy-vlan/mes-nastrojka-port-security-mes1400-mes2400.html

References

1. Olifer, V. G., & Olifer, N. A. (2021). *Computer networks: Principles, technologies, and protocols* (5th anniversary ed.). Piter.
2. *CAM-table overflow attack: Protection methods*. (n.d.). Security.Lab. Retrieved November 11, 2025, from https://cyberleninka.ru/article/n/ataka-cam-table-overflow-metody-zaschity
3. NAG. (n.d.). *Configuring Port Security on SNR switches*. NAG Documentation. Retrieved November 11, 2025, from https://nag.wiki/pages/viewpage.action?pageId=25107728
4. Uymin, A. G. (2024). *Computer networks: L2 technologies. A practical course*. IPR Media.
5. Cisco Systems. (2023). *Cisco Catalyst 2960 Series Switches Configuration Guide*. https://www.cisco.com/c/en/us/support/switches/catalyst-2960-series-switches/products-installation-and-configuration-guides-list.html
6. *Fundamentals of network security: Protecting L2 switches*. (2020). Habr. Retrieved January 11, 2025, from https://habr.com/ru/articles/502480/
7. Treshchev, I. A. (2022). On the implementation of MAC-flood attacks. eLIBRARY.RU. Retrieved November 11, 2025, from https://elibrary.ru/item.asp?id=49992198
8. Eltex. (n.d.). *Configuring Port Security on Eltex MES1400/MES2400 switches*. Eltex Knowledge Base. https://eltexcm.ru/baza-znanij/ethernet-kommutatory-mes/mes14xx24xx3400-xx37xx/interfejsy-vlan/mes-nastrojka-port-security-mes1400-mes2400.html

Информация об авторах

Фоменко Артём Владимирович – студент 3-его курса, факультет КБ ТЭК, группы КИ-23-01 ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И.М. Губкина», г. Москва, e-mail: 1studentnow1@gmail.com

Зеленов Ярослав Юрьевич – студент 3-его курса, факультет КБ ТЭК группы КИ-23-01 ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И.М. Губкина», г. Москва, e-mail: mobzila567@gmail.com

A. V. Fomenko [1], Ya. Yu. Zelenov [1]

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

PROTECTION AGAINST CAM TABLE OVERFLOW ATTACKS ON L2+ DEVICES

Abstract. In modern local area networks, the CAM Table Overflow attack poses a critical L2 security threat, causing the switch's MAC address table to become flooded with a flood of fake addresses. A successful attack puts the device into flooding mode, allowing the attacker to intercept sensitive traffic and places a critical load on hardware resources (CPU up to 85%, RAM up to 75%), disrupting network service availability. The objective of this study was to compare mitigation methods for this threat: Port Security, Storm Control, and DHCP Snooping. The research methodology included attack simulation using the macof utility and an evaluation of the effectiveness of defense mechanisms on Cisco, Eltex, and MikroTik equipment. The selection criteria included response speed, blocking accuracy, and impact on traffic. The experimental results confirmed the superiority of Port Security technology. When this mechanism is activated, the switch instantly (within 2-5 seconds) blocks the intruder's port in secure-shutdown mode, limiting the table to two entries instead of 8124. CPU load is reduced to 10%, and RAM is unloaded to 35%, while legitimate nodes continue to operate. Unlike similar mechanisms, Port Security provides direct protection against the root cause of the attack, rather than merely mitigating its consequences. It is concluded that implementing Port Security is the most universal and reliable solution for protecting L2+ switches from CAM table overflows. It is recommended to use this mechanism as a basic one.

Keywords: CAM table, MAC address, L2+ device, switch protection, Port Security, traffic interception

Information about the authors

Fomenko Artem Vladimirovich - 3rd year student, Faculty of Design Bureau of Fuel and Energy Complex, group KI-23-01, Federal State Autonomous Educational Institution of Higher Education "Gubkin Russian State University of Oil and Gas (National Research University), Moscow, e-mail: 1studentnow1@gmail.com

Zelenov Yaroslav Yurievich - 3rd year student, Faculty of Design Bureau of Fuel and Energy Complex group KI-23-01 of the Federal State Autonomous Educational Institution of Higher Education "RSU of Oil and Gas (NRU) named after I.M. Gubkin", Moscow, e-mail: mobzila567@gmail.com