УДК 004.056

Дорофеева Полина Алексеевна, студентка факультета комплексной безопасности ТЭК, Российский государственный университет нефти и газа имени И.М. Губкина, г. Москва

Dorofeeva Polina Alekseevna, Student of the Faculty of Integrated Security of Fuel and Energy Complex, Gubkin Russian State University of Oil and Gas, Moscow

Пазилов Даниил Александрович, студент факультета комплексной безопасности ТЭК, Российский государственный университет нефти и газа имени И.М. Губкина, г. Москва

Pazilov Daniil Aleksandrovich, Student of the Faculty of Integrated Security of Fuel and Energy Complex, Gubkin Russian State University of Oil and Gas, Moscow

НАСТРОЙКА И ТЕСТИРОВАНИЕ ЗАЩИТЫ PORT SECURITY

В статье рассматриваются принципы функционирования и практическая реализация механизма Port Security, предназначенного для защиты коммутаторов от атак, направленных на переполнение MAC-таблиц и несанкционированный доступ к сетевым ресурсам. Описаны теоретические основы работы функции, режимы реагирования на нарушение безопасности, а также проведён сравнительный анализ работы Port Security на оборудовании трёх различных производителей — Cisco, Eltex и MikroTik. Представлены результаты экспериментального тестирования атаки типа MAC-Flooding и последующего включения защитных механизмов. Полученные данные демонстрируют эффективность использования Port Security при обеспечении сетевой безопасности на канальном уровне и подчёркивают необходимость его настройки в корпоративных сетях. Особое внимание уделено сравнительным особенностям реализации Port Security и поведению оборудования в условиях атаки.

The article examines the principles of operation and practical implementation of the Port Security mechanism, designed to protect switches from attacks aimed at

MAC table overflow and unauthorized access to network resources. Theoretical foundations of the feature’s operation, security violation response modes, and a comparative analysis of Port Security performance on equipment from three different manufacturers — Cisco, Eltex, and MikroTik — are described. The results of experimental testing of a MAC flooding attack and subsequent activation of protection mechanisms are presented. The obtained data demonstrate the effectiveness of using Port Security to ensure network security at the data link layer and emphasize the importance of its configuration in corporate networks. Special attention is given to the comparative characteristics of Port Security implementation and the behavior of network devices under attack conditions.

Ключевые слова: Port Security, MAC-Flooding, безопасность сети, коммутатор, Cisco, Eltex, MikroTik, защита портов.

Keywords: Port Security, MAC Flooding, network security, switch, Cisco, Eltex, MikroTik, port protection.

Обзор литературы

Рассмотрим топологию, описывающую сеть из компьютеров PC1, PC2, связанных между собой с помощью коммутатора:

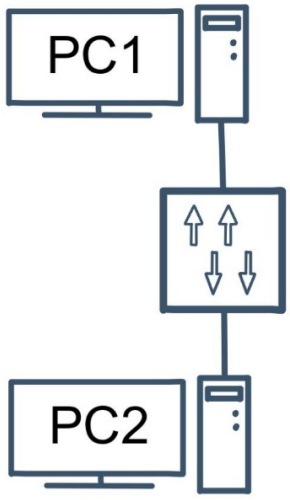


Рисунок 1 – Топология примера

Предположим, что с PC1 были отправлены некоторые данные,

предназначенные получателю PC2 с определенным MAC-адресом. Но наш коммутатор, получив пакеты, не знает кому их направить далее, так как не имеет в своей таблице устройства с таким адресом. Его следующим

действием становится поиск в сети. Производится широковещательный запрос на все подключённые к интерфейсам устройства, на который, в конечном итоге, должен откликнуться PC2, увидев свой адрес в пакете. После чего наш коммутатор может спокойно доставить данные до получателя.

Таким образом, была произведена отправка данных с PC1 на PC2. При следующей передаче трафика коммутатор обратиться к устройству, чей MAC-адрес содержится в таблице MAC-адресов.

Максимальный размер такой таблицы ограничен, чем обычно и пользуются злоумышленники. Чтобы переполнить её, достаточно сымитировать отправку фреймов с огромным количеством неизвестных для коммутатора адресов получателей. В случае переполнения MAC-таблицы коммутатор рассылает все полученные данные на каждый из имеющихся портов. В таком случае, злоумышленнику, подключённому к рассматриваемой сети и находящемуся в нужном VLAN-е, остается только просмотреть все проходящие пакеты, проходящие через атакуемый коммутатор. Чтобы избежать подобной утечки данных, необходимо правильно настроить Port security на коммутаторе.

Port Security – одна из важнейших функций защиты коммутаторов, призванная ограничивать количество поступающих MAC-адресов в таблицу коммутатора до допустимого администратором максимума. Таким образом, во время привязки все неподходящие адреса будут проигнорированы, а далее коммутатор будет следовать одному из трёх сценариев, которые также будут рассмотрены в этой статье. С помощью Port Security стало возможным предотвратить такие атаки как DHCP Starvation, MAC-Flooding (переполнение таблицы коммутации), MAC-Spoofing (подмена MAC-адресов).

Типы изученных MAC-адресов:

1. Статические MAC-адреса - MAC-адреса, которые вручную настроены на порту, из режима конфигурации порта.

2. Динамические MAC-адреса - MAC-адреса, которые динамически изучаются и хранятся только в таблице адресов. Стираются при перезапуске

коммутатора.

3. Sticky MAC-адреса - MAC-адреса, которые могут быть изучены динамически или сконфигурированы вручную, затем сохранены в таблице адресов и добавлены в текущую конфигурацию. Чтобы использовать sticky-режим запоминания адресов, необходимо настроить sticky-обучение. Без включения обучения адреса будут удаляться из конфигурации при перезагрузке или выключении коммутатора.

Режимы реагирования:

Port security имеет три режима реагирования на нарушение безопасности:

1. Protect (none) — когда количество безопасных MAC-адресов достигает максимального ограничения настроенного на порту, пакеты с неизвестным MAC-адресом отправителя отбрасываются, пока не будет освобождено место среди безопасных MAC-адресов или их количеств не будет увеличено.

2. Restrict (send-alarm) — когда количество безопасных MAC-адресов достигает предела, настроенного на порту, пакеты с неизвестным MAC-адресом отправителя отбрасываются пока не будет освобождено место среди безопасных MAC-адресов или их количеств не будет увеличено. В этом режиме при нарушении безопасности отправляются SNMP trap и сообщение syslog.

3. Shutdown (send-disable) — режим, установленный на коммутаторах по умолчанию. Нарушение безопасности приводит к блокировке интерфейса и его выключению. Отправляются SNMP trap и сообщение syslog.

Таблица 1 - Сценарии реагирования

Режим реагирования	Передача траффика	Отправка сообщения syslog	Увеличение счётчика нарушений	Выключение порта
Protect	-	-	-	+

Restrict	-	+	+	-
Shutdown	-	+	+	+

Таблица 2 – Характеристики оборудования

Производитель	Системное ПО	Порты	Буфер	Таблица MAC, макс. записей	Port Security
MikroTik	SwOS Version 6.48.4	24	2 МБ	До 16000	-
Eltex	Version 10.2.5.2	24	512 КБ	До 8192	+
Cisco	Cisco IOS Software, Version 15.0(2)SE9	24	2 МБ	До 8192	+

Вопросы безопасности локальных сетей и механизма защиты портов коммутатора рассматривались в ряде работ. В исследовании Р.Р. Якубова и А.А. Сулейманова [2] анализируются различные механизмы защиты коммутаторов и их уязвимости. И.В. Соколов [3] подробно описывает методы противодействия атакам, связанным с переполнением MAC-таблицы. В работе К.Д. Новикова [4] исследуется применение Port Security для обеспечения безопасности сетевой инфраструктуры. Однако во всех этих исследованиях основной акцент сделан либо на теоретическом анализе, либо на рассмотрении механизмов защиты в рамках одного типа оборудования.
В отличие от перечисленных источников, в данной статье проведён сравнительный анализ работы Port Security на трёх разных типах коммутаторов (Cisco, Eltex и Mikrotik), а также выполнено практическое

тестирование MAC-Flooding атаки и рассмотрены реальные результаты её влияния на сеть.

Методы исследования

Тип исследования: экспериментальное.

В ходе эксперимента была построена топология из трёх ПК и коммутатора. С атакующего устройства (PC3) при помощи утилиты Macof (пакет Dsniff) производилась атака MAC-Flooding. На разных коммутаторах (Cisco Catalyst 2960, Eltex MES1428 и MikroTik CRS326-24G-2S+RM) была отключена встроенная защита, а затем включена функция Port Security (или аналогичные механизмы). Далее фиксировались результаты работы устройств в разных режимах.

Результаты исследования

Рассмотрим топологию:

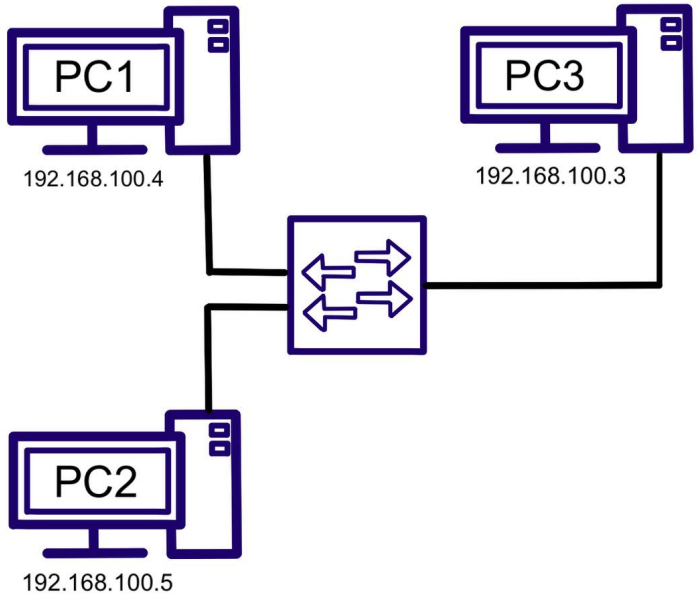


Рисунок 2 - Топология

Для демонстрации работы port security была произведена MAC-Flooding атака на коммутаторы Cisco, Eltex, MikroTik. После была осуществлена настройка Port Security на каждом из них. PC3 - наше атакующее устройство. MAC-Flooding был произведён с помощью инструмента Macof из набора DSniff предназначенного для анализа сетевого трафика.

1. Для начала компьютерам была назначена статическая IP-адресация.

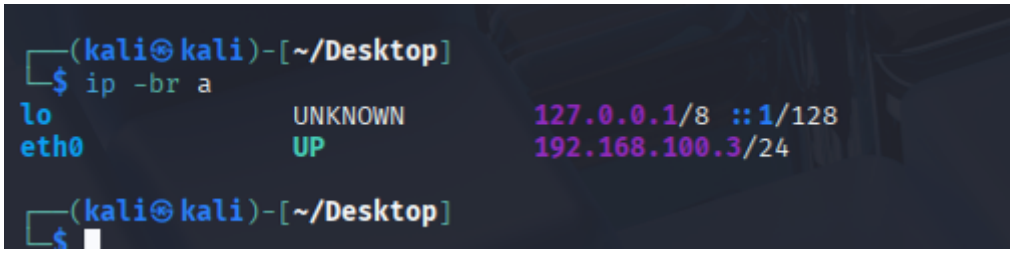


Рисунок 3 - IPv4 на устройстве PC3

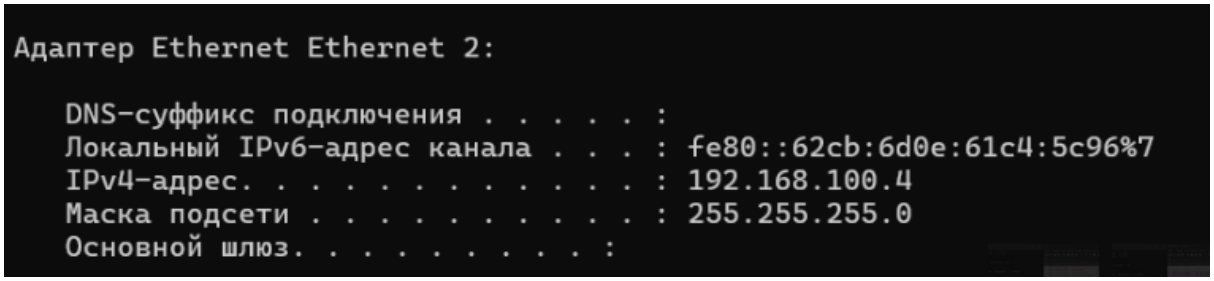


Рисунок 4 - IPv4 на устройстве PC1

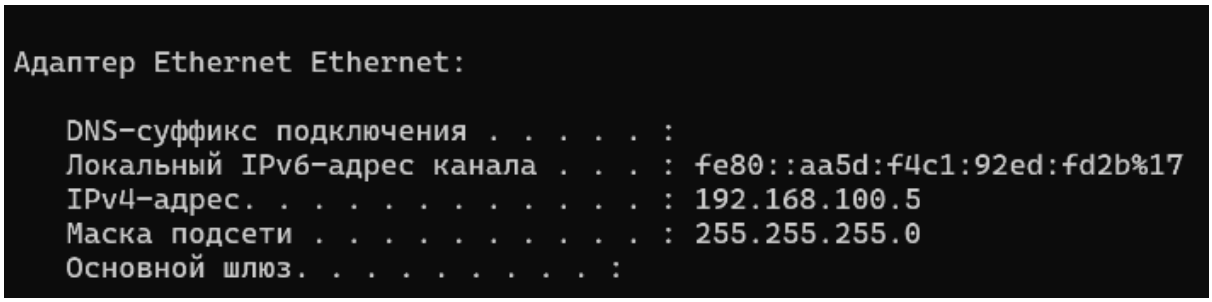


Рисунок 5 - IPv4 на устройстве PC2

2. На коммутаторах Mikrotik, Cisco и Eltex атакующее устройство было подключено к 24 порту. Для успешного проведения атаки была отключена система защиты порта.

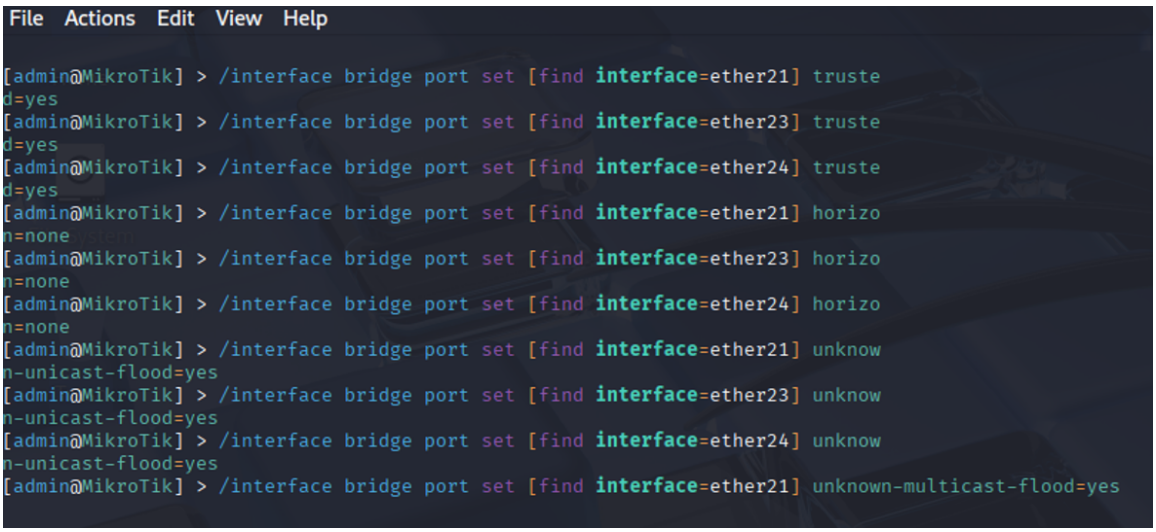


Рисунок 6 - Отключение защиты порта на Mikrotik

```
[admin@MikroTik] > /interface bridge port set [find interface=ether23] unknown-multicast-flood=yes
[admin@MikroTik] > /interface bridge port set [find interface=ether24] unknown-multicast-flood=yes
[admin@MikroTik] > /interface bridge port set [find interface=ether21] br-flood=yes
bridge  broadcast-flood
[admin@MikroTik] > /interface bridge port set [find interface=ether21] broadcast-flood=yes
[admin@MikroTik] > /interface bridge port set [find interface=ether23] broadcast-flood=yes
[admin@MikroTik] > /interface bridge port set [find interface=ether24] broadcast-flood=yes
[admin@MikroTik] >
```

Рисунок 7 - Отключение защиты порта на Mikrotik

```
SW2960#show port-security interface FastEthe
SW2960#show port-security interface FastEthernet0/22
Port Security              : Disabled
Port Status                : Secure-down
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 0
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0

SW2960#show port-security interface FastEthernet0/21
Port Security              : Disabled
Port Status                : Secure-down
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 0
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0

SW2960#show port-security interface FastEthernet0/23
Port Security              : Disabled
Port Status                : Secure-down
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 0
```

Рисунок 8 - Отключение защиты порта на Cisco

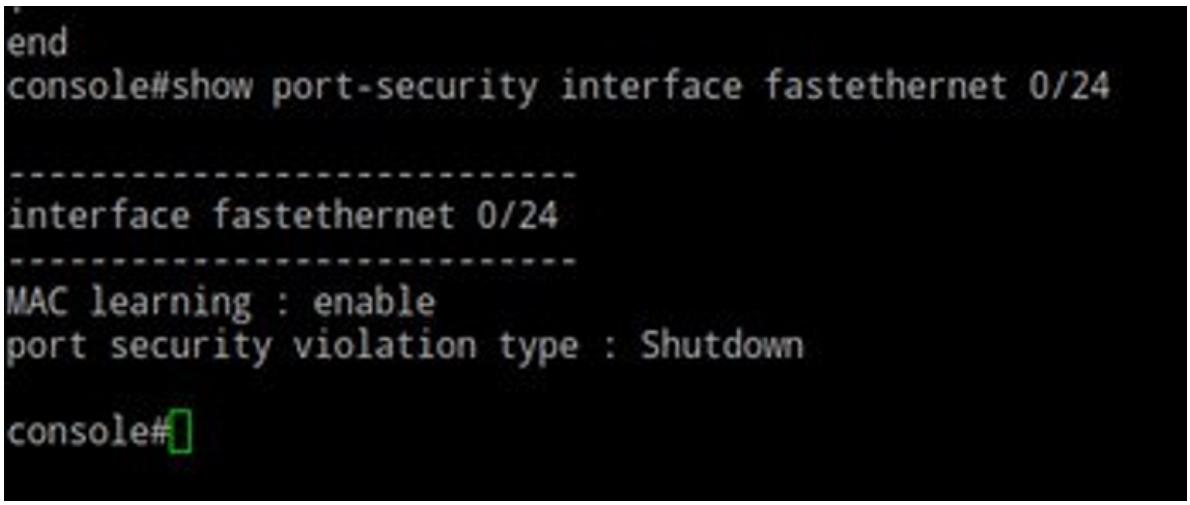


Рисунок 9 - Отключение защиты порта на Eltex

3. Далее с помощью утилиты dsniff команды macoff -i eth0 -d <ip-адрес коммутатора> было сгенерировано бесконечное количество MAC-адресов.

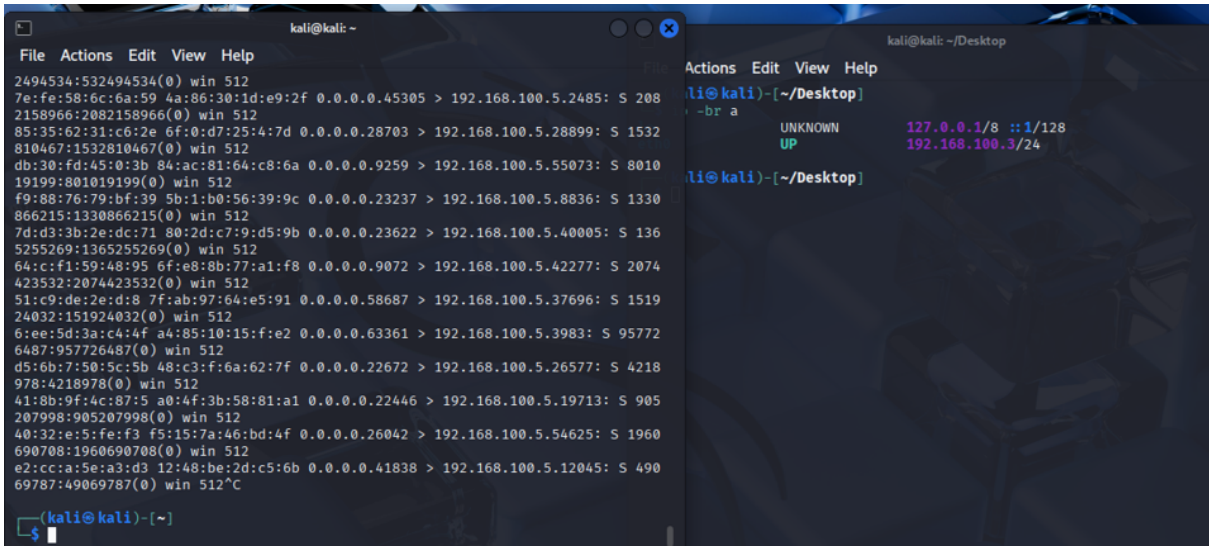


Рисунок 10 - Работа утилиты dsniff

4. Во время атаки таблица MAC - адресов переполняется и имеет вид, показанный на рисунках 11 - 12.

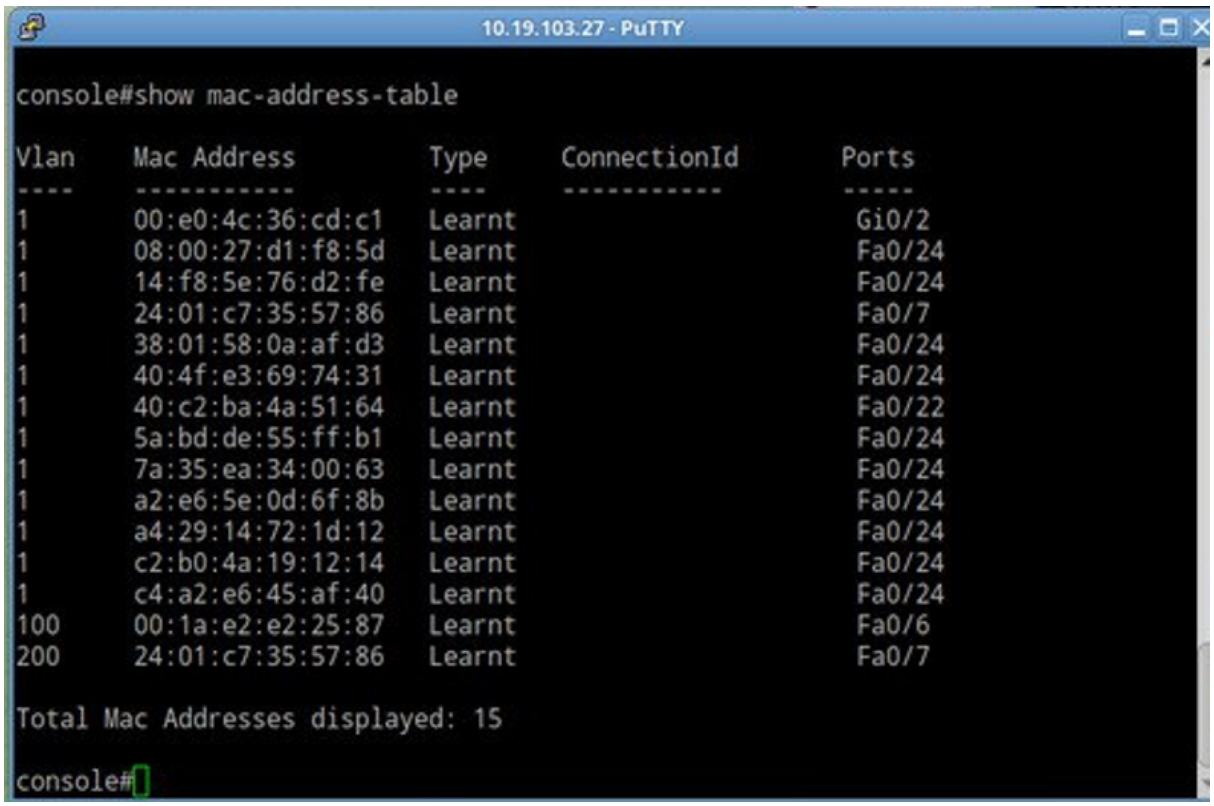


Рисунок 11 - MAC-таблица коммутатора Eltex в процессе атаки

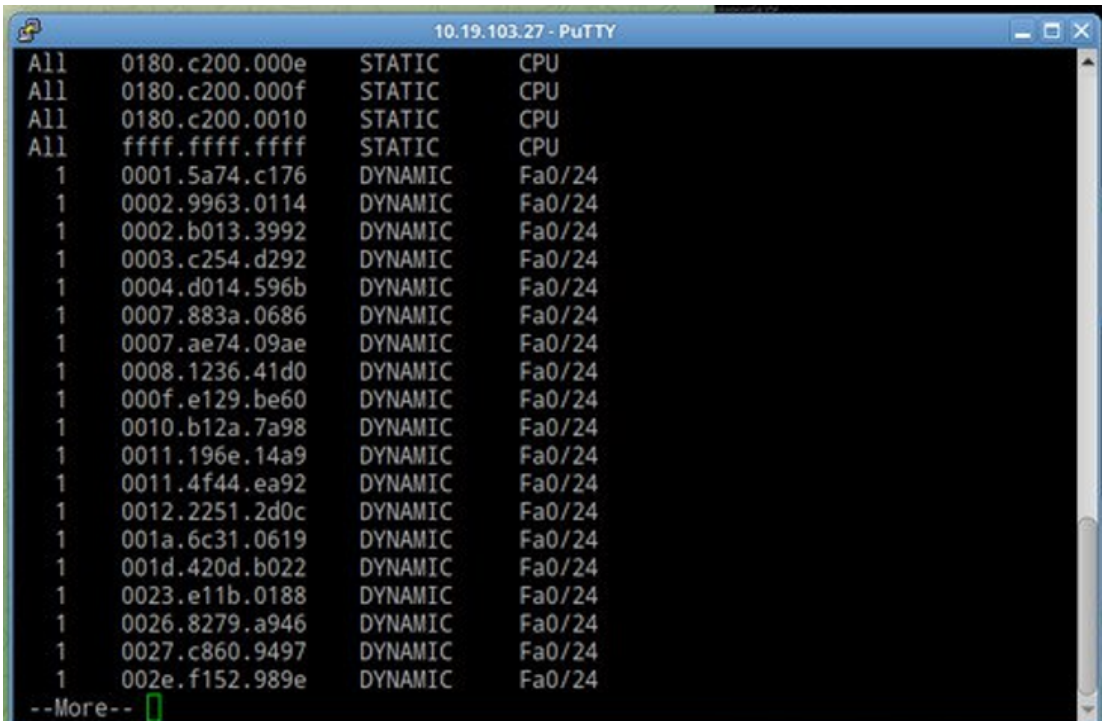


Рисунок 12 - MAC-таблица коммутатора Cisco в процессе атаки

5. Атака с PC3 (192.168.100.3) на коммутатор была произведена успешно. Результатом стало появление пакетов на PC1(192.168.100.4), пересылаемых между PC3 и PC2 (192.168.100.5). Результат атаки идентичен на каждом из коммутаторов.

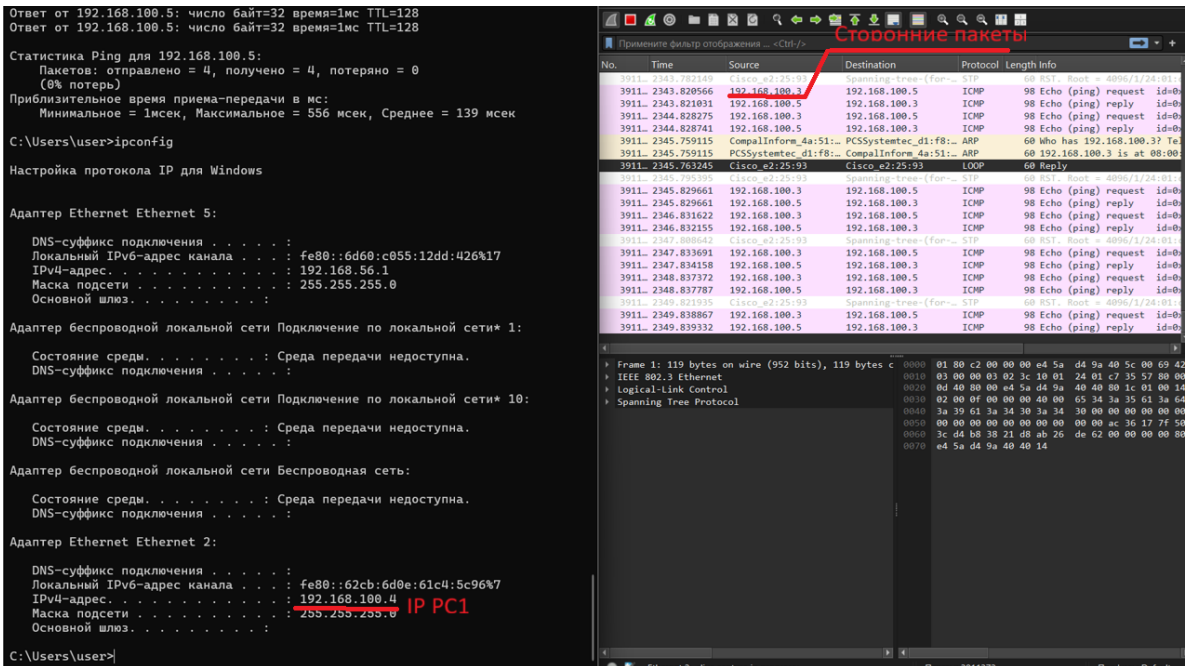


Рисунок 13 - MAC-таблица коммутатора Cisco в процессе атаки

6. Затем на коммутаторах Cisco и Eltex была включена защита Port Security. На коммутаторе Mikrotik была включена возможность автоматического очищения MAC-таблицы, так как на данном типе коммутатора отсутствует защита Port Security.

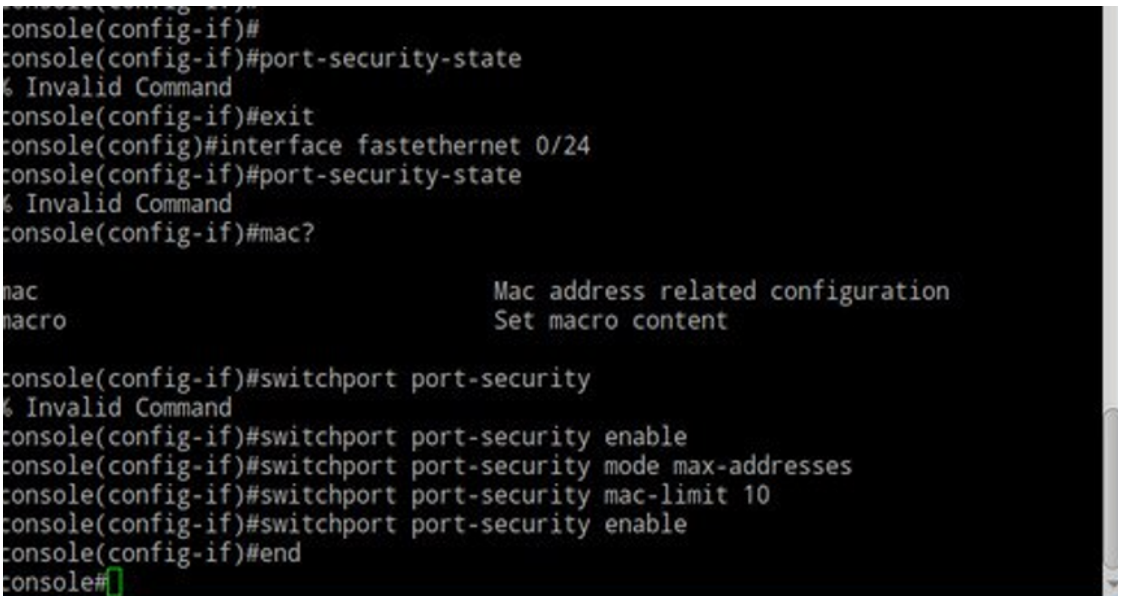
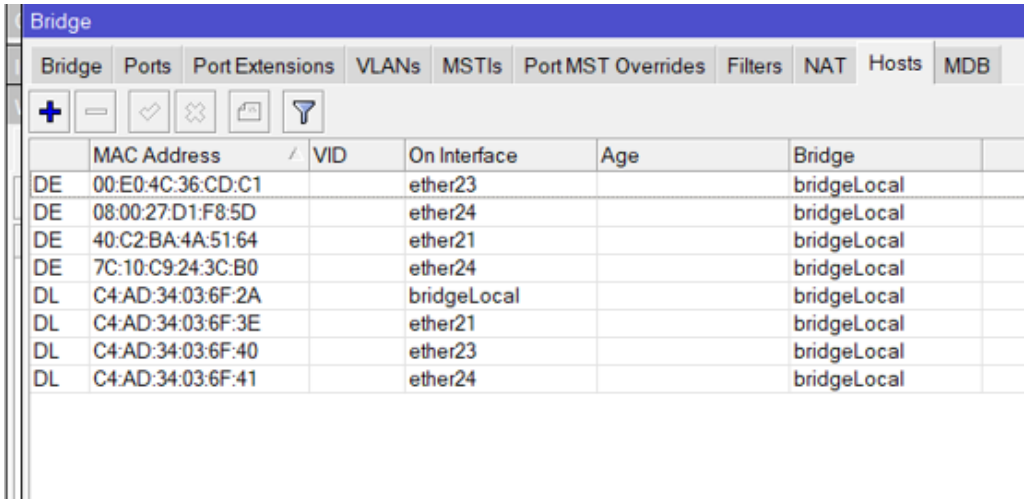


Рисунок 14 - Включение Port Security на Eltex

Рисунок 15 - Включение Port Security на Cisco



	MAC Address	VID	On Interface	Age	Bridge
DE	00:E0:4C:36:CD:C1		ether23		bridgeLocal
DE	08:00:27:D1:F8:5D		ether24		bridgeLocal
DE	40:C2:BA:4A:51:64		ether21		bridgeLocal
DE	7C:10:C9:24:3C:B0		ether24		bridgeLocal
DL	C4:AD:34:03:6F:2A		bridgeLocal		bridgeLocal
DL	C4:AD:34:03:6F:3E		ether21		bridgeLocal
DL	C4:AD:34:03:6F:40		ether23		bridgeLocal
DL	C4:AD:34:03:6F:41		ether24		bridgeLocal

Рисунок 16 - Очищенная таблица MAC-адресов на Mikrotik

7. После включения Port Security атака была произведена повторно. На коммутаторе Cisco был продемонстрирован режим реагирования shutdown. На коммутаторе Eltex - protect.

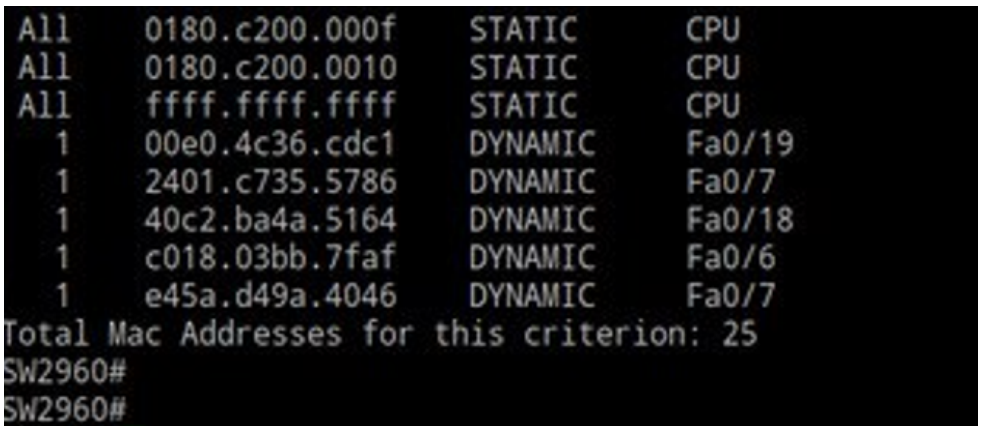


Рисунок 17 - Режим реагирования shutdown

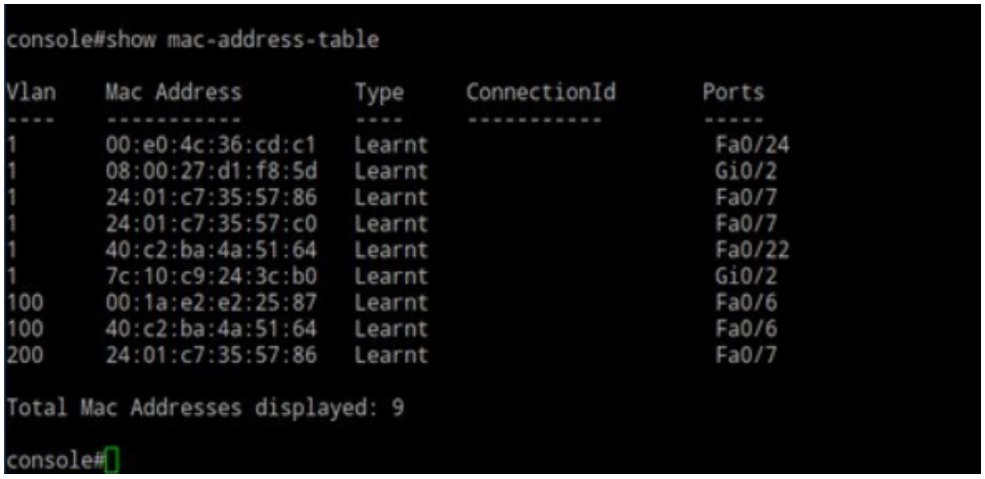


Рисунок 18 - Режим реагирования protect

Для систематизации данных, полученных в ходе эксперимента, ниже представлены сводные таблицы с конфигурациями и результатами тестирования.

Таблица 3 – Исходная конфигурация сетевых интерфейсов

Устройство	IP-адрес	Маска подсети	Шлюз
PC1	192.168.100.4	255.255.255.0	-
PC2	192.168.100.5	255.255.255.0	-
PC3 (атакующий)	192.168.100.3	255.255.255.0	-

Таблица 4 – Параметры атаки MAC-Flooding

Параметр	Значение
Инструмент	macof (пакет dsniff)
Целевой порт	24
Команда	macof -I eth0 -d <IP-коммутатора>

Таблица 5 – Конфигурация механизмов защиты на коммутаторах

Производитель	Модель	Активированный механизм	Конфигурация
Cisco	Catalyst 2960	Port Security	switchport port-security switchport port-security maximum 1 switchport port-security violation shutdown
Eltex	MES1428	Port Security	port-security max-addr-count 1 port-security action protect
MikroTik	CRS326-24G-2S+RM	Очистка MAC-таблицы	Включение автоматического удаления MAC-адресов

Таблица 6 – Сравнительные результаты эксперимента

Производитель	Результат до включения	Результат после включения	Эффективность Защиты

	защиты	защиты	
Cisco	Таблица MAC-адресов переполнена	Порт, через который проходила атака, отключен	Высокая
Eltex	Таблица MAC-адресов переполнена	Трафик блокируется	Высокая
MikroTik	Таблица MAC-адресов переполнена	Таблица медленно очищается автоматически	Низкая

Проведенное исследование и практический эксперимент наглядно демонстрируют важность функции Port Security для защиты сетевой инфраструктуры на канальном уровне. Было подтверждено, что без активации механизмов защиты коммутаторы уязвимы к атаке MAC-Flooding, которая приводит к переполнению таблицы MAC-адресов и переходу устройства в режим хаба.

На коммутаторах Cisco и Eltex была продемонстрирована эффективная работа функции по блокировке несанкционированной активности. Режимы реагирования shutdown и protect надежно пресекали попытки атаки, изолируя нарушителя и защищая целостность таблицы коммутации.

На оборудовании Mikrotik, где отдельная функция Port Security отсутствует, была показана альтернативная стратегия защиты — использование механизма автоматического удаления записей из MAC-таблицы. Этот подход также доказал свою эффективность в борьбе с переполнением.

Таким образом, выяснилось, что защита портов обязательной мерой безопасности для любой современной сети.

Список литературы

1. Уймин А.Г. «Компьютерные сети. L2-технологии: практикум» — Москва : Ай Пи Ар Медиа, 2024.
2. Исследование механизмов безопасности коммутаторов локальной вычислительной сети / Р.Р. Якубов, А.А. Сулейманов — URL: https://cyberleninka.ru/journal/article/issledovanie-mehanizmov-bezopasnosti-kommutatorov-lokalnoy-vychislitelnoy-seti (дата обращения: 01.09.2025).
3. Защита от атак, связанных с переполнением MAC-таблицы коммутатора / И.В. Соколов — URL: https://cyberleninka.ru/journal/article/zaschita-ot-atak-svyazannyh-s-perepolneniem-mac-tablitsy-kommutatora (дата обращения: 01.09.2025).
4. Обеспечение безопасности сетевой инфраструктуры на основе технологии защиты портов коммутатора / К.Д. Новиков — URL: https://cyberleninka.ru/journal/article/obespechenie-bezopasnosti-setevoy-infrastruktury-na-osnove-tehnologii-zaschity-portov-kommutatora (дата

обращения: 01.09.2025).

5. Коммутатор доступа Eltex MES1428: технические характеристики — URL: https://eltex-co.ru/catalog/kommutator_dostupa_mes1428/#compatibility (дата обращения: 01.09.2025).
6. Cisco Catalyst 2960 Series Switches Data Sheet — URL: https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-2960-series-switches/product_data_sheet0900aecd806b0bd8.html (дата обращения: 01.01.2025).
7. Port Security: A Glossary — URL: https://www.crowdsec.net/glossary/port-security (дата обращения: 01.09.2025).
8. Документация по коммутаторам Eltex — URL: https://docs.eltex-co.ru/pages/viewpage.action?pageId=150011977 (дата обращения: 01.01.2025).