Министерство образования Республики Беларусь

Учреждение образования

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет инфокоммуникаций

Кафедра защиты информации

Практическая работа № 1

«Виды Spoofing атак и методы защиты от них»

Шифр: 173

Проверила:

Белоусова Е.С.

Выполнила:

ст. гр. 961401

Савченко Е.А.

­

Минск 2022

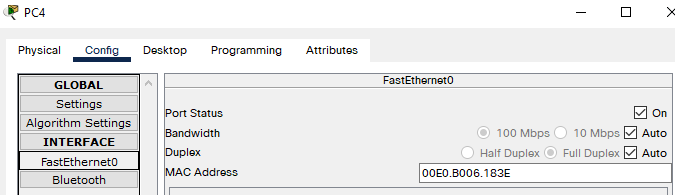
**Цель:** изучить механизмы spoofing атак и методы защиты от них.

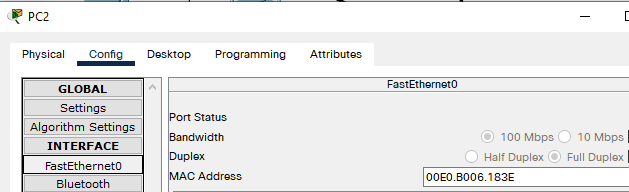
**Ход работы:**

1. *Атака MAC-spoofing*

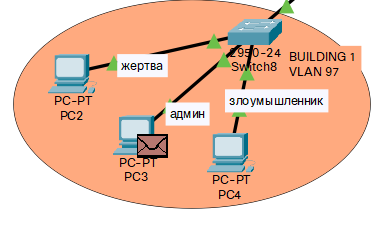
Cisco Packet Tracer

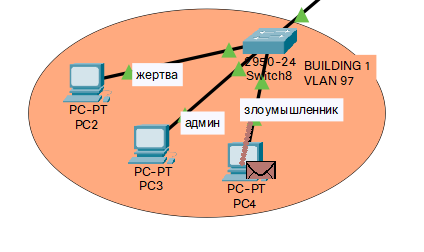
Заменяю МАС-адрес злоумышленника (PC4) на MAC-адрес жертвы (PC2)





Далее отправляю Simple PDU от админа (PC3) к жертве (PC2)

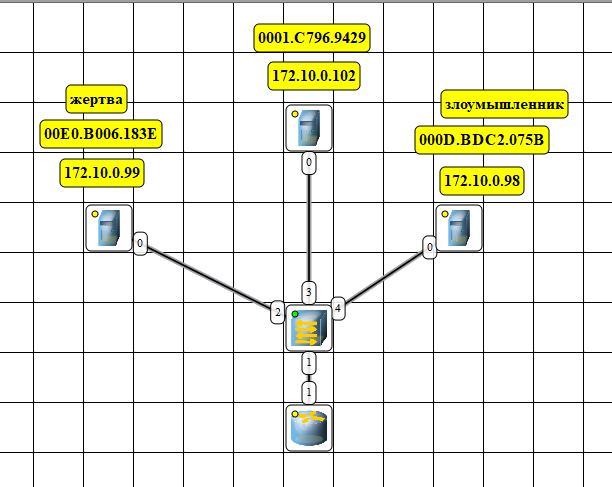




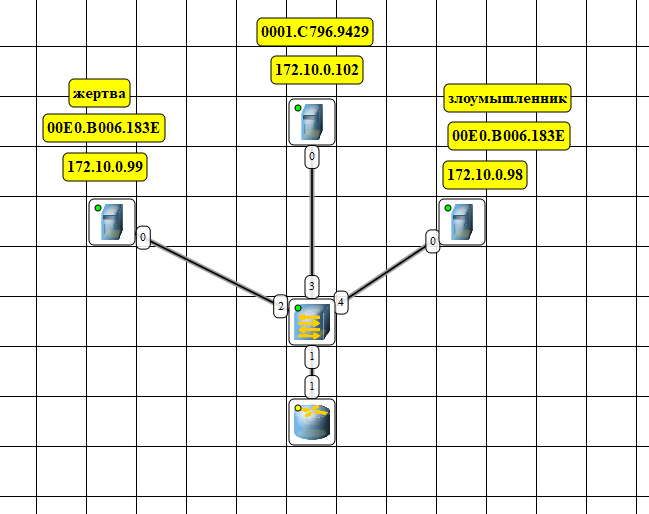
Как видно из рисунков, злоумышленник перехватил пакет.

NetEmul

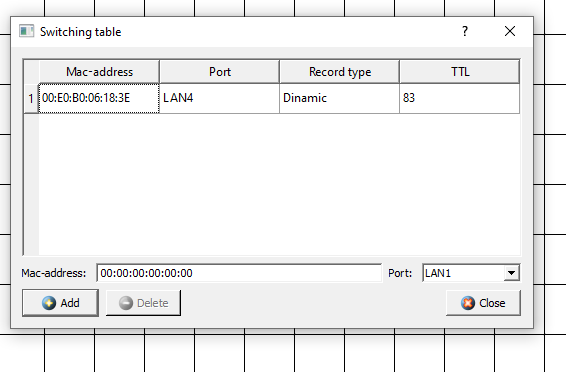
Исходные данные



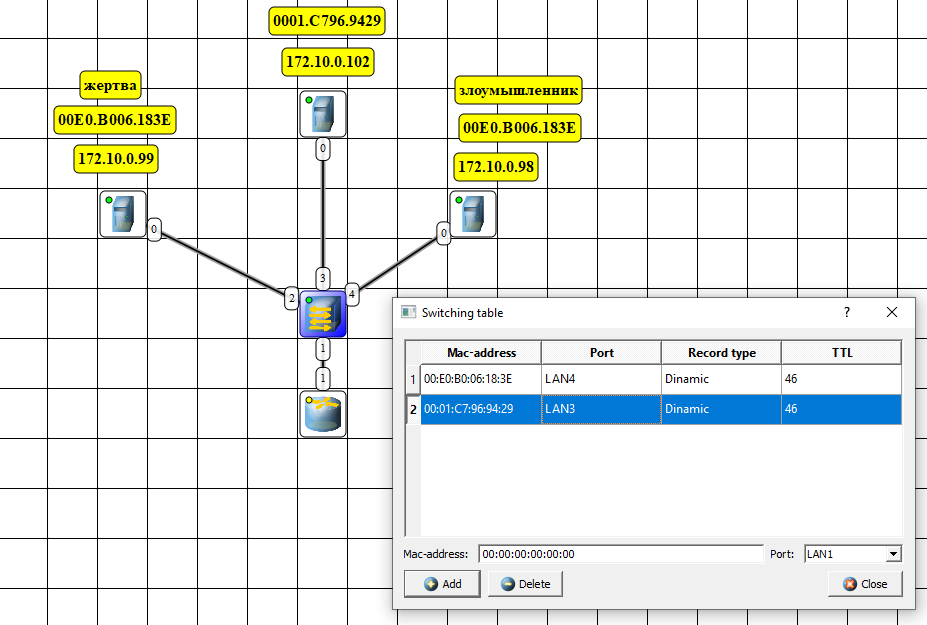
Для проведения атаки злоумышленнику необходимо заменить свой мас-адрес на мас-адрес жертвы



Новый мак-адрес отобразился в таблице коммутатора

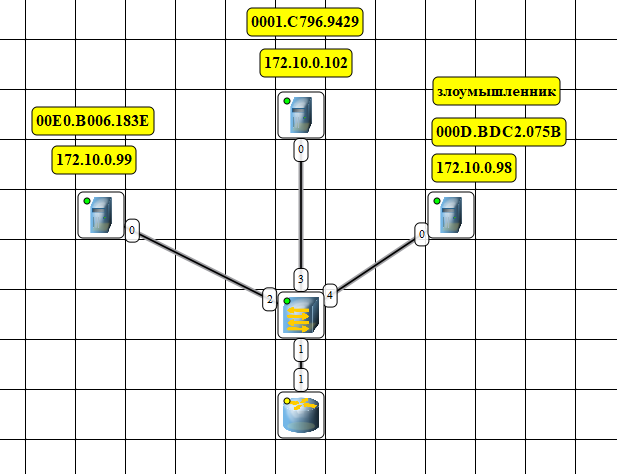


Далее с центрального компьютера отправляю данные по мак-адресу жертвы (сейчас злоумышленник имеет такой же мак-адрес) и происходит перехват пакетов, они дошли не до жертвы (предполагаемого получателя), а попали к злоумышленнику.

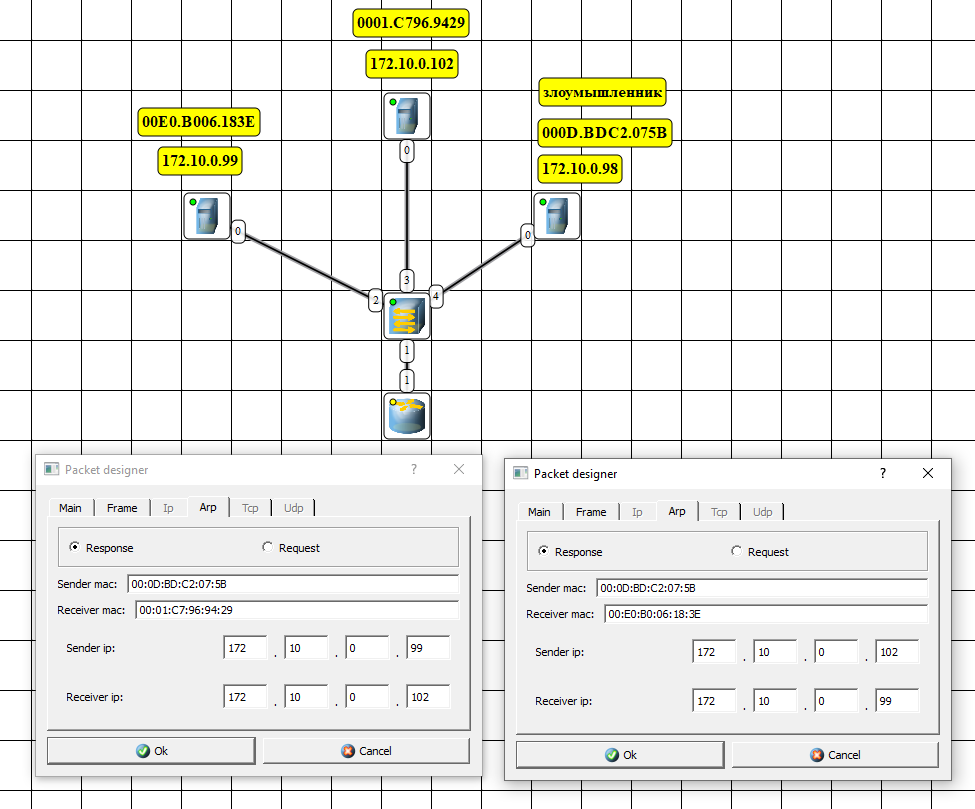


1. *Arp-spoofing*

Исходные данные

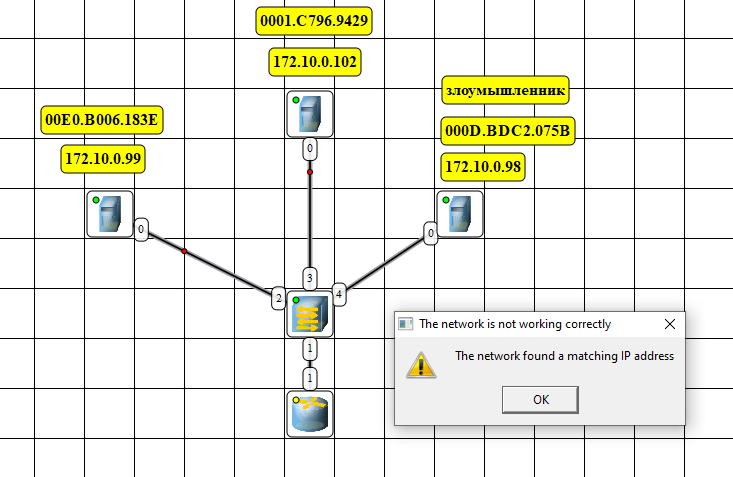


От лица злоумышленника формирую два arp-пакета со следующими данными:

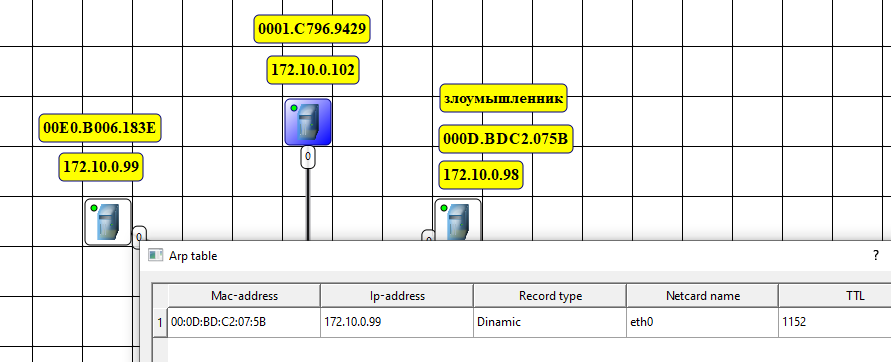


Следовательно, когда к устройству назначения придет пакет, то в свою arp-таблицу он запишет мас- и ip-адрес отправителя ( где мак-адрес принадлежит злоумышленнику, а ip-адрес соседнему устройству).

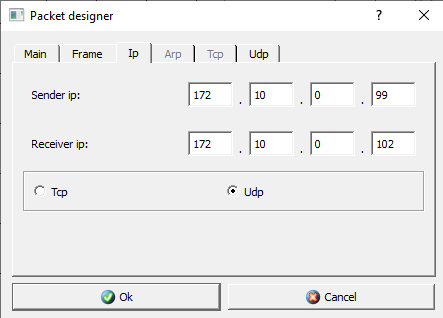
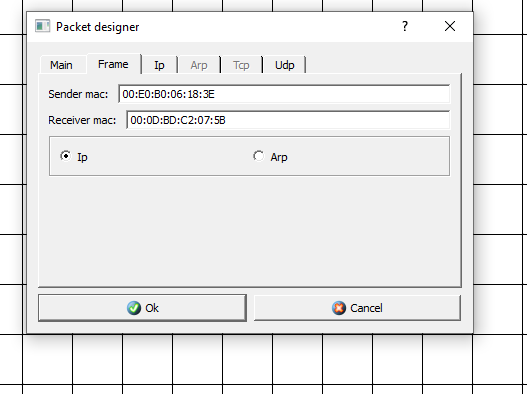
В программе наблюдаю данную ошибку, так как устройство получило пакет, где его ip-адрес указан в качестве отправителя, а оно же ничего не отправляло…



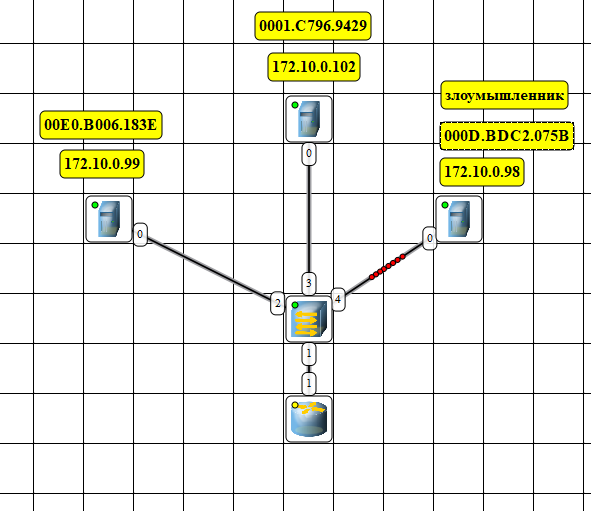
Проверяю таблицу одного из устройств-получателей и наблюдаю несоответствия(собственно, этого злоумышленник и добивается)



Теперь от устройства с испорченной таблицей отправляю пакетики соседнему устройству, заполняю поля:

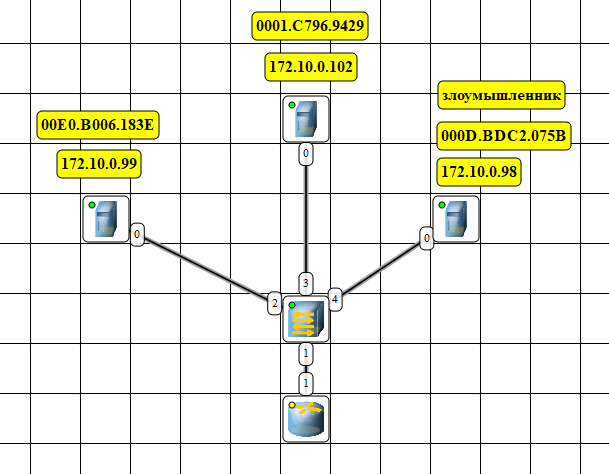


В результате, данные пришли к злоумышленнику, а не предполагаемому получателю.

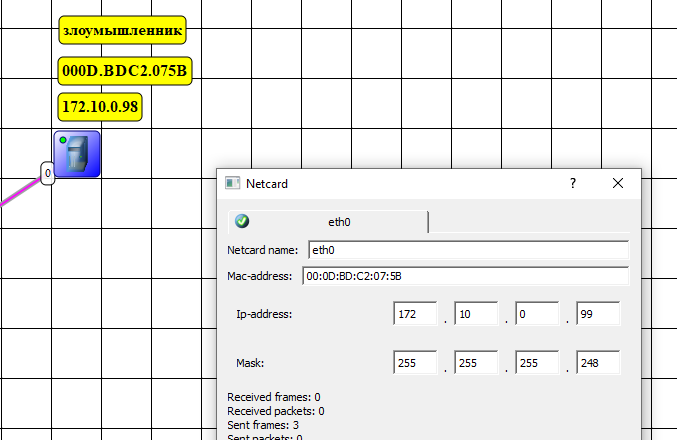


1. Ip -spoofing

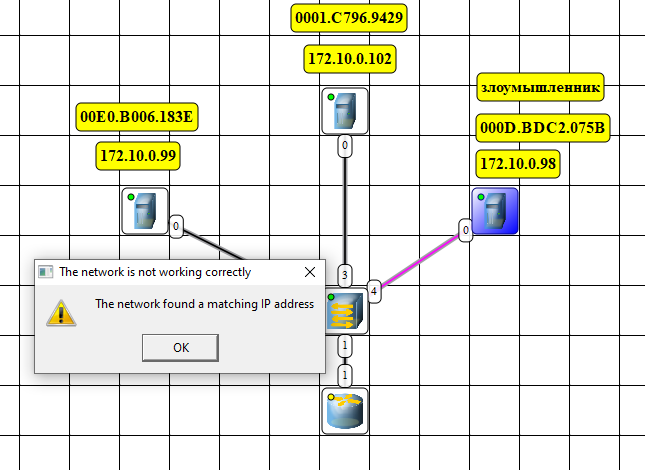
Исходные данные



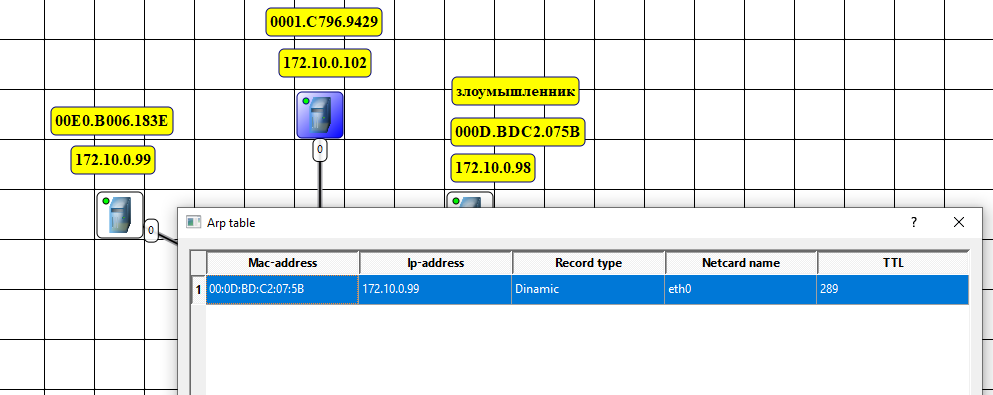
Злоумышленник меняет свой ip-адрес на адрес жертвы:



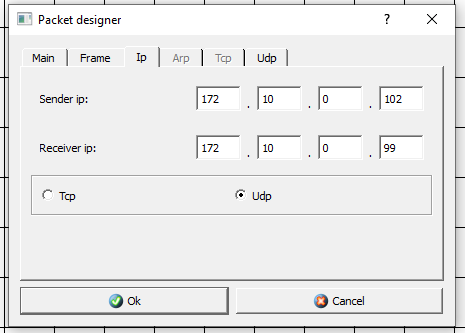
Об этом узнают устройства в сети и я наблюдаю ошибку, так как оригинальное устройство сообщает, что здесь что-то не то

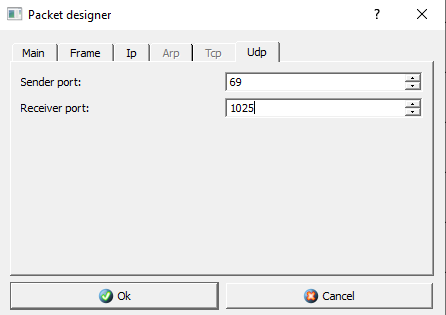
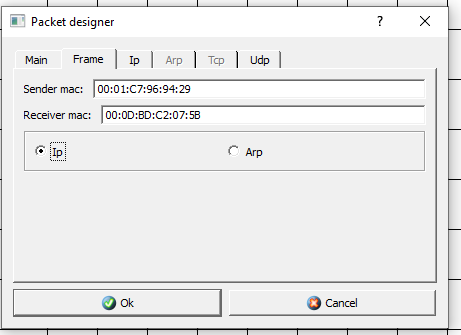


Если посмотреть в таблицу центрального устройства, то видно, что в табличке неправильные данные, несоответствующие (но оно об этом, конечно, не знает)

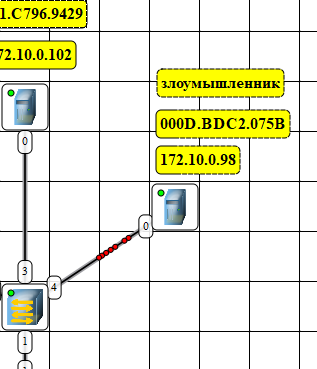


Отправляю данные к моей жертве, для этого заполняю таблицу, используя данные которые у меня есть (я же не знаю, что они неверные)



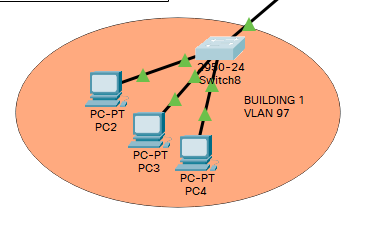


В результате мои пакетики дошли до злоумышленника, а не предполагаемого получателя.

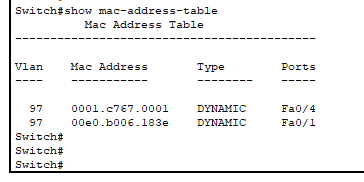


1. *Cam-table overflow*

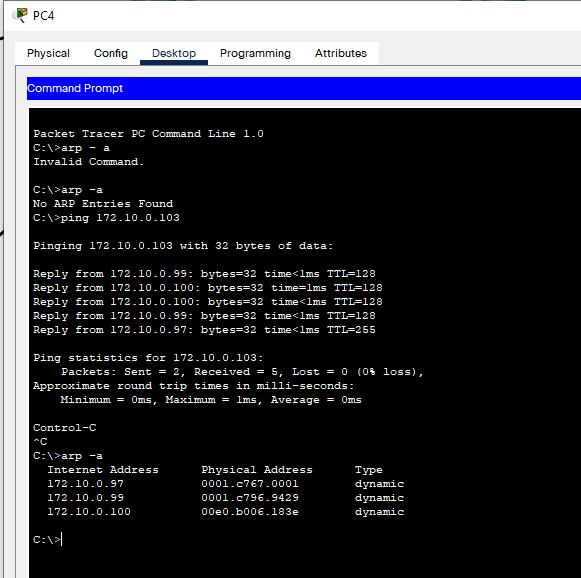
Исходные данные

\

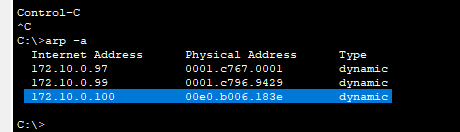
Исходная таблица мас-адресов switch8



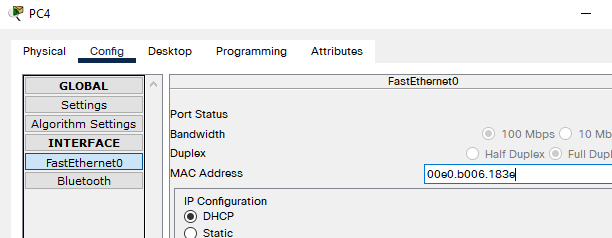
Допустим, злоумышленник действует с PC4. Сначала он проверяет свою таблицу arp, ничего там не находит. После чего он отправляет ping на широковещательный адрес сети, затем снова проверяет таблицу и уже находит там ip- и mac-адреса.



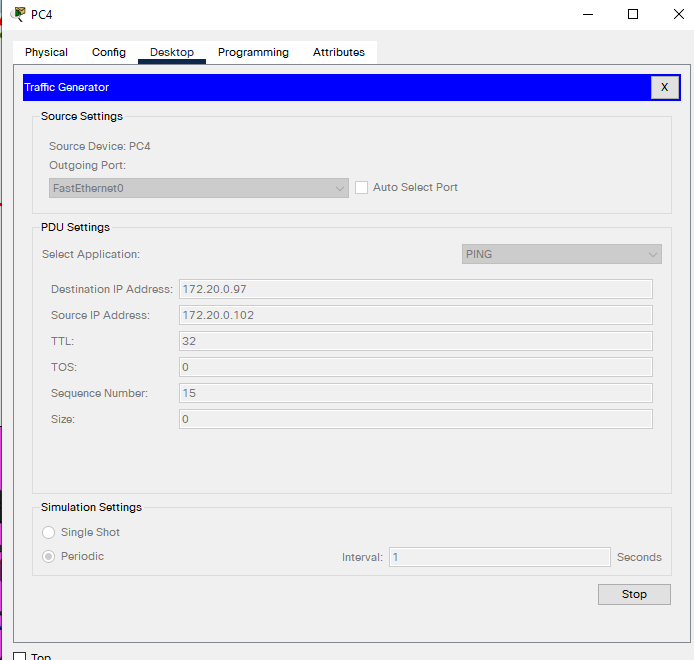
Выбирает любой понравившийся адрес и делает подмену мас-адреса. В моем случае это будет третья строчка:



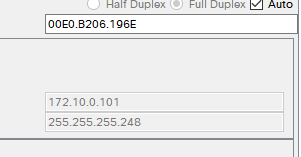
Мас-адрес злоумышленника становится таким же

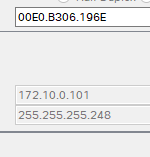


Теперь постоянно отправляем на коммутатор пакеты, чтобы он их обрабатывал и заполнял arp – таблицу. Для этого использую traffic generator.

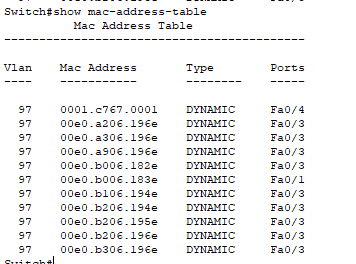


Изменяю мак-адреса много раз



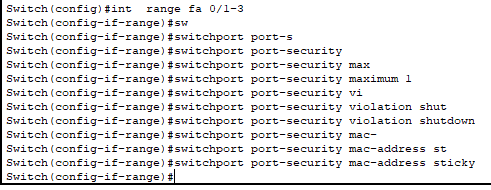


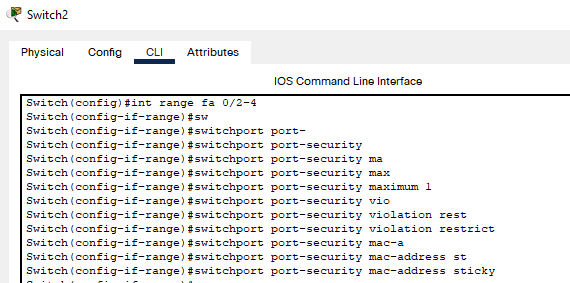
Наша таблица стала больше, следовательно, если продолжить так делать, то в какой-то момент таблица переполнится и маршрутизатор не сможет обрабатывать поступающие пакеты, следовательно, начнет их пересылать всем подряд.

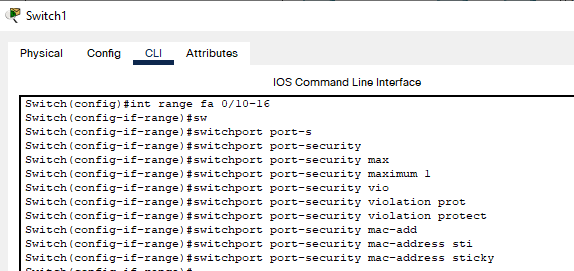


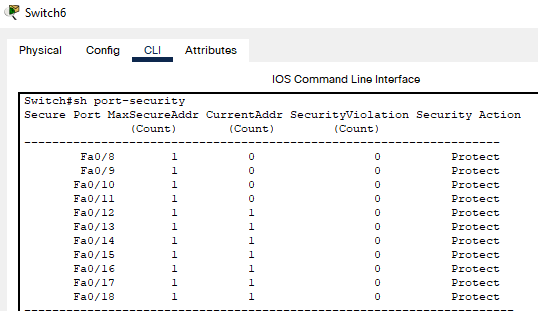
1. Port-security

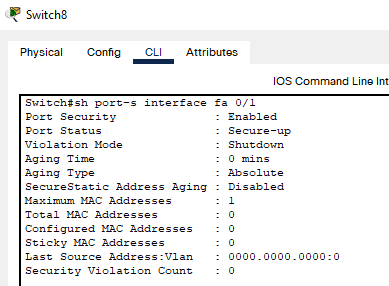
Switch 8

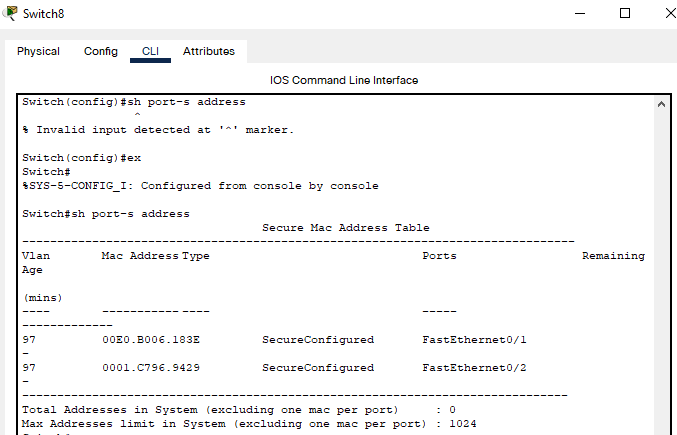












**Вывод:** Spoofing – это подмена. В ходе выполнения лабораторной работы я познакомилась с некоторыми видами данной атаки. Например, mac- и ip-spoofing происходят на основе подмены злоумышленником mac и ip-адресов соответственно. При arp-spoofing злоумышленник передает неверные данные в arp-таблицы других устройств, указав свой мак-адрес и ip-адрес соседнего устройства. АтакаCam-table overflow направлена на переполнение таблицы arp. В этом случае злоумышленник ждет момент, где таблица переполнится и маршрутизатор не сможет обрабатывать поступающие пакеты, следовательно, начнет их пересылать всем подряд. После чего я познакомилась с одним из методов защиты от вышеприведенных атак , а именно подключение фильтрации по Mac-адресам на коммутаторе, которая подключается с помощью функции port-security.