МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН

Некоммерческое акционерное общество

«АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ ИМЕНИ ГУМАРБЕКА ДАУКЕЕВА»

Кафедра IT - Инжиниринг

**ЛАБОРАТОРНАЯ РАБОТА №4**

По дисциплине «Современные системы маршрутизации и коммутации в компьютерных сетях»

На тему: Защита ЛВС от атак канального уровня

Специальность 7M06103-Вычислительная техника и программное обеспечение

Выполнил Сакан Ерлан Группа МВТн-21-2

\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_«\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_201\_\_\_г.

(оценка) (подпись)

Алматы 2022

**Цель работы:** Целью лабораторной работы является изучение методов проектирования, развертывания и настройки механизмов защиты в коммутируемых ЛВС от атак канального уровня типа MAC-flooding и MAC-spoofing.

Одним из механизмов защиты ЛВС от атак является механизм port security, реализованный на коммутаторах. Механизм port security позволяет осуществлять фильтрацию кадров, поступающих на отдельные порты коммутатора ЛВС, на основе MAC-адреса источника.

При активизации данного защитного механизма на порту коммутатора создается список ассоциированных (разрешенных) с ним MAC-адресов. Кадры, поступающие на порт коммутатора с активизированной функцией port security, MAC-адреса которых не принадлежат данному списку, уничтожаются. При этом сам порт коммутатора может переходить в режим shutdown.

Существует два метода построения списка разрешенных MAC-адресов — метод статического назначения и метод динамического изучения.

Метод статического назначения разрешенных MAC-адресов применяется на коммутаторах доступа ДМЗ, центров обработки данных и т.д. При этом на порту коммутатора указывается конкретный MAC-адрес.

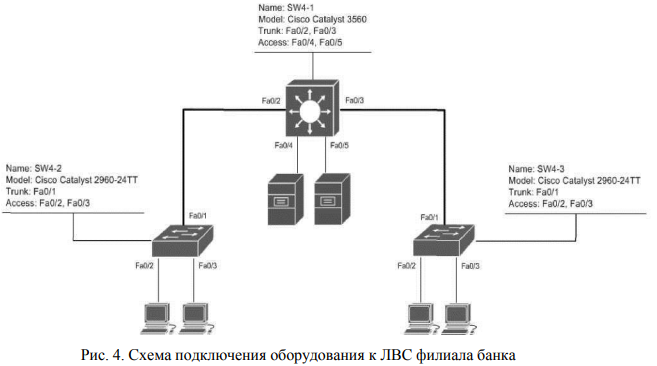
Метод динамического изучения адресов определяет максимальное количество MAC-адресов, ассоциируемых коммутатором с портом в течение некоторого времени. Такой способ построения таблицы адресов, как правило, применять на уровне доступа ЛВС или в сетях филиалов.

При нарушении безопасности — при поступлении на защищаемый порт коммутатора кадра с запрещенным MAC-адресом - возможно одно из трех событий: порт отключается (режим защиты shutdown), кадр отвергается коммутатором (режим защиты protect), кадр отвергается коммутатором, увеличивается счетчик нарушений порта и генерируется SNMP-сообщение (режим защиты restrict).

В динамически изменяемой сетевой инфраструктуре рекомендуется ограничиваться одним MAC-адресом для порта коммутатора и использовать режим protect, в серверных группах — статически задавать списки MAC-адресов и использовать режим shutdown, в VoIP-сегментах — ограничиваться двумя или тремя MAC-адресами с активизацией режима restrict.

Дополнительным механизмом формирования списка MAC-адресов является механизм sticky. Он позволяет добавить статически заданные или динамически выученные MAC-адреса в конфигурационный файл ОС коммутатора.

В сегменте ЛВС филиала (см. рис. 4), построенном на базе двух коммутаторов уровня доступа Cisco Catalyst 2960 и коммутатора уровня ядрараспределения Cisco Catalyst 3560, обеспечить защиту от атак типа MACflooding и MAC-spoofing.



На коммутаторе уровня доступа SW4-3 настроить механизм port security в динамическом режиме для рабочих станций: interface range fa0/2-3 switchport mode access switchport port-security switchport port-security maximum 1 switchport port-security violation protect.

Выполнить аналогичные настройки механизма port security на коммутаторе SW4-2.

На коммутаторе уровня ядра-распределения SW4-1 настроить механизм port security в статическом режиме с привязкой к заданному MACадресу для порта FastEthernet0/4:

interface fa0/4

switchport mode access

switchport port-security

switchport port-security maximum 1

switchport port-security mac-address

xxxx.yyyy.zzzz

switchport port-security violation shutdown

На коммутаторе уровня ядра-распределения SW4-1 настроить механизм port security в статическом режиме с опцией sticky для порта

FastEthernet0/5: interface fa0/5

switchport mode access

switchport port-security

switchport port-security maximum 1

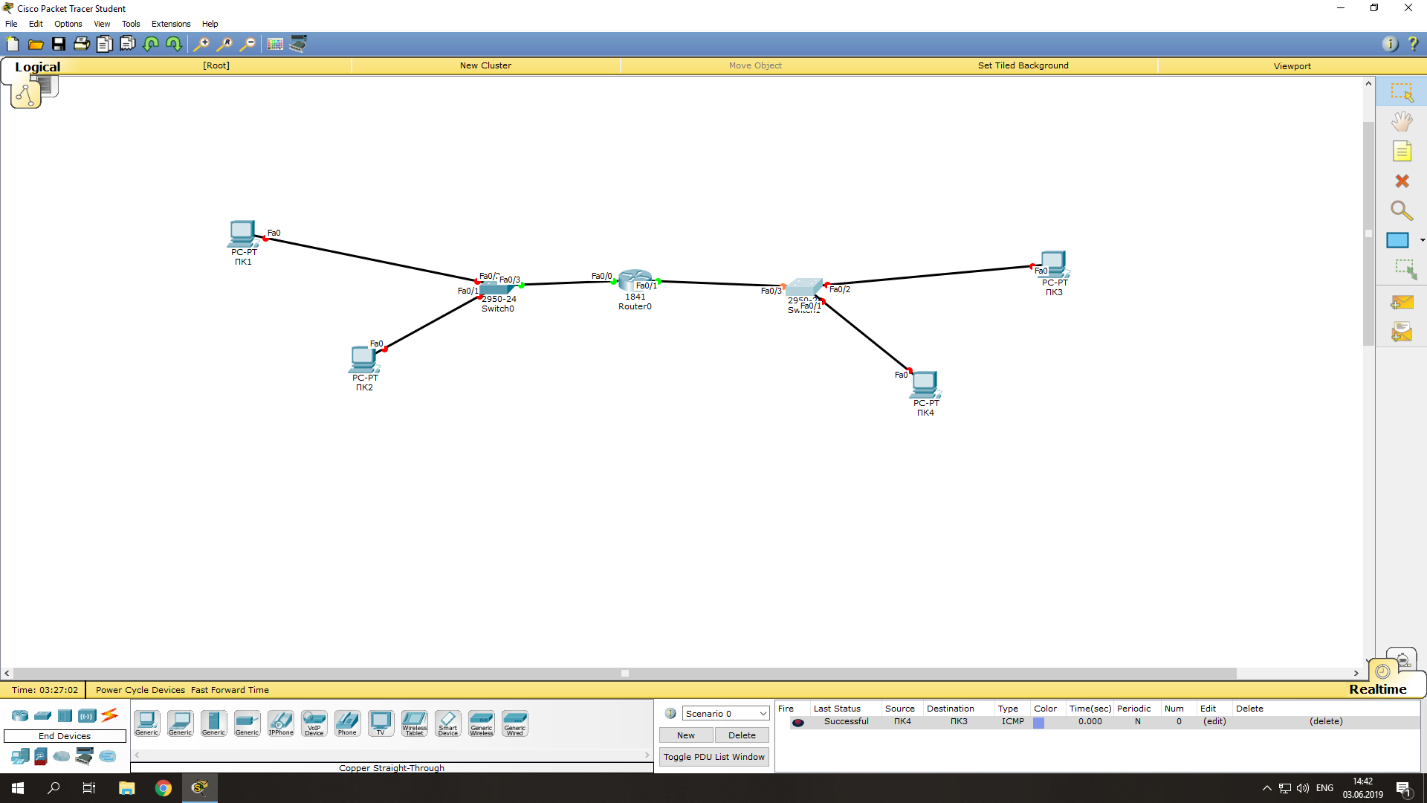
switchport port-security mac-address sticky switchport port-security violation

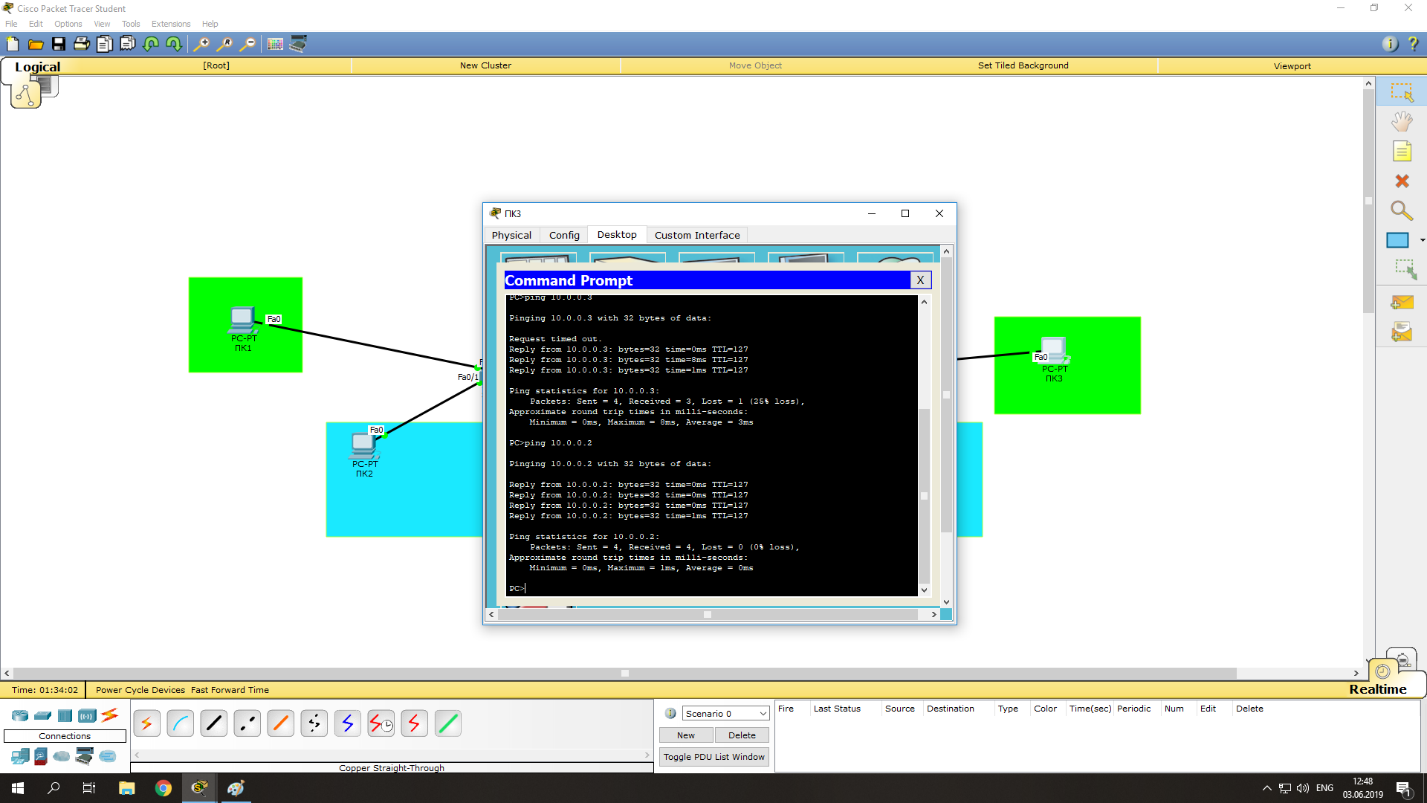
shutdown

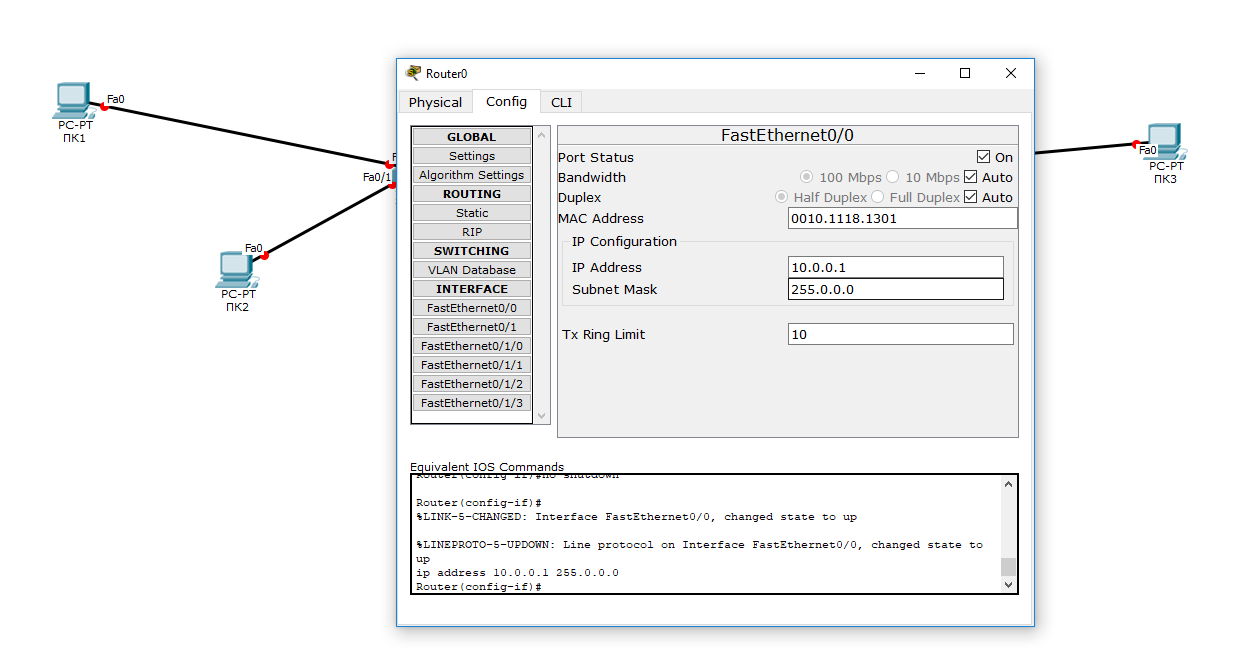
Проверить корректность настроек механизма безопасности port security коммутаторов ЛВС путем моделирования атаки типа MACspoofing. Задать MAC-адрес рабочей станции, подключенной к порту коммутатора со статическим методом формирования списка MAC-адресов, несоответствующий требованиям политики безопасности. Убедиться в переводе порта коммутатора в режим shutdown или protect.

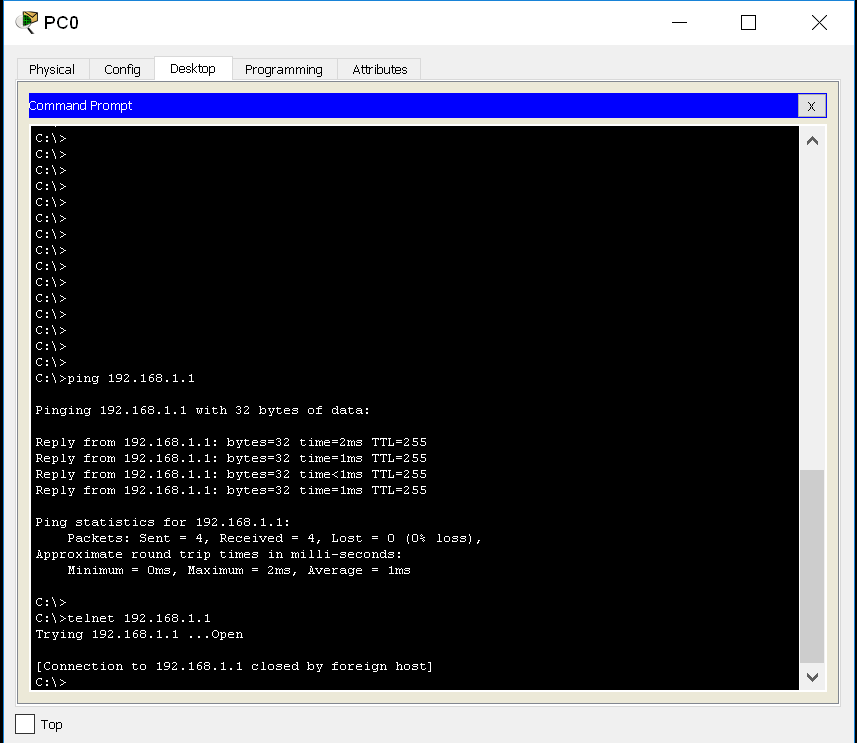
Проверить корректность настроек механизма безопасности port security коммутаторов ЛВС путем моделирования атаки типа MAC-flooding.

На порт коммутатора с динамическим методом формирования списка разрешенных MAC-адресов подключить коммутатор с несколькими рабочими станциями. Убедиться в переводе порта коммутатора в режим shutdown или protect.









Switch>en

Switch#conf t

Switch(config)#vlan 10

Switch(config-vlan)#name Office1

Switch(config-vlan)#exit

Switch(config)#vlan 20

Switch(config-vlan)#name Office2

Switch(config-vlan)#exit

Switch(config)#vlan 30

Switch(config-vlan)#name Office3

Switch(config-vlan)#exit

Switch(config)#end

Router>en

Router#conf t

Router(config)#int gig 0/0.10

Router(config-subif)#encapsulation dot1Q 10

Router(config-subif)#ip address 10.0.0.254 255.255.255.0

Router(config-subif)#exit

Router(config)#int gig 0/0.20

Router(config-subif)#encapsulation dot1Q 20

Router(config-subif)#ip address 20.0.0.254 255.255.255.0

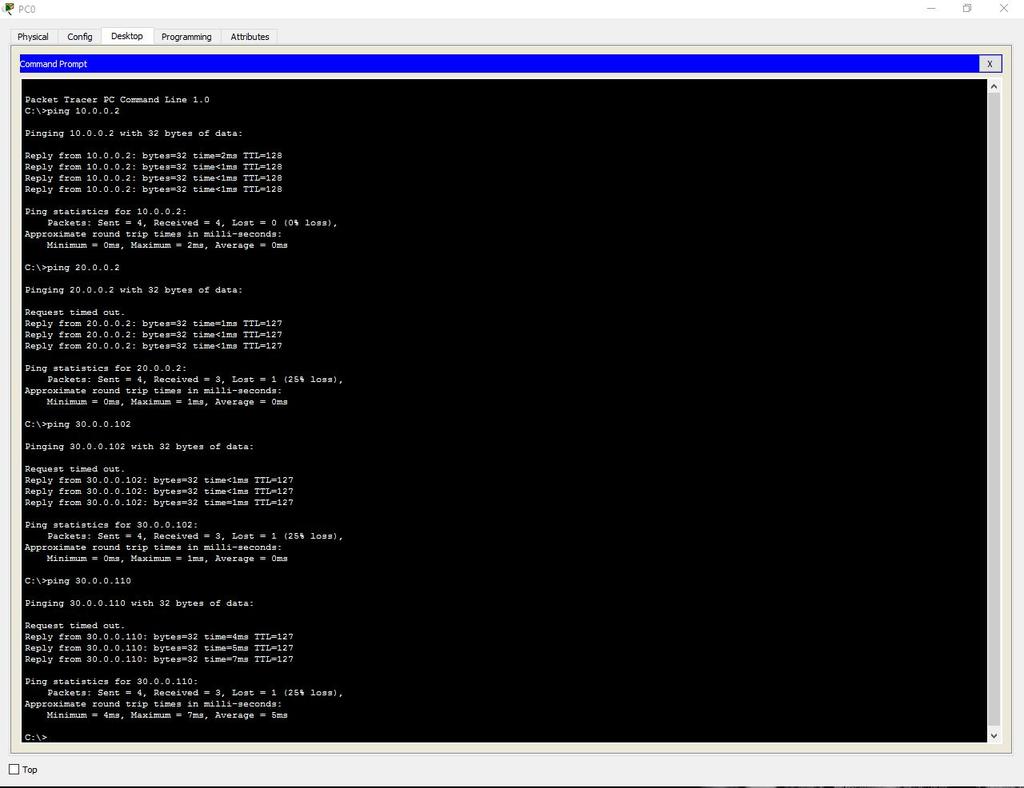
Router(config-subif)#exit

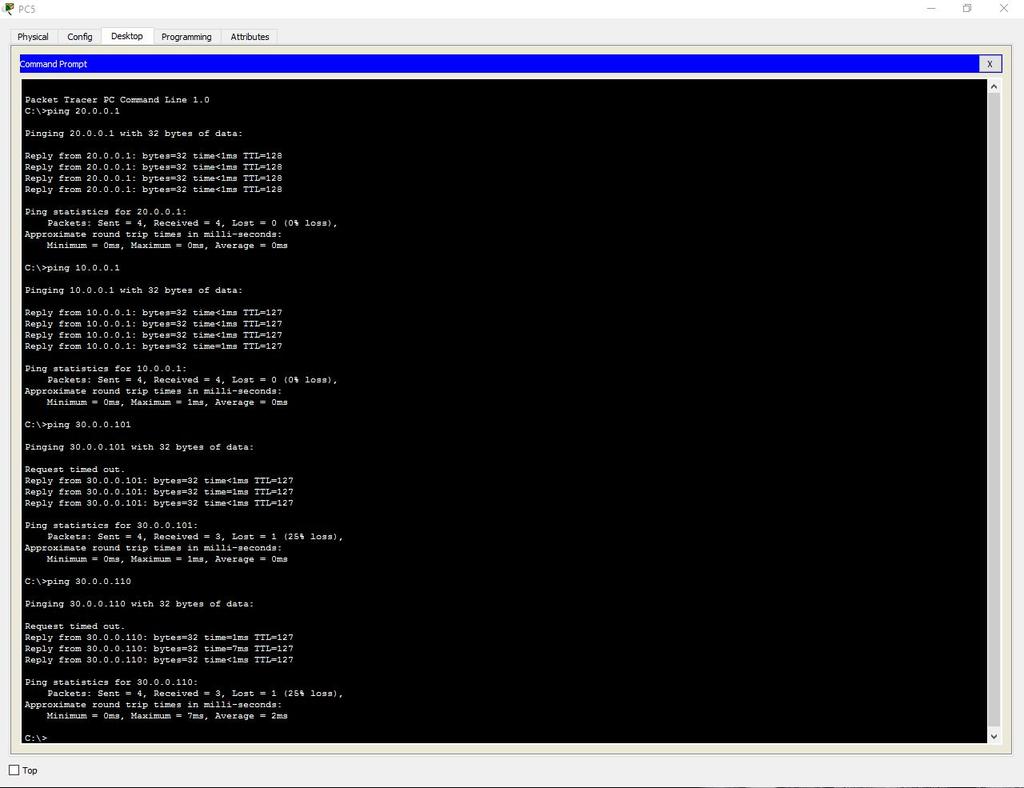
Router(config)#int gig 0/0.30

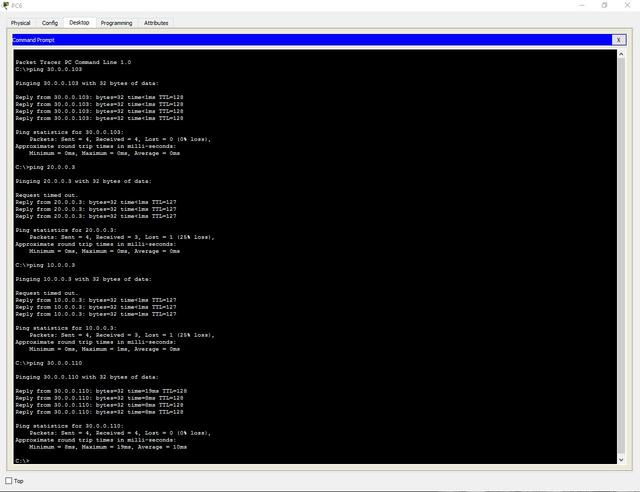
Router(config-subif)#encapsulation dot1Q 30

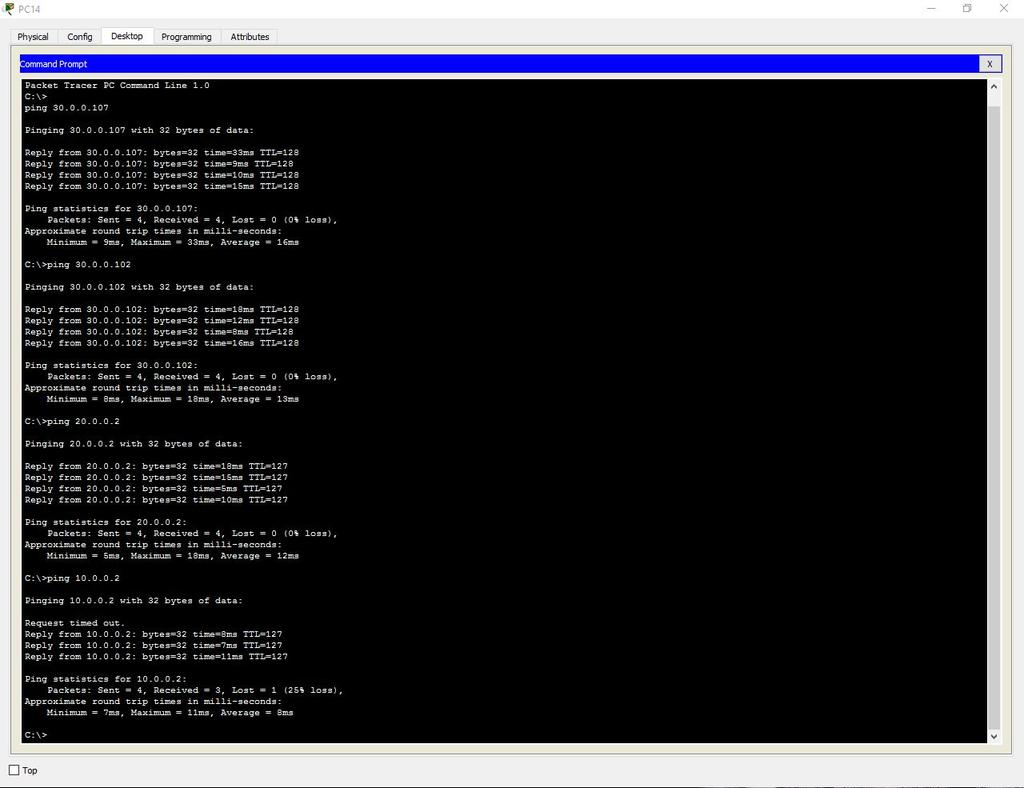
Router(config-subif)#ip address 30.0.0.254 255.255.255.0

Router(config-subif)#end









**Вывод**

В данной лабораторной работе мы изучили методы проектирования, развертывания и настройки механизмов защиты в коммутируемых ЛВС от атак канального уровня типа MAC-flooding и MAC-spoofing.