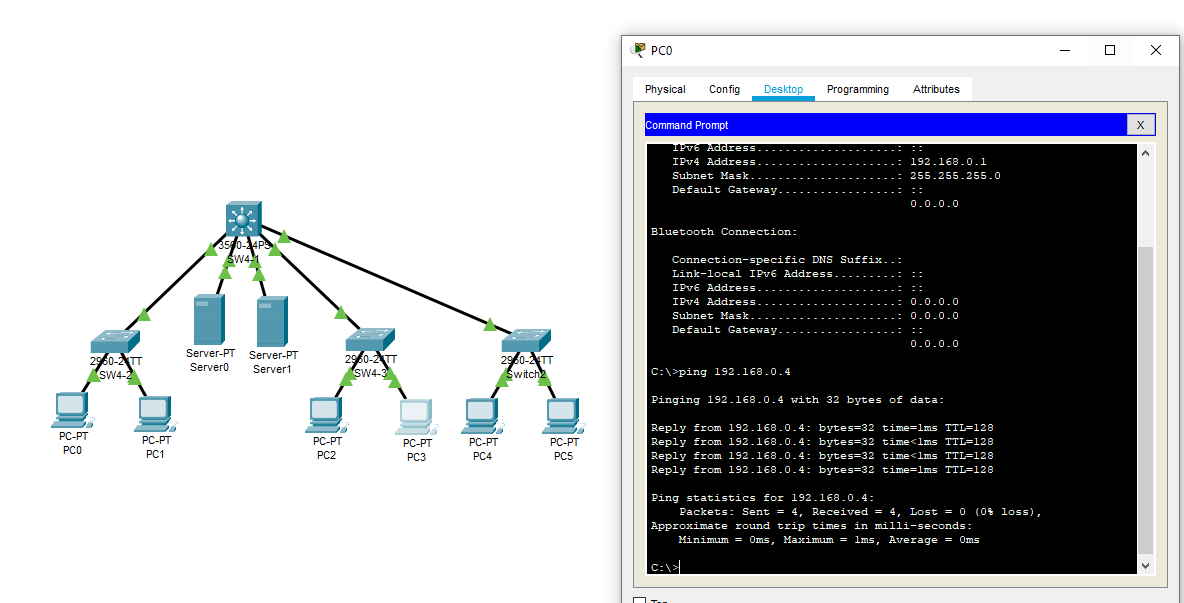
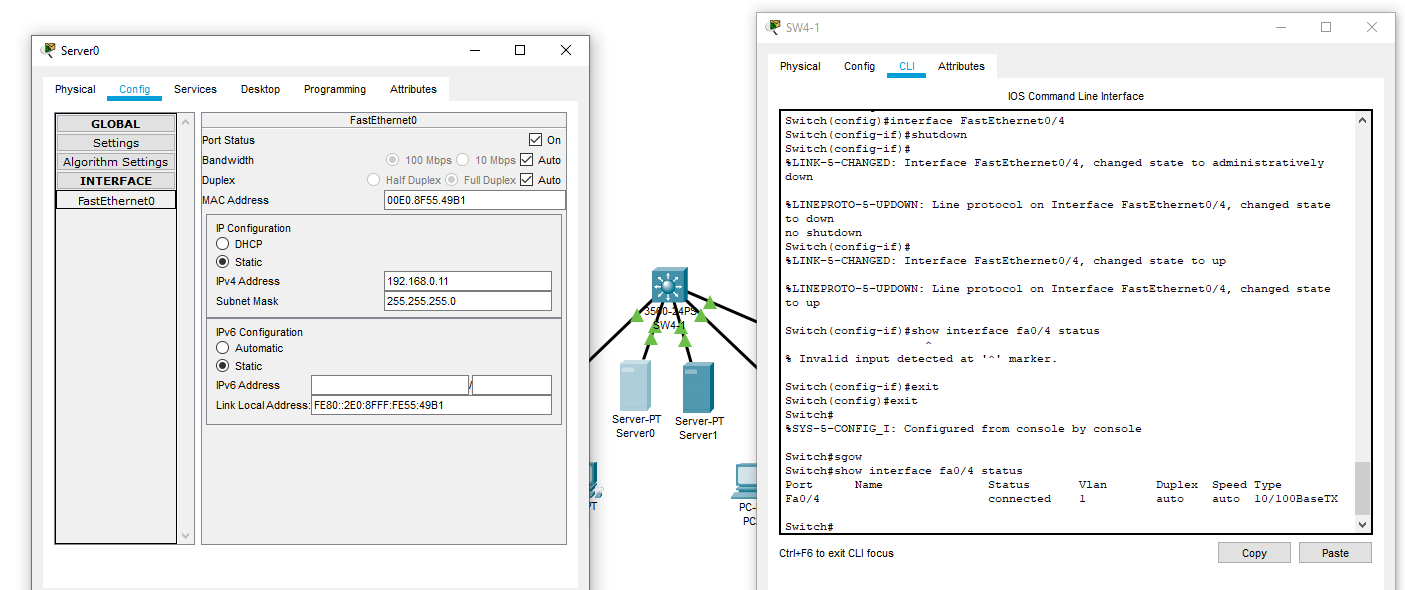
Дровосеков Д.А. КМБ-16

Проверим работоспособность созданной сети, ping PC3 c PC0

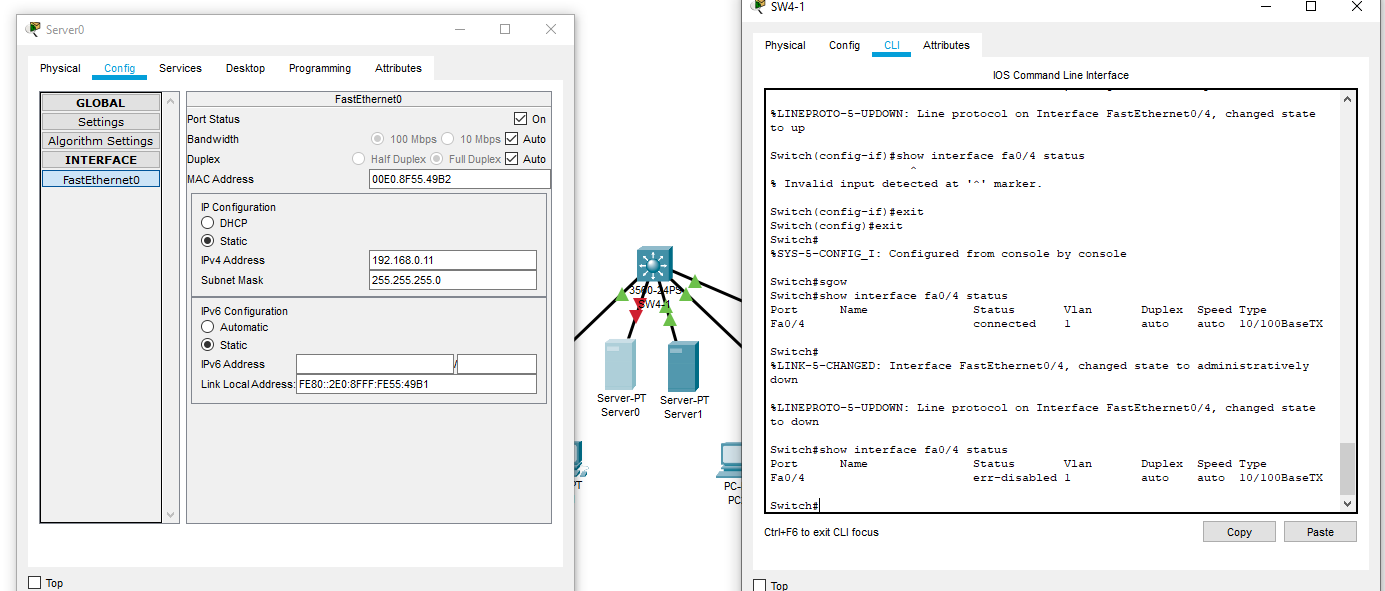


**Проверить корректность настроек механизма безопасности port security коммутаторов ЛВС путем моделирования атаки типа MAC-spoofing. Задать MAC-адрес рабочей станции, подключенной к порту коммутатора со статическим методом формирования списка MAC-адресов, несоответствующий требованиям политики безопасности.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

Работа с легальным MAC адресом

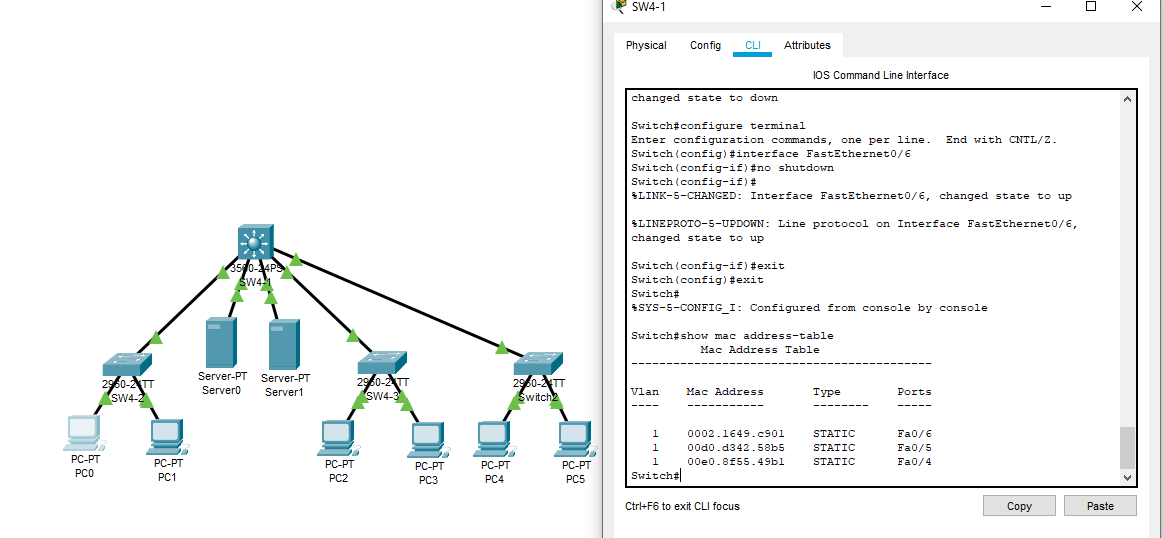


MAC адрес изменен, на нелегальный, видим блокировку порта

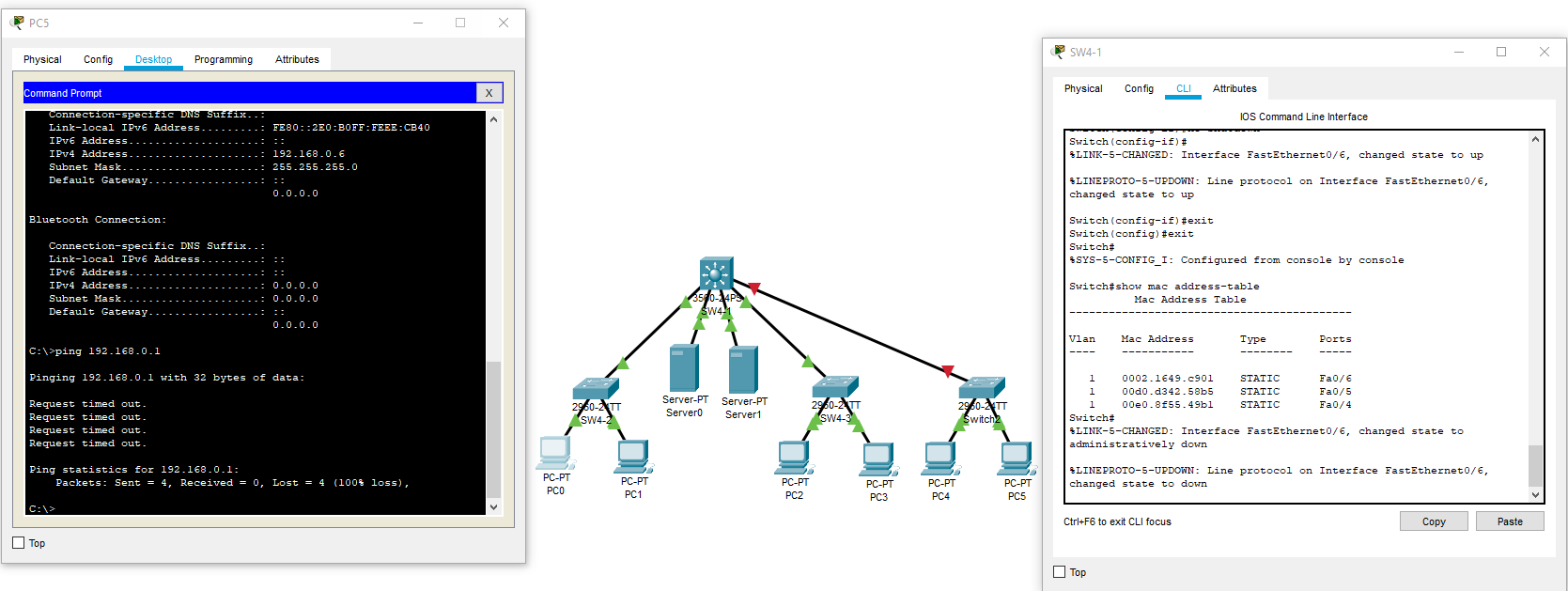


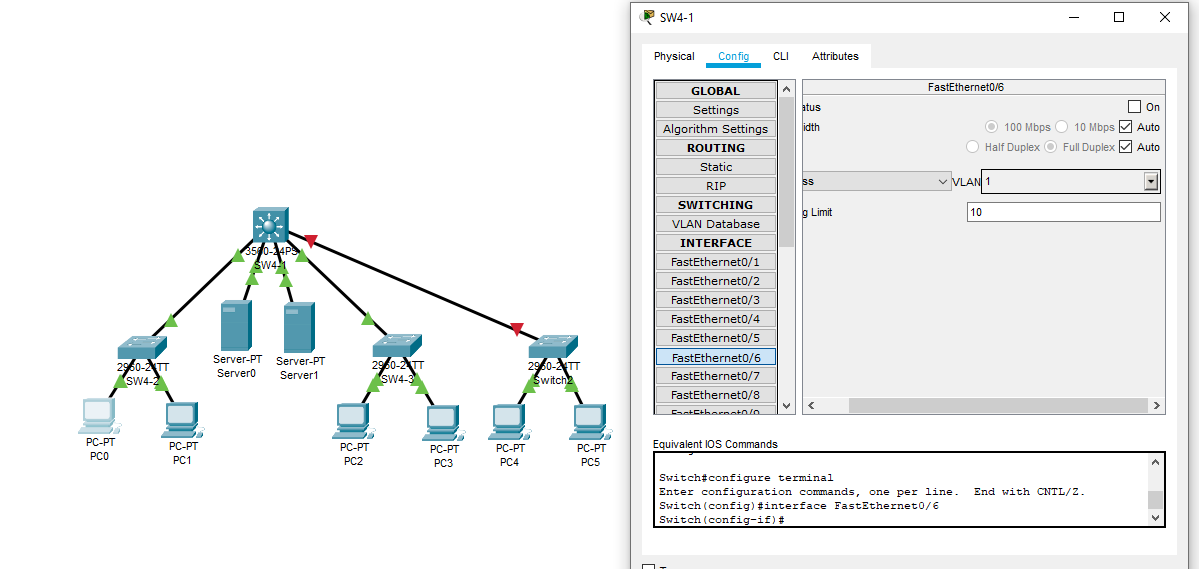
**Шаг 6. Проверить корректность настроек механизма безопасности port security коммутаторов ЛВС путем моделирования атаки типа MAC-flooding. На порт коммутатора с динамическим методом формирования списка разрешенных MAC-адресов подключить коммутатор с несколькими рабочими станциями. Убедиться в переводе порта коммутатора в режим shutdown или protect.**

Проверим таблицу MAC-адресов коммутатора и подключим к соответствующему порту коммутатор с несколькими подключёнными рабочими станциями



Если командой ping проверить соединение между PC5 и PC0, то их MAC-адреса попадут в таблицу коммутатора. Т.к. порт ограничен в один MAC-адрес, он будет заблокирован.





1. Описать назначение и принцип работы механизма port security sticky для статического метода формирования MACадресов.

Port-Security – это функция коммутатора, при помощи которой мы можем указать каким устройствам можно пропускать трафик через определенные порты. Устройство определяется по его MAC-адресу. Эта функция предназначена для защиты от несанкционированного подключения к сети и атак, направленных на переполнение таблицы MAC-адресов. При помощи нее мы можем указывать конкретные адреса, с которых разрешен доступ или указывать максимальное количество MAC-адресов, которые могут передавать трафик через порт.

Статические MAC-адреса – MAC-адреса, которые вручную настроены на порту, из режима конфигурации порта при помощи команды switchport port-security mac-address [MAC-адрес] . MAC-адреса, сконфигурированные таким образом, сохраняются в таблице адресов и добавляются в текущую конфигурацию коммутатора.

2. Объяснить рекомендацию задания максимального количества MAC-адресов на порту коммутатора с динамическим методом формирования списка из двух или трёх разрешенных MAC-адресов.

В VoIP-сетях к одному порту коммутатора, как правило, подключается два устройства: IP телефон и компьютер пользователя, подключение большего количество устройств, говорит о несанкционированном подключении.

3. Возможно ли применение механизма port security для защиты от атак типа ARP spoofing и DHCP spoofing?

При привязке физического адреса к порту коммутатора, коммутатор проверяет приходящие на этот порт пакеты по заголовкам Ethernet. Arp-пакеты имеют 4 поля с физическими адресами: два принадлежат уровню Ethernet (адрес отправителя и адрес получателя) и два – собственно ARP-протоколу (так же: адрес отправителя и адрес получателя). Значит, достаточно задать верными поля Ethernet, а поле ARP-протокола с физическим адресом отправителя любым и такой пакет спокойно пройдёт через коммутатор и создаст фиктивную запись в таблице жертвы. Аналогично для DHCP spoofing