# Лабораторная работа №3.1. Режим симуляции в Cicso Packet Tracer.

Состав сети: 4 узла, сервер, принтер и два концентратора. Концентраторы меж собой соединяются кроссоверным кабелем (рис.2.1).

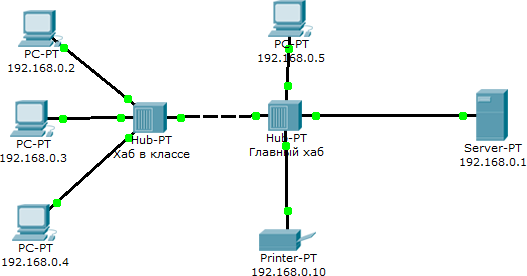


Рис.2.1. Схема сети.

Нужно перейти в режим симуляции (Shift+S), либо кликнув на иконку симуляции в правом нижнем углу рабочего пространства. Здесь мы видим окно событий, кнопка сброса (очищает список событий), управление воспроизведением и фильтр протоколов. Предложено много протоколов, но отфильтруем пока только ICMP, это исключит случайный трафик между узлами.

Для перехода к следующему событию используем кнопку "Вперёд", либо автоматика (рис.2.2).

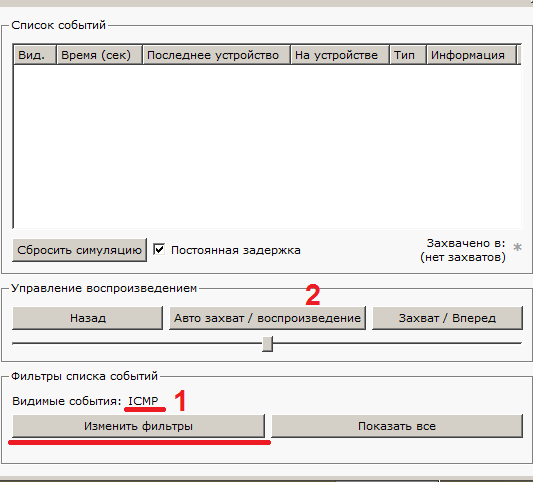


Рис.2.2. Интерфейс симулятора. Посылаем PING-запрос.

С одного из узлов попробуем пропинговать другой узел. Выбираем

далеко расположенные узлы, чтобы наглядней увидеть, как будут проходить пакеты по сети в режиме симуляции. Итак, входим на узел .4 и пошлём пинг- запрос на узел .5.

С розового узла пингуем зелёный. На розовом узле образовался пакет (конвертик), который ждёт (иконка паузы на нём). Запустить пакет в сеть можно нажав кнопку "Вперёд" в окне симуляции (рис.2.3).

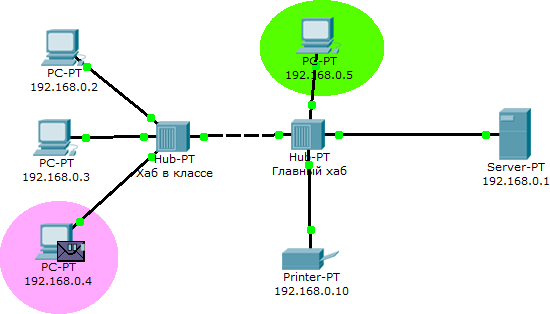


Рис.2.3. Демонстрация работы симулятора.

Так же в окне симуляции мы увидим этот пакет, отметив его тип (ICMP) и источник (192.168.0.4) – рис.2.4.

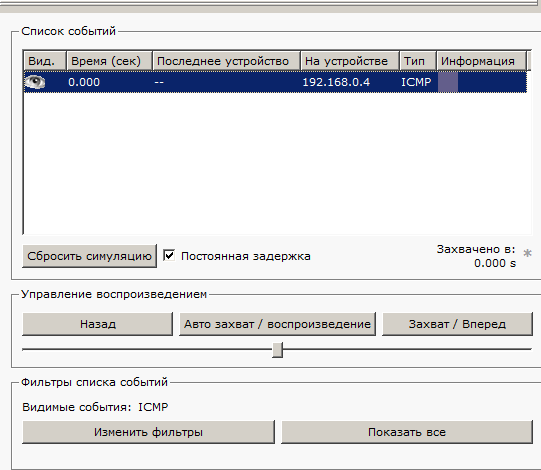


Рис.2.4. Мониторинг работы протоколов.

Клик на пакете покажет нам подробную информацию. При этом мы увидим модель OSI. Сразу видно, что на 3-ем уровне (сетевой) возник пакет на исходящем направлении, который пойдёт до второго уровня, затем до первого, на физическую среду и передастся на следующий узел (рис.2.5).

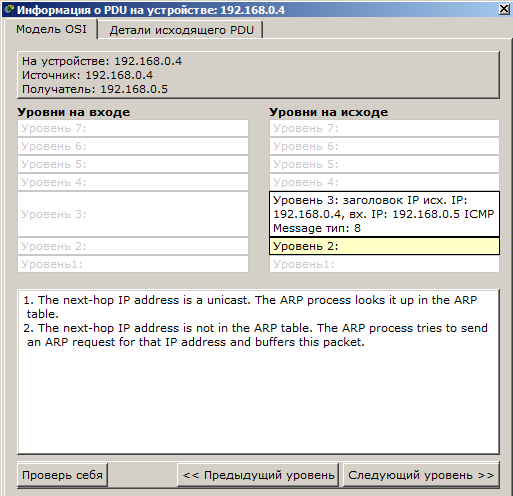


Рис.2.5. Мониторинг работы на модели OSI.

А на другой вкладке можно посмотреть структуру пакета (рис.2.6).

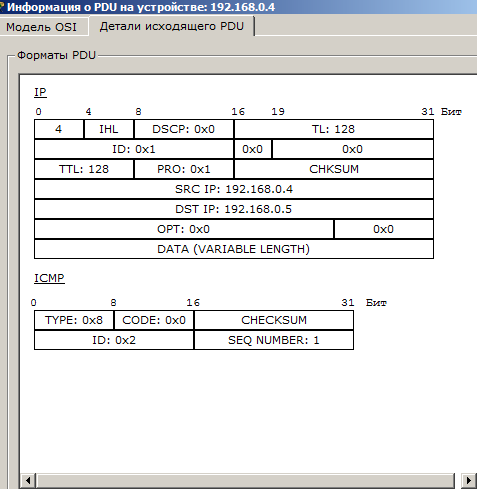


Рис.2.6. Структура пакета.

Нажмём кнопку "Вперёд". И пакет тут же двинется к концентратору. Это единственное сетевое подключение с этой стороны (2.7).

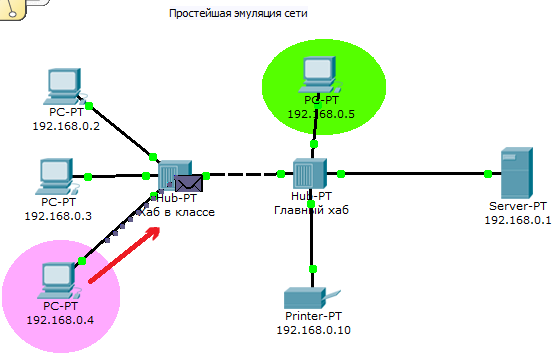


Рис.2.7. Прохождение пакета. Первый этап.

Концентратор повторяет пакет на всех остальных портах в надежде, что на одном из них есть адресат (рис.2.8)

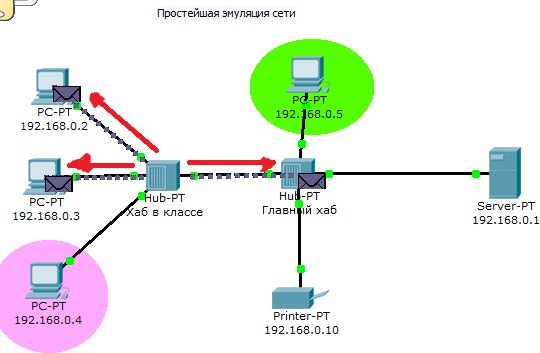


Рис.2.8. Прохождение пакета. Второй этап.

Если пакеты каким-то узлам не предназначенны, они просто игнорируют их (рис.2.9).

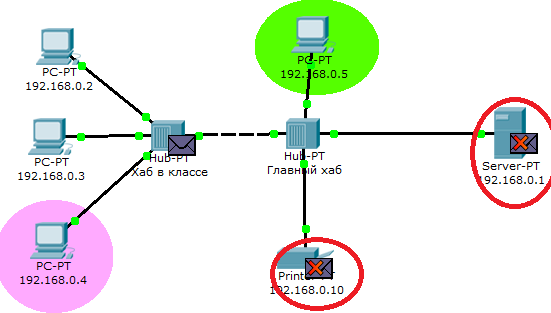


Рис.2.9. Прохождение пакета. Третий этап.

Когда пакет вернётся обратно, то увидим подтверждение соединения:

Контрольные вопросы.

1. Для чего используется режим симуляции?
2. Как просмотреть прохождение пакета по уровням модели OSI?
3. Можно ли определить причину того, что посланный в режиме симуляции пакет не дошел до адресата и на каком этапе произошел сбой работы сети?
4. Укажите в составе пакета IP адреса отправителя и получателя.
5. Как изменить фильтры списка событий?
6. Как в режиме симуляции определить, какие протоколы были задействованы в работе сети?
7. Как в режиме симуляции проследить изменение содержимого пакета при прохождении его по сети?
8. Перечислите основные возможности режима симуляции.

# Лабораторная работа № 3.2 ПОДКЛЮЧЕНИЕ К СЕТЕВОМУ ОБОРУДОВАНИЮ

**Цель работы**: Познакомиться с методами управления активным сетевым оборудованием

Способы подключения сетевого оборудования:

* С помощью консольного кабеля;
* По Telnet/SSH;
* Web-интерфейс;
* Специализированное ПО (SDM, IME, CSM); Для подключения необходимо:
* Компьютер;
* Консольный кабель;
* Переходник USB-to-Com;
* ПО (Putty/SecureCRT)

Рассмотрим процесс подключения коммутатора в Cisco Packet Tracer:

1. Подключаемся по консоли:
   1. Запускаем Cisco Packet Tracer;
   2. В рабочую область добавляем компьютер и коммутатор (2960). И соединяем консольным кабелем (Console) RS 232-Console. В конфигурации компьютера выбираем Terminal;
   3. В Terminal заходим в привилегированный режим с помощью команды enable.
   4. Перед настройкой необходимо войти в режим «глобального конфигурирования» с помощью команды configure terminal.
   5. Для безопасности создадим пароль на вход в привилегированный режим. Набираем enable password parol. Вместо parol вводим свой пароль.
   6. Однако применение enable password не совсем безопасно. Если ввести show run, то мы увидим строку enable password parol. Для того чтобы это скрыть сделаем следующее:
      * Набираем команду configure terminal. Затем вводим команду service password-encryption.
      * Выходим из режима конфигурации и вводим команду show run. Как видно из рис.10 пароль зашифрован

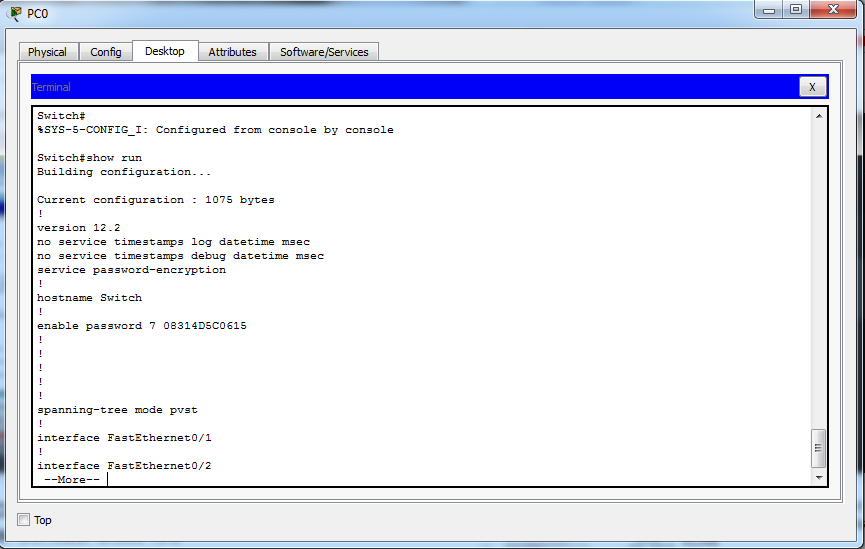


Рис. 10. Пароль на привилегированный режим с помощью команды enable secret

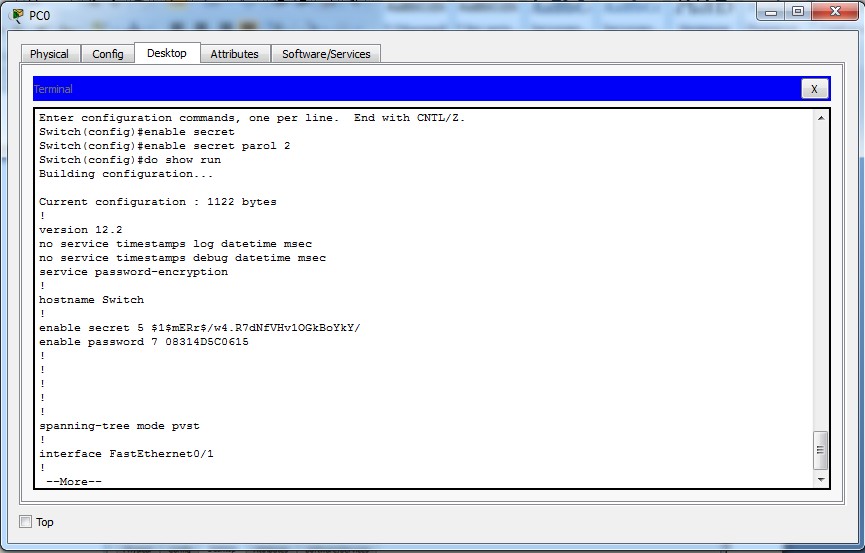


Рис. 11. Пароль на привилегированный режим с помощью команды enable password

* 1. Второй способ задания пароля:
     + Заходим в режим «глобального конфигурирования». Вводим команду enable secret parol2;
     + Затем выходим из режима конфигурации и вводим команду show run. И на рис. 11 видно, что наш второй пароль также зашифрован. При этом приоритет имеет именно этот пароль.

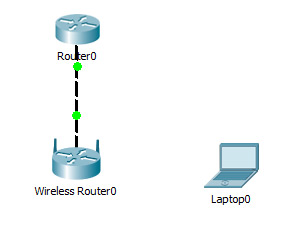
1. Создадим пользователя.
   1. Заходим в привилегированный режим «глобального конфигурирования»;
   2. Вводим команду username admin privilege?. Выходит значение от 0-
2. При 15 пользователю доступны все команды. Здесь admin – имя пользователя. Затем вводим команду username admin 15 password parol. Здесь parol – пароль. Локальный пользователь создан;
   1. Установим авторизацию на подключение к консоли:
      1. Заходим в режим «конфигурирования терминальных линий». В режиме «глобального конфигурирования» набираем команду line console 0;
      2. Набираем команду login local;
      3. Выходим из всех режимов конфигурации с помощью команды end. Теперь при попытке входа в консоль требуется ввести имя пользователя и пароль, вводим их. Доступ к консоли защищен;
   2. Задаем IP адрес устройства.
      1. Заходим в режим «глобального конфигурирования». Вводим команду interface Vlan1;
      2. Набираем команду ip address 192.168.1.1 255.255.255.0. Здесь 192.168.1.1 – IP адрес, 255.255.255.0 – маска подсети для того, чтобы убедиться, что интерфейс поднят набираем команду no shutdown;
      3. Выходим из режима конфигурирования интерфейса с помощью команды end.
   3. Настроим виртуальные терминальные линии;
      1. Заходим в режим глобального конфигурирования. Набираем команду line vty 0 4;
      2. Определим транспортный протокол. Введем команду transport input

telnet;

* + 1. Создадим пароль на вход с помощью команды login local;
    2. Выходим из режима конфигурирования и сохраняем конфигурации write memory;
  1. Конфигурация сохранена. Чтобы проверить выполним следующие действия:
     1. Для этого в Cisco Packet Tracer подключим компьютер прямым кабелем с коммутатором по FastEthernet;
     2. Сконфигурируем IP адрес из той же сети, что и IP адрес нашего коммутатора. В настройках компьютера в IP адресе введем 192.168.1.2;
     3. В командной строке вызовем команду telnet 192.168.1.1 с адресом коммутатора;
     4. Коммутатор запросил имя пользователя и пароль (Username – admin, password – parol). Таким образом, мы зашли удаленно на наш коммутатор.

**Лабораторная работа №3.3 WI-FI**

Создать модель локальной сети, состоящей из обычного домашнего wi-fi роутера и  маршрутизатора, который имитирует провайдера Интернета. Использовать интерфейс Fast Ethernet. Добавим ещё пользовательское устройство, например ноутбук. Установим модуль wi-fi (WPC300N) в ноутбук.

****

Настройка модели

1)Настройки маршрутизатора провайдера Router0 (жирным выделено то, что необходимо ввести с клавиатуры:

Router>en  
Router#  
Router#conf t  
Enter configuration commands, one per line. End with CNTL/Z.  
Router (config)#int fa0/0  
Router (config-if)#ip address 210.210.0.1 255.255.255.252  
Router (config-if)#no shutdown

Router (config-if)#  
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

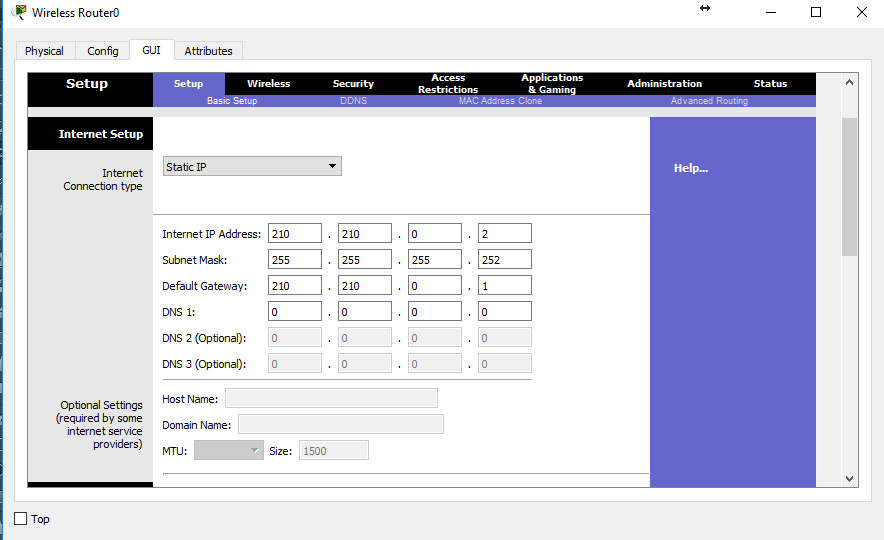
Router (config-if)#end  
Router#  
%SYS-5-CONFIG\_I: Configured from console by console

Router#wr mem  
Building configuration...  
[OK]

2)Настройки домашнего wi-fi маршрутизатора Wireless Router0

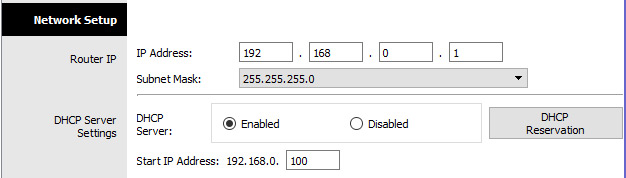
выполняется  с помощью веб интерфейса.

Настройка внешнего интерфейса во вкладке Setup показана на рисунке.

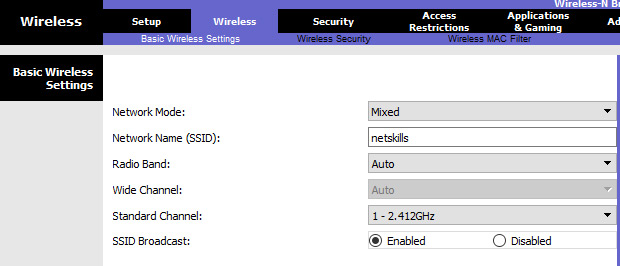
****

Настройка локальной сети (Network Setup)

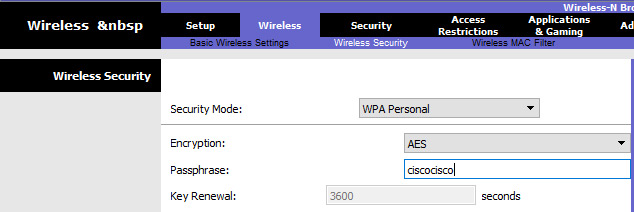
Выбираем по умолчанию ip-адрес 192.168.0.1, маска 24-битная 255.255.255.0, разрешён DHCP-сервер, начало раздачи с адреса 192.168.0.100 и всё. После чего незабываем сохранить настройки, нажать на кнопку внизу формы Save Settings.

****

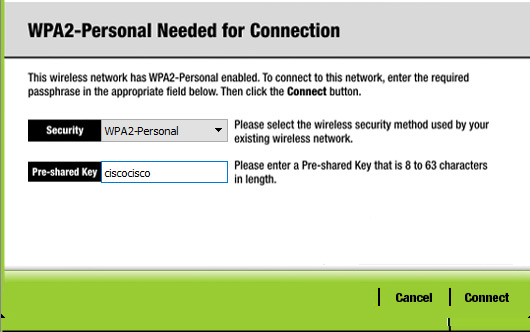
Настройки во вкладке Wireless, т.е. wi-fi. Выбираем основные настройки вайфая: режим (mode), мы выбираем смешанный (mixed); идентификатор сети (SSID) — netskills; ширина канала (Radio Band) — auto; частоту — 1-2.412HGz; видимость сети (SSID Broadcast) — видимая (enable). Сохраняем настройки.

****

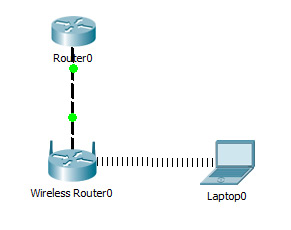
Переходим ко вкладке Wireless Security. Выбираем режим шифрования WPA2 Personal, алгоритм шифрования AES, ключевое слово для выбранного режима шифрования не менее 8 символов. Сохраняем.

****

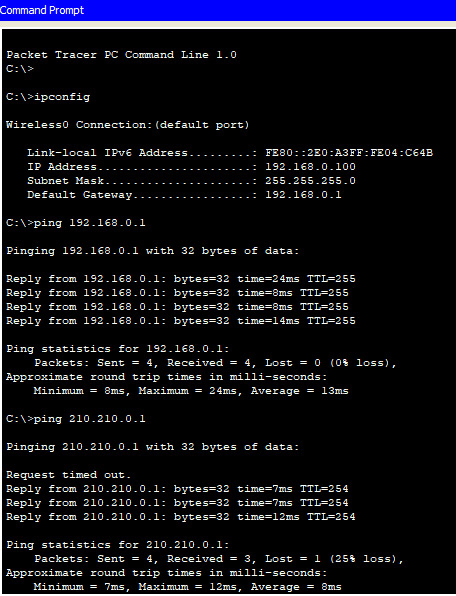
3)Настройка wi-fi адаптера на ноутбуке. Вкладка Desktop->PC Wireless->Connect. Смотрим доступные нам сети. Нажимаем кнопку Connect для подключения к сети netskills.

****

Если настройки произведены верно, то появиться пунктирная линия между wi-fi маршрутизатором и ноутбуком как на рисунке.

****

Введём на ноутбуке в командной строке команду ipconfig, чтобы проверить правильность настроек. Из рисунка видно, что DHCP- сервер присвоил правильный ip 192.168.0.100 Пропингуем шлюз (wi-fi маршрутизатор) и пропингуем адрес интернет провайдера. На рисунке видно, что в обоих случаях пинг идёт.

****

При этом NAT мы не использовали, так как практически на всех wi-fi маршрутизаторах NAT используется по умолчанию.