

Введение

Дисциплина «Сети и системы телекоммуникаций» направлена на подготовку в будущей профессиональной деятельности, при выполнении которой требуются знания и умения, связанные с выполнением студентами принципов создания и функционирования сетей передачи данных, правил функционирования телекоммуникационного оборудования, а также принципов работы сетевых протоколов.

Процесс изучения дисциплины включает лекции, лабораторные занятия и самостоятельную работу. Цель лабораторных занятий – приобретение навыков создания и настройки локальных вычислительных сетей с использованием современного сетевого оборудования. В ходе лабораторного практикума решаются следующие задачи:

- Закрепить и актуализировать теоретические знания, полученные на лекциях
- Познакомиться с основными видами сетевого оборудования, используемого в современных телекоммуникационных сетях
- Получить навыки установки и настройки сетевого оборудования
- Познакомиться с основными сетевыми протоколами и особенностями их настройки
- Получить первоначальные навыки поиска и устранения неисправностей в современных телекоммуникационных сетях

Общие указания к проведению лабораторных работ

Занятия проводятся в специализированном компьютерном классе. Каждая лабораторная работа выполняется индивидуально на персональном компьютере. Для выполнения лабораторной работы студенту достаточно владеть элементарными навыками пользователя персонального компьютера, уметь работать с клавиатурой и мышью, следовать методическим указаниям и инструкциям.

При подготовке к лабораторной работе необходимо пользоваться методическими указаниями, относящимися к данной работе, и теоретическими сведениями из пройденного теоретического курса. Настоятельно рекомендуется выполнять лабораторные работы в соответствии с календарным планом в течение всего семестра, так как предложенный порядок выполнения работ соответствует полученным на лекциях знаниям и способствует закреплению пройденного теоретического материала.

Все лабораторные работы выполняются в виртуальной лаборатории при помощи специализированного программного обеспечения – Cisco Packet Tracer. Это свободно доступный программный продукт, разработанный и выпускаемый фирмой Cisco Systems в учебных целях.

Cisco Packet Tracer – это симулятор телекоммуникационных сетей, он позволяет строить работоспособные модели сети, настраивать маршрутизаторы и коммутаторы (преимущественно производства фирмы Cisco Systems), в произвольных топологиях с поддержкой разных протоколов. В симуляторе реализованы серии маршрутизаторов Cisco 800, 1800, 1900, 2600, 2800, 2900 и коммутаторов Cisco Catalyst 2950, 2960, 3560, а также межсетевой экран ASA 5505. Беспроводные устройства представлены маршрутизатором Linksys WRT300N, точками доступа и сотовыми вышками. Кроме того, есть серверы DHCP, HTTP, TFTP, FTP, DNS, AAA, SYSLOG, NTP и EMAIL, рабочие станции, различные модули к компьютерам и маршрутизаторам, IP-фоны, смартфоны, хабы, а также облако, эмулирующее глобальные сети. Объединять сетевые устройства можно с помощью различных типов кабелей, таких как прямые и обратные патч-корды, оптические и коаксиальные кабели, последовательные кабели и телефонные пары.

Cisco Packet Tracer позволяет создавать довольно сложные макеты сетей, что зачастую нереально сделать на реальном оборудовании, проверять на работоспособность топологии. Однако, реализованная функциональность устройств ограничена и не предоставляет всех возможностей реального

оборудования, но зато приспособлена для понимания основных концепций устройства вычислительных сетей.

Отчётность по курсу

В качестве отчёта по лабораторной работе принимается файл с созданной студентом сетью в формате Cisco Packet Tracer (с расширением pkt). Файл должен содержать:

- Визуальную схему сети
- Используемую в сети адресацию в виде надписей
- Сетевое и конечное оборудование в соответствии с заданием
- Линии связи между оборудованием
- Активное оборудование должно быть настроено согласно заданию
- Должны использоваться индивидуальные диапазоны IP-адресов, выделенные каждому студенту
- Сеть должна обеспечивать движение (а в некоторых лабораторных – также и блокирование) пакетов между узлами сети. Для проверки этого (если не указано обратное) используются:
 - Команда ping
 - Команда traceroute (tracert)
 - Визуализация движения пакетов средствами Cisco Packet Tracer (*Simulation Mode*)

Лабораторная работа № 1. ПРОСТЕЙШАЯ СЕТЬ

Цель работы: создать минимальную телекоммуникационную сеть при помощи Cisco Packet Tracer

Для организации простейшей сети необходимо:

- Два компьютера;
- Коммутационный кабель (патч-корд).

Коммутационный кабель бывает двух видов:

1. Прямой кабель (straight through cable)

Для соединения типа компьютер-коммутатор, коммутатор-маршрутизатор.

2. Перекрестный кабель (crossover cable)

Для соединения типа компьютер-компьютер, коммутатор-коммутатор, маршрутизатор-маршрутизатор.

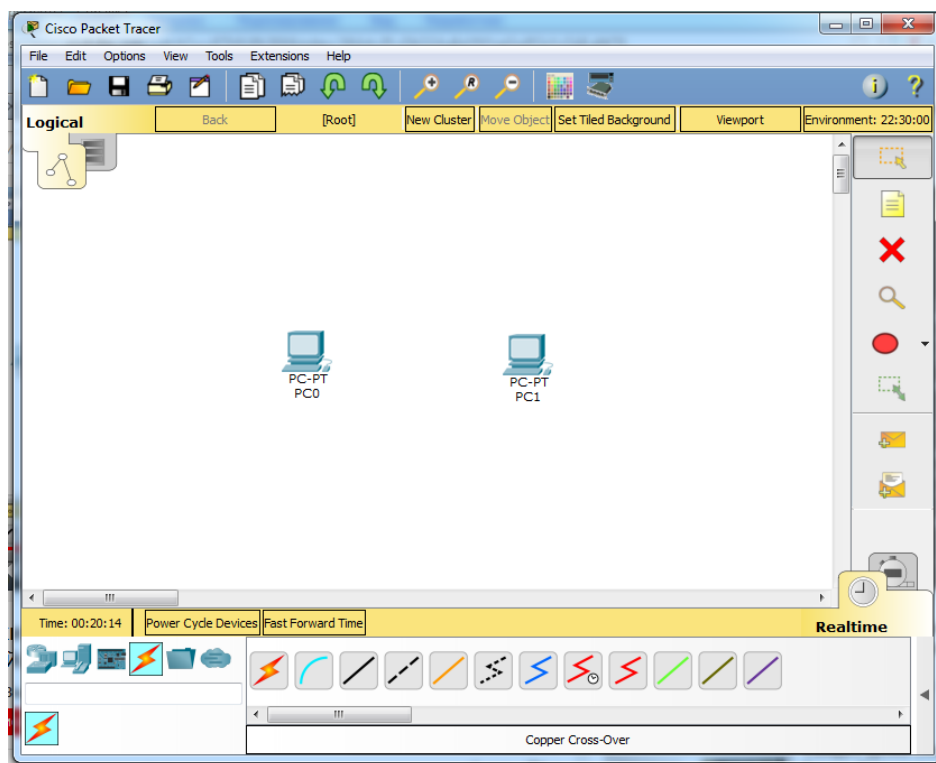


Рис. 1. Рабочая область Cisco Packet Tracer

Создаем простейшую сеть с помощью Cisco Packet Tracer:

1. Открываем Cisco Packet Tracer;

2. Выбираем компьютер и перетаскиваем его на рабочую область (рис.1);
3. Аналогично выбираем второй компьютер (рис. 1);
4. Переходим на вкладку Connections (рис. 1). Выбираем тип кабеля (в нашем случае перекрестный). И подключаем Fast Ethernet – Fast Ethernet (рис. 2).

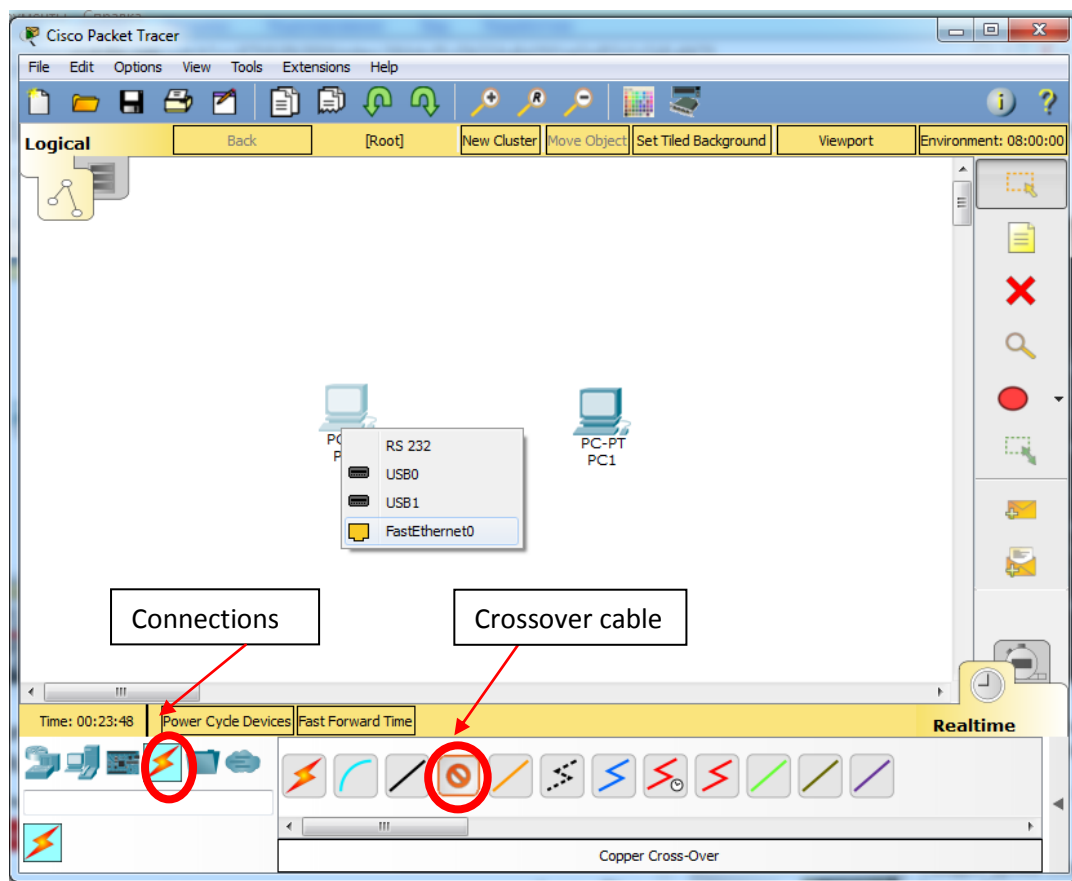


Рис. 2. Простейшая сеть

5. Переходим к настройке компьютеров. Переходим во вкладку Desktop-IP Configuration и вводим IP адрес (например, 192.168.1.1) (рис. 3). Аналогично проводим со вторым компьютером.

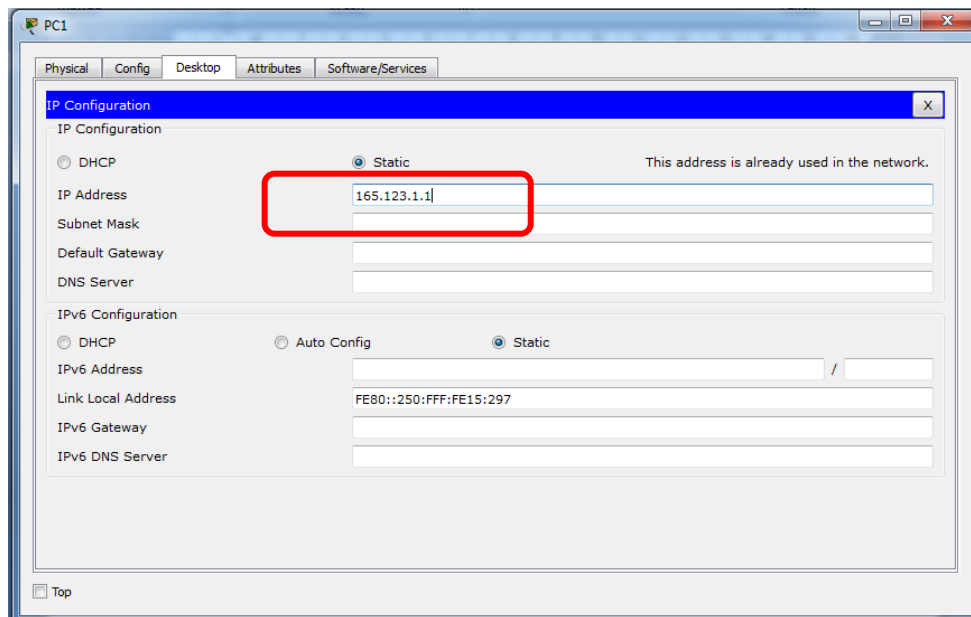


Рис. 3. Настройка компьютеров

6. Проверим соединение. Выбираем Desktop-Command Prompt. Вводим в нашем случае ping 192.168.1.1. Результат приведен на рис. 4.

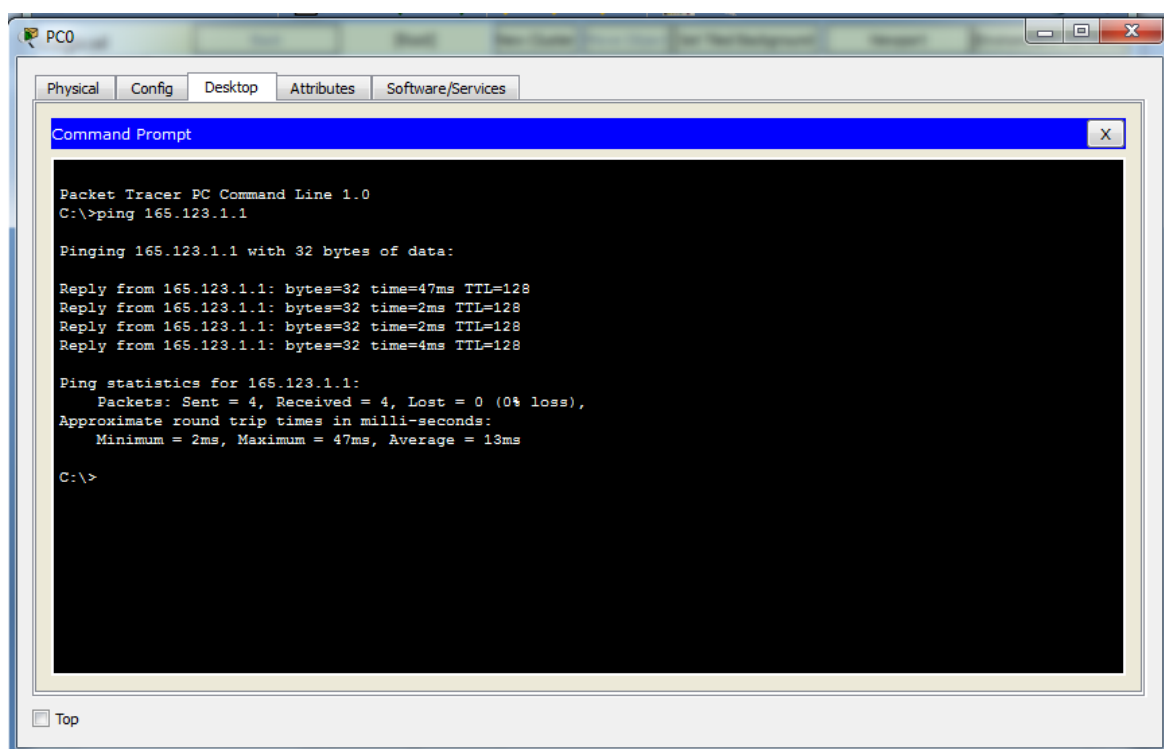


Рис. 4. Проверка соединения

Лабораторная работа № 2. ОРГАНИЗАЦИЯ СЕТИ С ПОМОЩЬЮ КОММУТАТОРА

Цель работы: построить работоспособную сеть на основе концентраторов и коммутаторов Ethernet

Если в сети появляется более двух компьютеров, то необходимы следующие устройства:

- Сетевой концентратор (hub);
- Коммутатор (switch).

Для организации сети с помощью коммутатора с использованием Cisco Packet Tracer необходимо:

1. Запустить Cisco Packet Tracer;
2. Пусть в сети будет 4 компьютера. Перетаскиваем 1 компьютер, настраиваем IP адрес (например, 192.168.1.1, как было сделано в лабораторной работе №1). Аналогично создаем 2-4 компьютеры. В настройках IP адреса, меняем только одну цифру (в нашем случае 192.168.1.2). Результат на рис.5
3. Рассмотрим 2 случая.
 - 3.1. В первом выбираем Switches – коммутатор 2960 (рис. 5).
 - Переходим на вкладку Connections (как было сделано в лабораторной работе №1). Выбираем тип кабеля (в нашем случае прямой). И подключаем Fast Ethernet – Fast Ethernet (рис. 6). Если link загорелся зеленым, то значит наша сеть функционирует;
 - Аналогично лабораторной работе №1 проверим работоспособность сети. На рис. 7 приведен результат проверки для компьютера 2 с компьютерами 1,3 и 4.
 - 3.2. Во втором случае выбираем Hubs (рис. 8).
 - Переходим на вкладку Connections. Выбираем тип кабеля (в нашем случае прямой) и подключаем;
 - Проверяем работоспособность сети.

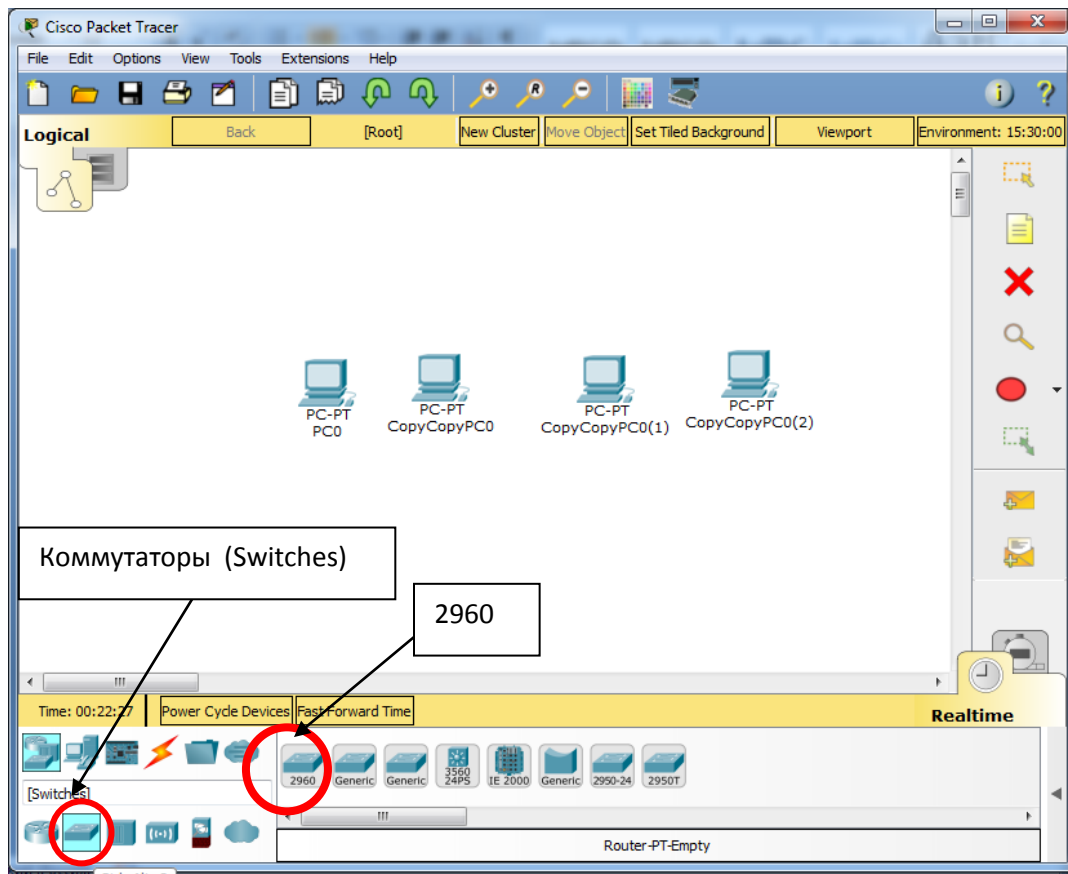


Рис. 5. Организация сети 4 компьютеров

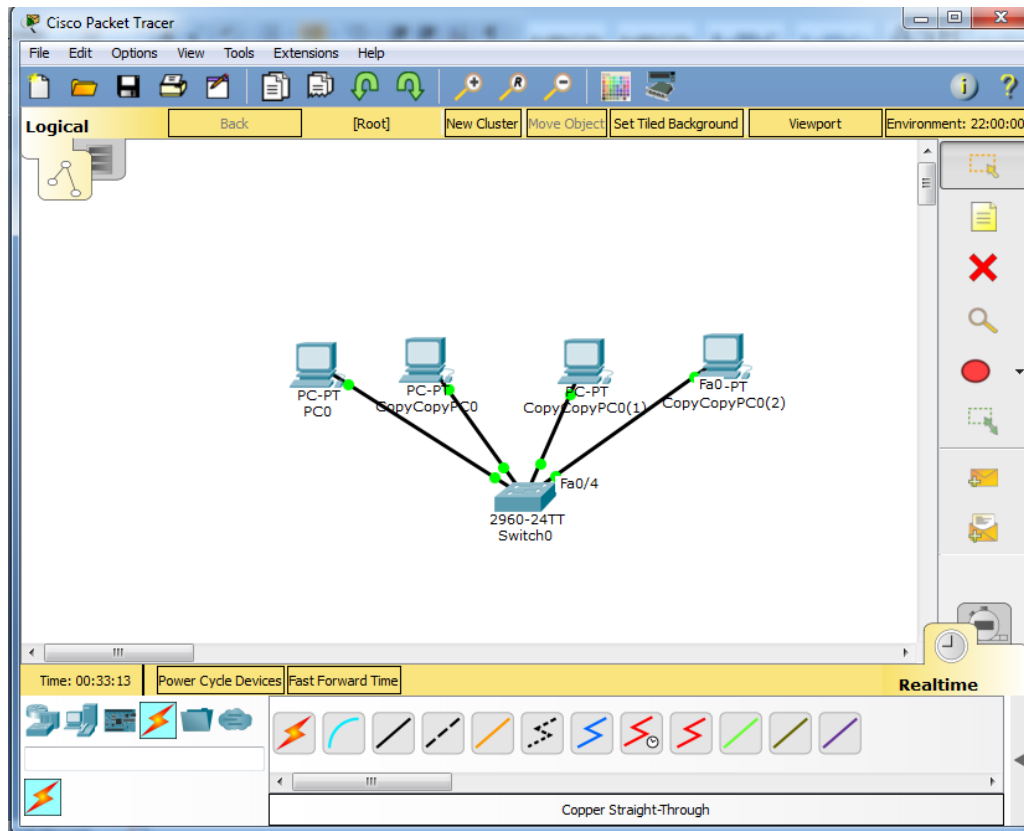


Рис. 6. Организация сети 4 компьютеров с помощью коммутатора

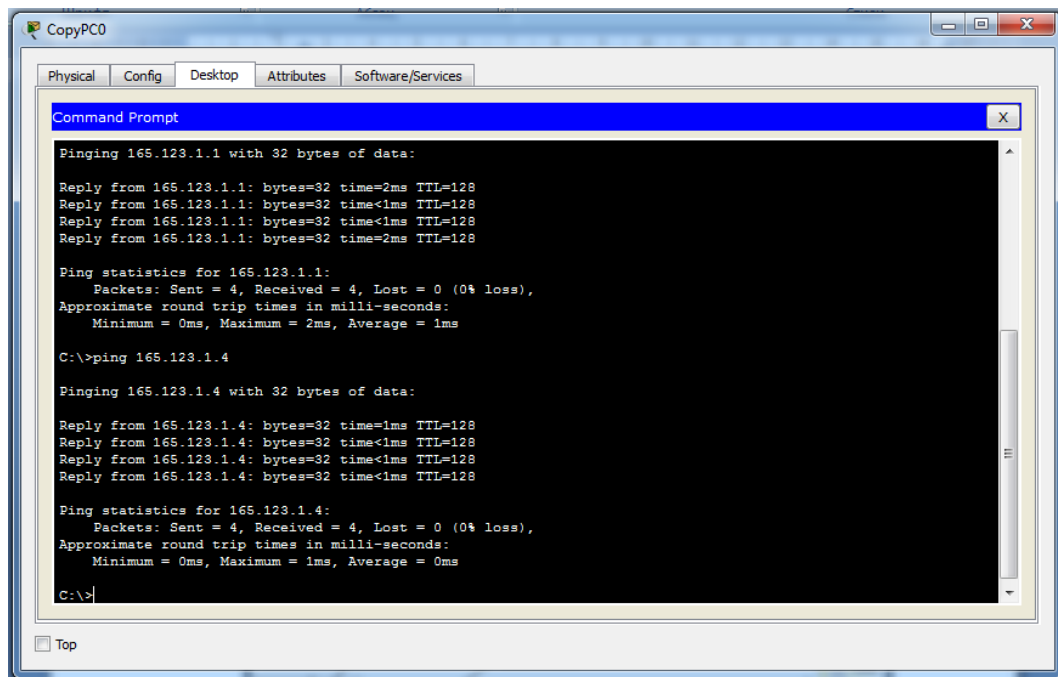


Рис. 7. Проверка работы сети

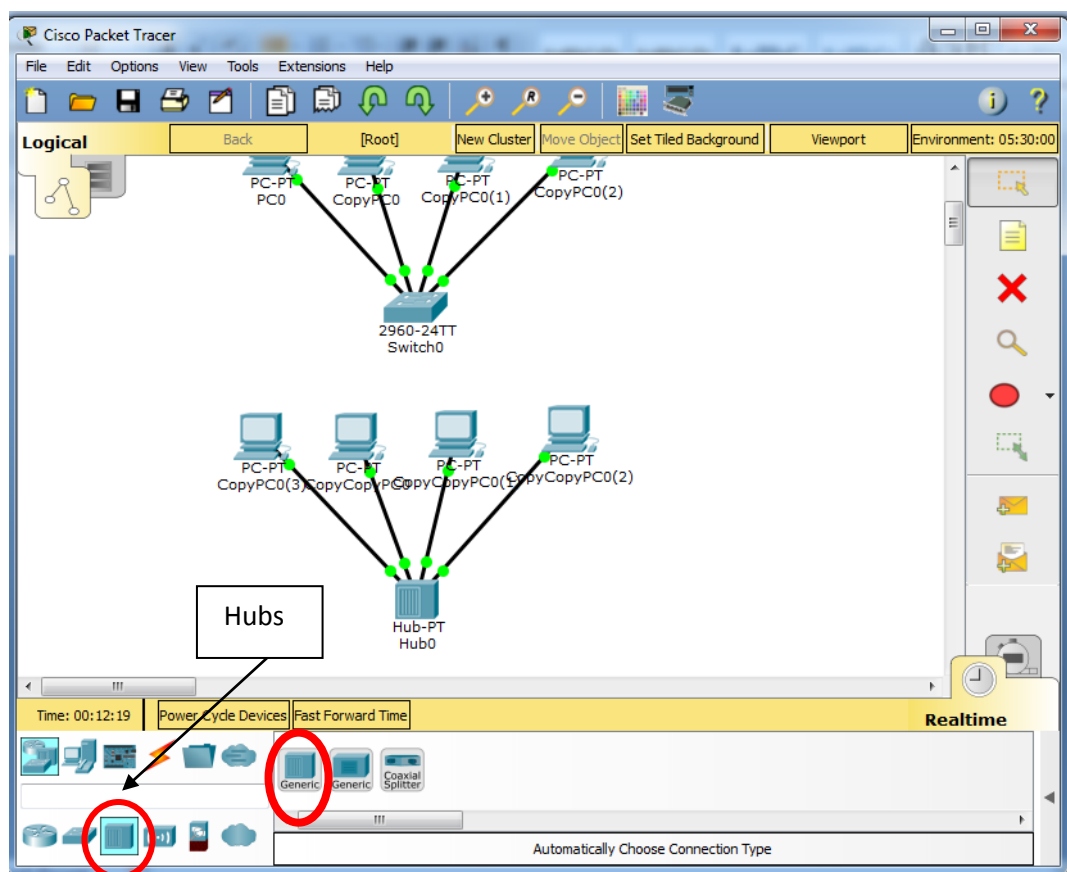


Рис. 8. Организация сети 4 компьютеров с помощью hub

4. Воспользуемся визуализацией прохождения пакета с помощью функции Add Simple PDU (P). Например, с компьютера 2 передаем пакет на компьютер 3.

5. Затем переходим во вкладку Simulation – Capture/Forward. Результат передачи приведен на рис. 9.

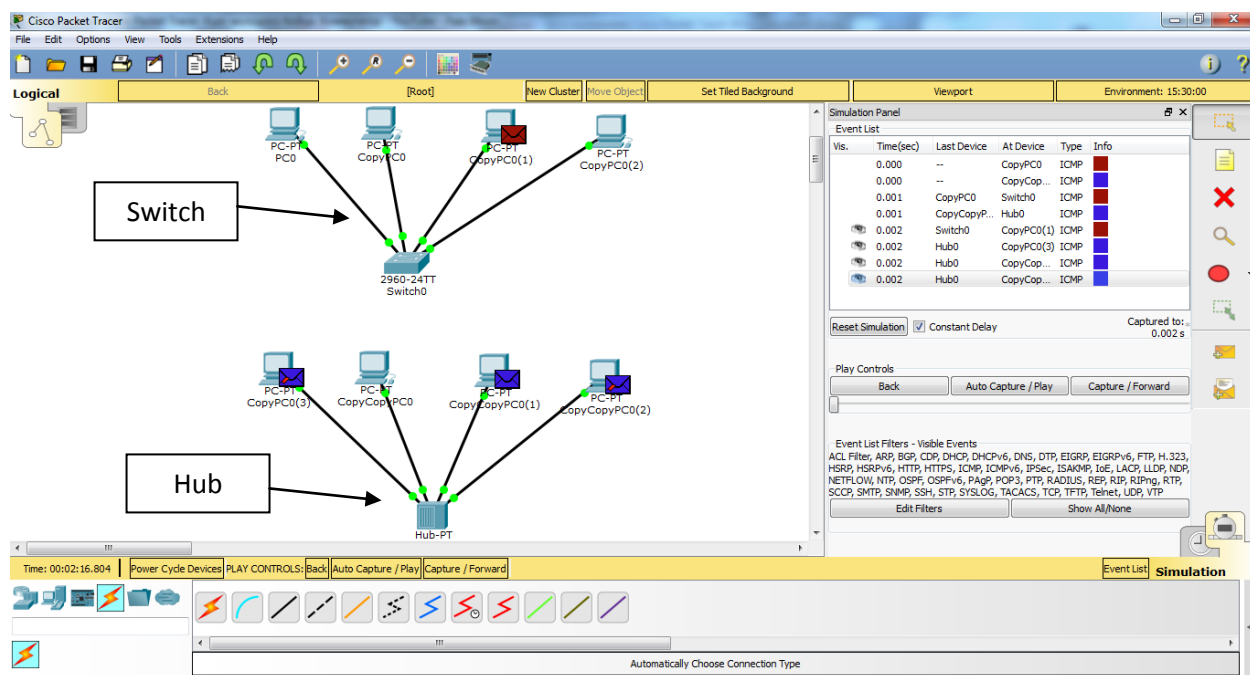


Рис. 9. Результат передачи пакета с компьютера 2 на компьютер 3

Лабораторная работа № 3. 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:

1.1. Запускаем Cisco Packet Tracer;

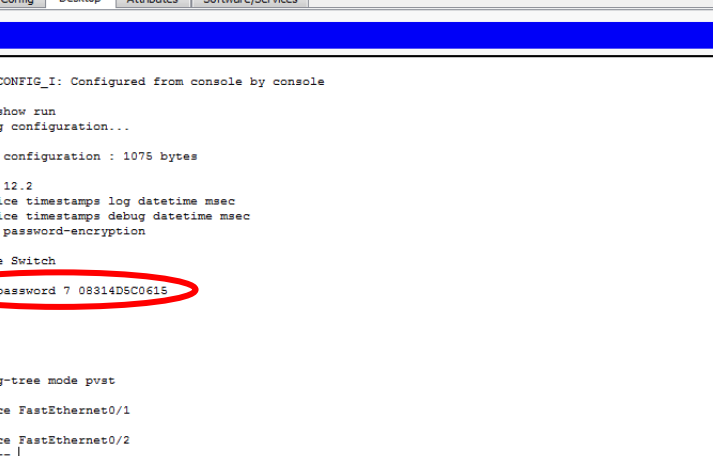
1.2. В рабочую область добавляем компьютер и коммутатор (2960). И соединяем консольным кабелем (Console) RS 232-Console. В конфигурации компьютера выбираем Terminal;

1.3. В Terminal заходим в привилегированный режим с помощью команды enable.

1.4. Перед настройкой необходимо войти в режим «глобального конфигурирования» с помощью команды configure terminal.

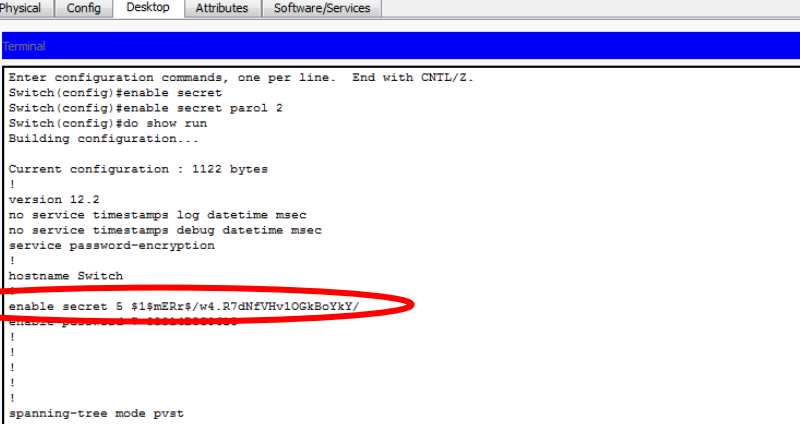
1.5. Для безопасности создадим пароль на вход в привилегированный режим. Набираем enable password parol. Вместо parol вводим свой пароль.

1.6. 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:

- 
- The screenshot shows a PC window titled "PC0" with a terminal window open. The terminal window has a blue header bar with the word "terminal" and a close button. The terminal content shows the following commands and output:
- ```
Switch#
Switch#sys-config I: Configured from console by console

Switch#show run
Building configuration...

Current configuration : 1075 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Switch
!
enable password 7 08314D5C0615
!
!
!
!
spanning-tree mode pvst
!
interface FastEthernet0/1
!
interface FastEthernet0/2
--More--
```
- The command "enable password 7 08314D5C0615" is circled in red. The terminal window has a scrollbar on the right side.



The screenshot shows a PC window titled "PC0" with a terminal application open. The terminal has tabs for "Physical", "Config", "Desktop", "Attributes", and "Software/Services". The "Config" tab is active, displaying a terminal session with the following text:

```
terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#enable secret
Switch(config)#enable secret parol 2
Switch(config)#do show run
Building configuration...

Current configuration : 1122 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname Switch
enable secret 5 1mERs/w4.R7dNFVHv1OGkBoYkY/
enable password 8 888888888888
!
!
!
!
!
!
spanning-tree mode pvst
!
interface FastEthernet0/1
!
--More--
```

The line `enable secret 5 $1$mERs/w4.R7dNFVHv1OGkBoYkY/` is circled in red.

### 1.7. Второй способ задания пароля:

- 14

- 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.

## 2. Создадим пользователя.

2.1. Заходим в привилегированный режим «глобального конфигурирования»;

2.2. Вводим команду `username admin privilege?`. Выходит значение от 0-15. При 15 пользователю доступны все команды. Здесь `admin` – имя пользователя. Затем вводим команду `username admin 15 password parol`. Здесь `parol` – пароль. Локальный пользователь создан;

## 3. Установим авторизацию на подключение к консоли:

3.1. Заходим в режим «конфигурирования терминальных линий». В режиме «глобального конфигурирования» набираем команду `line console 0`;

3.2. Набираем команду `login local`;

3.3. 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;

## 4. Задаем IP адрес устройства.

4.1. Заходим в режим «глобального конфигурирования». Вводим команду `interface Vlan1`;

4.2. 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`;

4.3. Выходим из режима конфигурирования интерфейса с помощью команды `end`.

## 5. Настроим виртуальные терминальные линии;

5.1. Заходим в режим глобального конфигурирования. Набираем команду `line vty 0 4`;

5.2. Определим транспортный протокол. Введем команду `transport input telnet`;

5.3. Создадим пароль на вход с помощью команды `login local`;

5.4. Выходим из режима конфигурирования и сохраняем конфигурации `write memory`;

6. Конфигурация сохранена. Чтобы проверить выполним следующие действия:

6.1. Для этого в Cisco Packet Tracer подключим компьютер прямым кабелем с коммутатором по FastEthernet;

6.2. Сконфигурируем IP адрес из той же сети, что и IP адрес нашего коммутатора. В настройках компьютера в IP адресе введем 192.168.1.2;

6.3. В командной строке вызовем команду `telnet 192.168.1.1` с адресом коммутатора;

6.4. Коммутатор запросил имя пользователя и пароль (Username – admin, password – parol). Таким образом, мы зашли удаленно на наш коммутатор.

## **Лабораторная работа № 4. ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИИ VIRTUAL LOCAL AREA NETWORK**

**Цель работы:** создать сеть, состоящую из двух независимых виртуальных подсетей

**Преимущества VLAN:**

- Помогает структурировать сеть;
- Используется для обеспечения безопасности;
- Используется для объединения;
- Уменьшает количество широковещательного трафика.

**Типы портов:**

- Access Port – для подключения конечных устройств;
- Trunk Port – для соединения между коммутаторами.

В данной лабораторной работе рассмотрим две схемы:

1. Схема с одним коммутатором. Для этого выполним следующие действия:

- Создаем VLAN;
- Определяем Access порты.

2. Схема с двумя коммутаторами. Для этого выполним следующие действия:

- Создаем VLAN;
- Определяем Access порты;
- Определяем Trunk порты.

Рассмотрим процесс создания VLAN в Cisco Packet Tracer.

**Схема с одним коммутатором:**

1. Запускаем Cisco Packet Tracer;
2. Добавляем коммутатор 2960;
3. Добавляем 4 компьютера;
4. Используем прямым кабелем каждый компьютер с коммутатором;

5. Пусть компьютеры PC0, PC1 принадлежат одному сегменту (например, технологи). А PC2 и PC3 принадлежат второму сегменту (например, менеджеры). Выделим каждый сегмент своим цветом. Для этого выберем функцию Draw и выделим каждый сегмент (например, эллипсом) своим цветом (рис. 12);

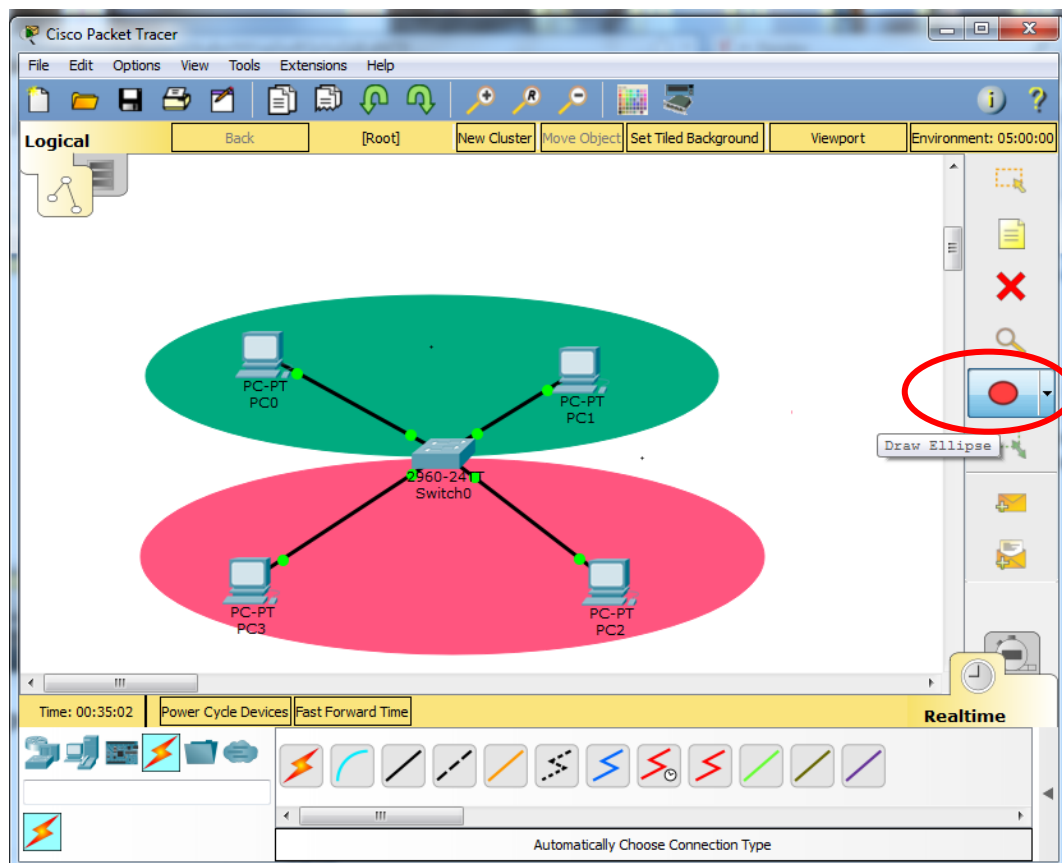


Рис. 12. Схема с одним коммутатором

6. Заходим в настройки коммутатора (вкладка CLI). Входим в привилегированный режим, режим глобального конфигурирования:

6.1. На данном этапе необходимо определить VLAN, в котором будут находиться данные пользователи. По умолчанию все порты коммутатора находятся в VLAN1, мы определим в другой. Для этого создадим VLAN2 (команда `VLAN 2`) и дадим имя `technologi` (команда `name технологи`). Выходим из режима VLAN;

6.2. Теперь настроим интерфейс. Мы подключили PC0 к порту Fast Ethernet0/1, а PC0 к порту Fast Ethernet0/4. Данные порты необходимо определить в только что созданный VLAN2. Для этого заходим в настройки



интерфейса Fast Ethernet0/1 с помощью команды interface Fast Ethernet 0/1. Определяем, что данный порт функционирует в режиме Access (команда switchport mode access), и определяем VLAN2 (команда switchport access VLAN 2). Аналогично настраиваем порт Fast Ethernet0/4. Выходим из режима конфигурирования. Прделанную работу можно проверить с помощью команды show VLAN или show VLAN brief. Из рис. 13 можно увидеть, что порты Fast Ethernet 0/1 и Fast Ethernet 0/4 определены в VLAN2;

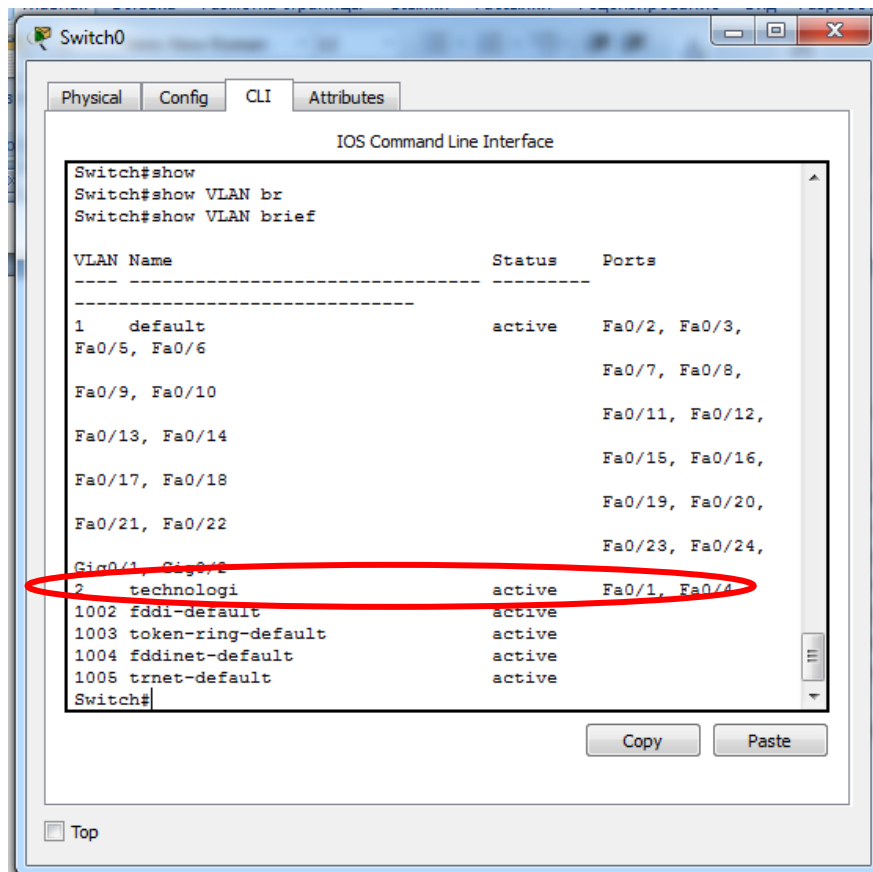


Рис. 13. Настройка портов fastEthernet0/1 и fastEthernet0/4

6.3. Прodelать аналогичные действия для сегмента менеджеры в VLAN3 с названием managers. Для нашего случая результат приведен на рис. 14;

6.4. Теперь зададим IP адреса (например, для PC0 зададим 192.168.2.1, для PC1 зададим 192.168.2.2, для PC2 зададим 192.168.3.2, для PC3 зададим 192.168.3.1).

6.5. Проверим. Заходим в Command Prompt для сегмента technologi. Набираем ping 192.168.2.2. Аналогично проведите со вторым сегментом.

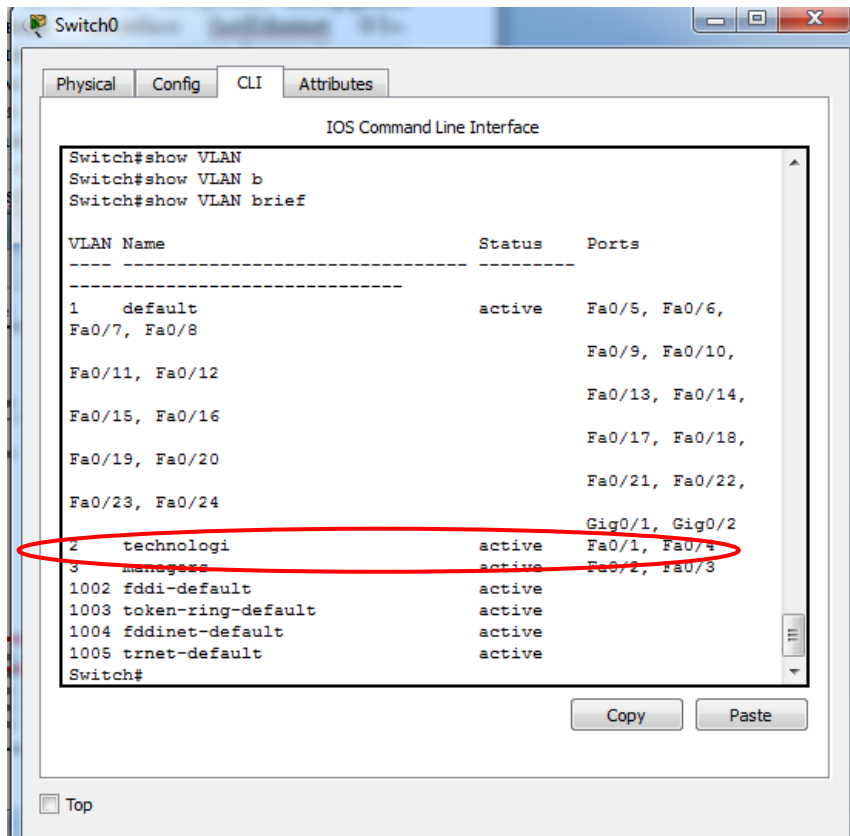


Рис. 14. Настройка портов fastEthernet0/2 и fastEthernet0/3

### Схема с двумя коммутаторами:

1. Создадим еще одну сеть, состоящую из одного коммутатора и 4 компьютеров, соединим два коммутатора перекрестным кабелем к портам GigabitEthernet (рис. 15). Для удобства скопируем первую сеть.

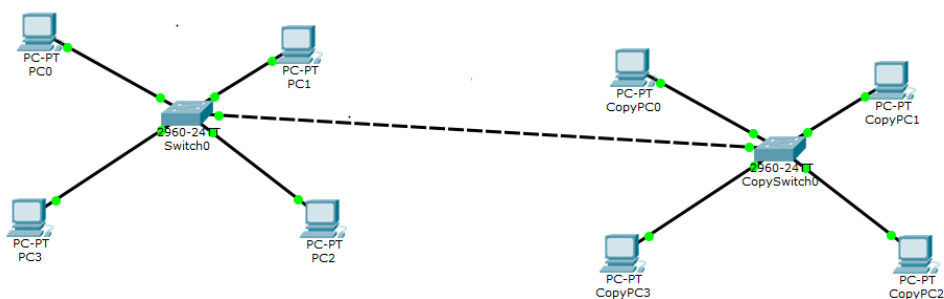


Рис. 15. Схема с двумя коммутаторами

2. Добавим IP адреса, для компьютеров CopyPC0 – 192.168.2.3, CopyPC1 – 192.168.2.4, CopyPC3 – 192.168.3.3, CopyPC4 – 192.168.3.4. И объединим их в два сегмента *technologi* и *managers*;

3. Настройки для коммутатора сохранены.
4. Настроим Trunk порт:
  - 4.1. Режим конфигурирования. Набираем команду `interface gigabitEthernet 0/1, switchport mode trunk`. Указываем VLAN, которые мы хотим передавать через наше физическое соединение с помощью команды `switchport trunk allowed vlan 2,3`.
  - 4.2. Настраиваем Trunk порт для второго коммутатора.
5. Проверьте взаимодействие данных компьютеров.

## Лабораторная работа № 5. УСТРАНИЕНИЕ ПЕТЕЛЬ С ПОМОЩЬЮ ПРОТОКОЛА STP

**Цель работы:** создать отказоустойчивую сеть Ethernet с использованием протокола остовного дерева

Методы организации отказоустойчивых каналов связи:

- Резервирование соединений;
- Агрегирование каналов – объединение нескольких физических каналов в один логический.

Spanning Tree Protocol (STP):

- Протокол 2-го уровня модели OSI;
- Защита от петель в сети;
- Автоматическое резервирование каналов;
- Время сходимости 30-50 секунд;
- Альтернативы: RSTP, MSTP (время сходимости менее секунды).

Алгоритм работы протокола STP:

1. Выбирается корневой коммутатор (Root Bridge);
2. Выбирается корневой порт на некорневом коммутаторе;
3. Выбор назначенного порта.

Состояние портов:

1. Блокировка;
2. Прослушивание;
3. Обучение;
4. Передача.

**Рассмотрим резервирование соединений:**

1. Запускаем Cisco Packet Tracer;
2. Добавляем 3 коммутатора (например, 2960). Соединим их;
3. Определим корневой коммутатор. Заходим в CLI коммутатора (например, в нашем случае это Switch2). Заходим в привилегированный режим. С помощью команды `show spanning tree` можно увидеть, что он является

корневым (рис. 16). Его порты находятся в режиме передачи и являются назначенными (рис. 16);

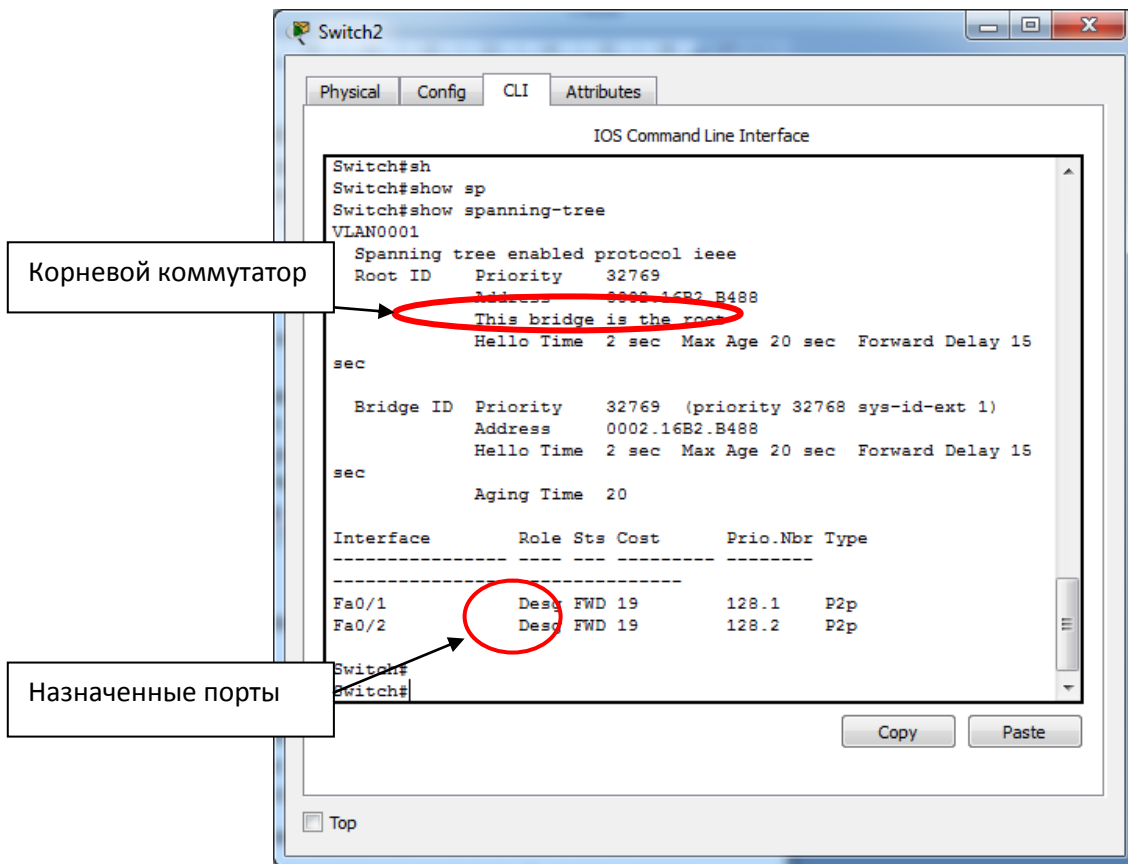


Рис. 16. CLI корневого коммутатора

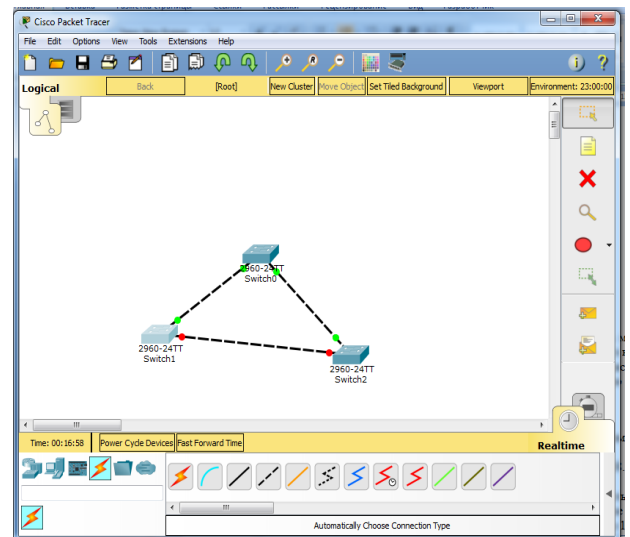
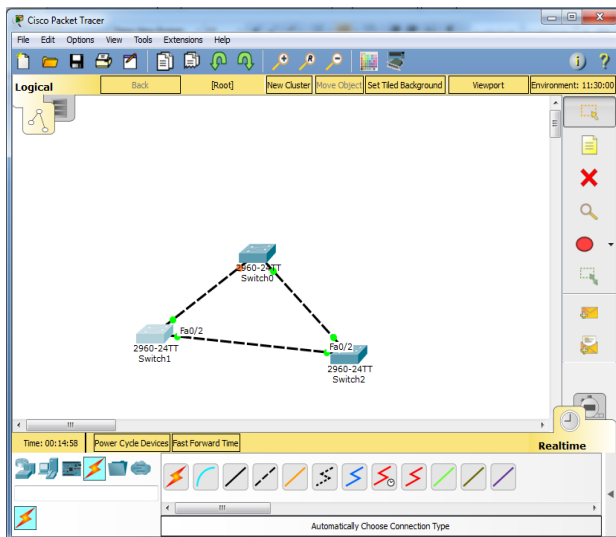


Рис. 17. Spanning Tree Protocol

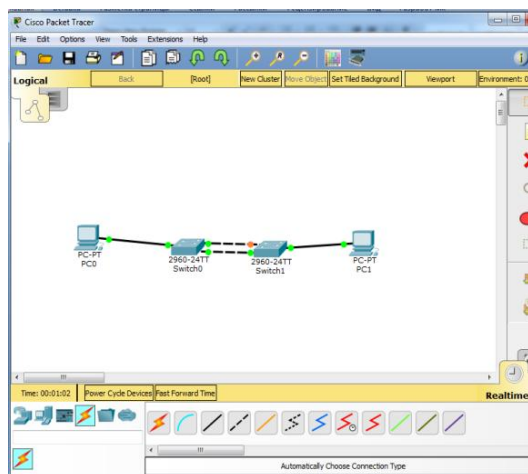
4. Аналогично посмотрим на других коммутаторах. Один порт является корневым, второй – назначенным. Также смотрим для оставшегося

коммутатора. Один порт является резервным в случае падения связи (рис. 17, а).

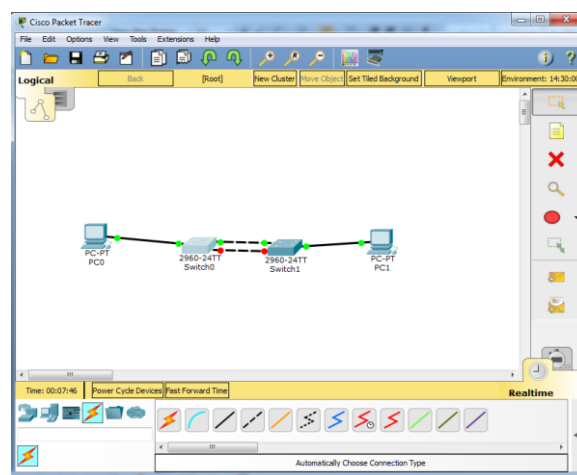
5. Проверим, что протокол STP работает. Погасим связь между корневым и некорневым коммутаторами. Заходим в режим глобального конфигурирования, режим интерфейса порта (в нашем случае fastEthernet 0/2 (рис. 17, а)) и выключим порт shutdown. После переинициализации портов можно увидеть, что у нас включилось резервное соединение (рис. 17, б).

Рассмотрим другой пример.

1. Добавим два коммутатора и два компьютера. Соединим их. Образовалась коммутационная петля (рис. 18).



а) Коммутационная петля



б) Резервное соединение

Рис. 18. STP и RSTP

2. Добавим IP адреса для компьютеров (например, 192.168.1.1 и 192.168.1.2). Проверим, есть ли связь с помощью Command Port. В нашем случае корневой коммутатор Switch0;

3. Проверим, как отразится на пользователе время работы STP (т.е. время сходимости). Для этого потушим порт (в нашем случае fa/Ethernet 0/2 на коммутаторе 0). Связь нарушена, на ее восстановление ушло 15-20 секунд (рис. 18б);

Сократим время переключения. Попробуем настроить протокол RSTP.

4. Заходим в режим глобального конфигурирования коммутатора (в нашем случае Switch0). С помощью команды `Spanning tree mod rapid-pvst` настраиваем RSTP. Аналогично настройте другой коммутатор;
5. Восстановим обратно порт fa/Ethernet 0/2 на коммутаторе Switch0 с помощью команды `no shutdown`. Переключение произошло *мгновенно*.
6. Проверьте соединение.

## Лабораторная работа № 6. АГРЕГАЦИЯ КАНАЛОВ ETHERCHANNEL

**Цель работы:** создать высокопроизводительную сеть путём агрегирования каналов

Варианты агрегирования каналов:

1. Динамическое агрегирование;
2. Статическое агрегирование.

Порты должны иметь одинаковые:

- Скорость;
- Режим дуплекса;
- Native VLAN;
- Диапазон разрешения VLAN;
- Trunking status;
- Тип интерфейса.

Рассмотрим агрегирование каналов:

### Пример статического агрегирования

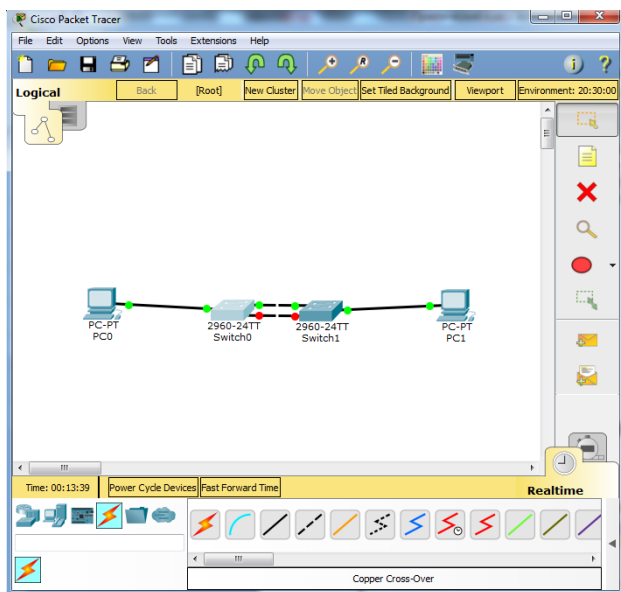
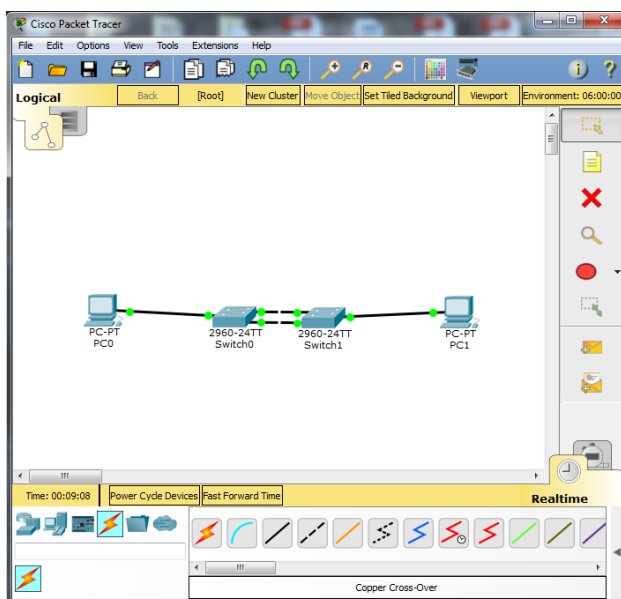
1. Запускаем Cisco Packet Tracer;
2. Добавляем 2 коммутатора 2960 и два компьютера, соединяем их.

Перед соединением коммутаторов настроим порты 0/1 и 0/2, именно их мы будем объединять в агрегированный канал. Заходим в привилегированный режим, режим глобального конфигурирования. Т.к. оба интерфейса будут содержать одинаковые настройки, то отредактируем оба интерфейса с помощью команды `interface range fastEthernet 0/1-2`. Определяем данные интерфейсы в группу 1 с помощью команды `«channel-group 1 mode on»`. Выходим и сохраняем;

3. Аналогично сделайте для второго коммутатора;
4. Теперь соединим эти два коммутатора по средствам fastEthernet 0/1 и fastEthernet 0/2. Обе связи активны (рис. 19, а);
5. Пропишем IP адреса компьютеров (192.168.1.1 и 192.168.1.2);



6. Для проверки отказоустойчивости отключим порт fastEthernet 0/1 у Switch0 и увидим, что будет активен только один канал (рис. 19, б);



а) Пример с агрегированием каналов

б) Проверка отказоустойчивости

Рис. 19. Пример статического агрегирования

### Пример динамического агрегирования

1. Добавим коммутатор 3го уровня 3560 и три коммутатора 2960;
2. Подключим каждый из коммутаторов двумя портами к центральному коммутатору, используя динамическое агрегирование:

2.1. Настроим коммутатор 3560. Режим конфигурирования. Создаем первый агрегированный канал (interface range fastEthernet 0/1-2). Выбираем channel-protocol lACP, присваиваем channel-group 1 mode active, выходим. Создаем второй агрегированный канал (interface range fastEthernet 0/3-4). Указываем протокол и channel-group 2 mode active. И аналогично создайте третий агрегированный канал для fastEthernet 0/5-6;

2.2. Переходим к настройкам коммутаторов доступа в режиме глобального конфигурирования с помощью команд interface range fastEthernet 0/1-2, channel-protocol lACP и channel-group 1 mode passive;

2.3. Аналогично производим на остальных двух коммутаторах;

2.4. Теперь соединим коммутаторы. Результат приведен на рис. 20.

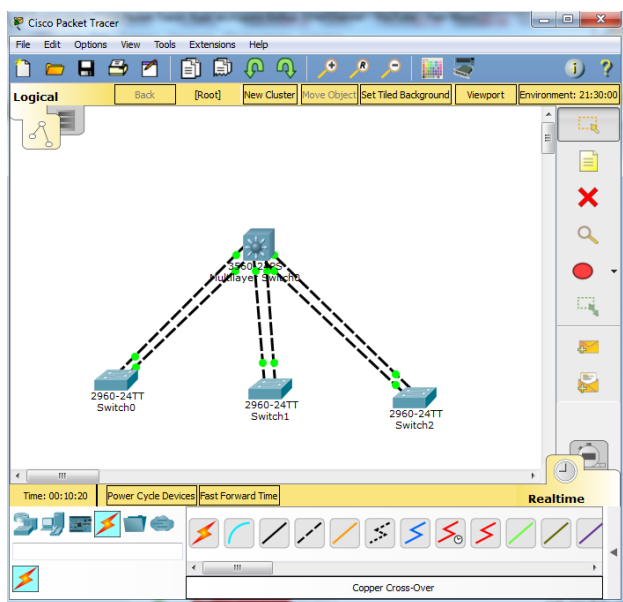


Рис. 20. Пример динамического агрегирования

## Лабораторная работа № 7. ИСПОЛЬЗОВАНИЕ КОММУТАТОРОВ ТРЕТЬЕГО УРОВНЯ

**Цель работы:** Создать локальную сеть, состоящую из нескольких подсетей на основе коммутатора 3 уровня

Коммутаторы третьего уровня модели OSI (L3):

- IP маршрутизация;
- Агрегирование коммутаторов уровня доступа;
- Используются в качестве коммутаторов уровня распределения;
- Высокая производительность.

Рассмотрим два примера (рис. 21).

Для начала рассмотрим пример (рис. 21, а), который включает в себя три компьютера и коммутатор L3:

1. Запускаем Cisco Packet Tracer;
2. Добавляем три компьютера и коммутатор 3560;
3. Переходим к настройке коммутатора. Привилегированный режим, режим глобального конфигурирования. Создадим три сегмента, т.е. три VLAN. С помощью команды `vlan 2, name vlan 2`, аналогично для `vlan 3` и `4`;
4. Необходимо определить порты, в которые подключаются пользователи в определенный VLAN:
  - 4.1. Режим глобального конфигурирования, режим конфигурирования интерфейса `interface fastEthernet 0/1, switchport mode access, switchport access vlan 2`.
  - 4.2. Тоже самое сделайте для оставшихся интерфейсов;
5. Проверим с помощью `show run`;
6. Т.к. это L3 коммутатор, то нам необходимы IP адреса на созданные нами сегменты:

6.1. В режиме глобального конфигурирования заходим в режим конфигурирования интерфейса vlan 2 с помощью команды `interface vlan 2` и с помощью команды `ip address 2.2.2.1 255.255.255.0` присвоим IP адрес.

6.2. Аналогично сделайте для остальных виртуальных интерфейсов vlan 3 и 4 (для vlan 3 IP 3.3.3.1 255.255.255.0, для vlan 4 IP 4.4.4.1 255.255.255.0);

7. Проверим настройки.

8. Перейдем к настройке компьютеров. Назначим IP адреса. PC0 находится во втором VLAN, зададим ему IP из той же сети. В нашем случае IP 2.2.2.2, 255.255.255.0 и шлюз зададим IP адрес L3 коммутатора на VLAN 2.

9. В настройках коммутатора необходимо указать, что он должен маршрутизировать трафик. Заходим в режим глобального конфигурирования. Команда `ip routing`. Сохраним конфигурацию (`wr mem`);

10. Аналогичные действия для других компьютеров.

11. Проверьте с помощью Command Prompt;

12. Проверьте межсетевое взаимодействие.

Рассмотрим пример (рис. 21, б), который включает в себя три компьютера и коммутатор L3:

1. Добавим коммутатор 3560, два коммутатора 2960 и четыре компьютера;

2. Пусть PC3 и PC5 находятся во втором VLAN, а PC4 и PC6 - в другом VLAN. Для удобства можно обозначить (рис. 21, б);

3. Настроим коммутаторы уровня доступа. Порт `fastEthernet 0/1` определим во второй VLAN, а порт `fastEthernet 0/2` определим в VLAN 3.

4. Теперь необходимо настроить trunk порт для центрального коммутатора:

4.1. Настроим порт `gigabitEthernet 0/1` с помощью команд `interface gigabitEthernet 0/1`, `switchport mode trunk`, `switchport trunk allowed vlan 2,3`.

Выходим и сохраняем.

5. Аналогичные действия выполняем для второго коммутатора уровня доступа;

6. Теперь настроим L3 коммутатор:

6.1. Коммутатор Switch0 подключается к коммутатору 3560 через порт gigabitEthernet 0/1, а Switch1 через порт gigabitEthernet 0/2. interface gigabitEthernet 0/1, switchport mode trunk encapsulation dot1q, switchport mode trunk, switchport trunk allowed vlan 2,3;

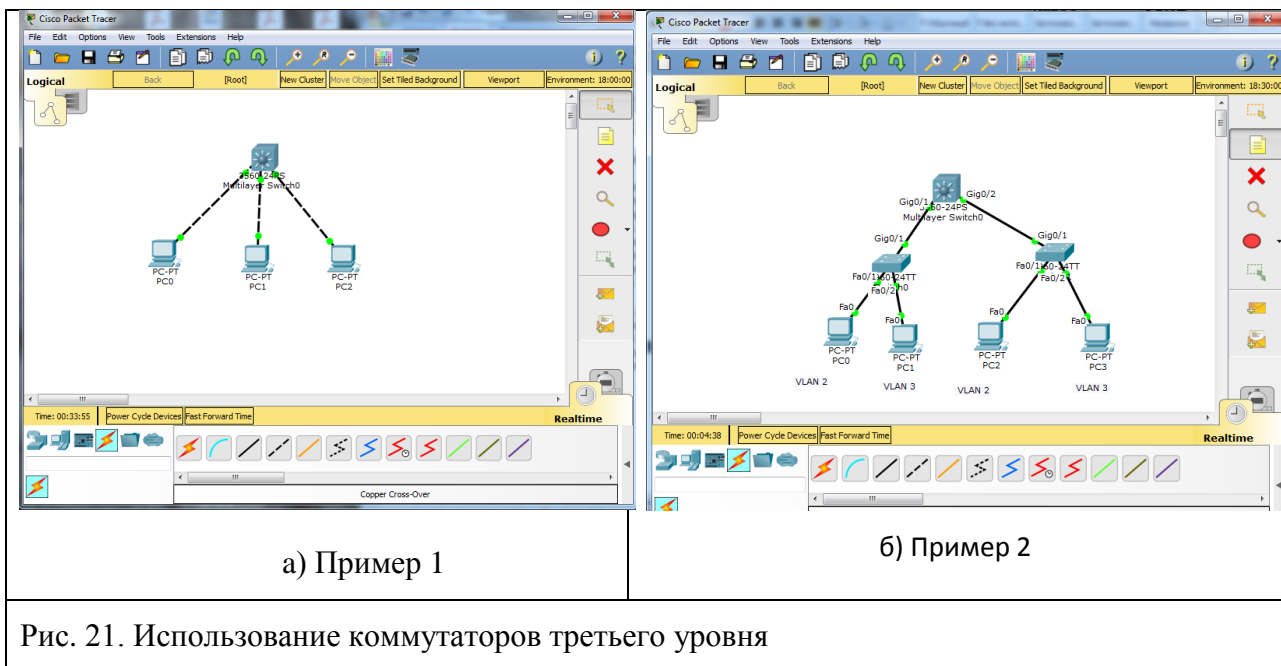
6.2. Аналогичные действия выполняем для интерфейса gigabitEthernet 0/2;

6.3. На созданные виртуальные интерфейсы присвоим IP адреса. Для это воспользуемся командами interface vlan 2, ip address 2.2.2.1 255.255.255.0. Аналогично для vlan 3 (IP адрес 3.3.3.1). Включаем «ip routing. Сохраняем;

6.4. Создаем VLAN 2 и 3 (Например, для VLAN vlan 2, name vlan 2).

7. Настроим компьютеры. Для PC3 IP адрес 2.2.2.2 и маска 255.255.255.0, шлюзом указываем IP адрес, который на vlan 2 в коммутаторе. Аналогично настраиваем оставшиеся компьютеры. Проверьте доступность.

8. Проверьте взаимодействие между сетями.



## Лабораторная работа № 8. МАРШРУТИЗАТОР

**Цель работы:** построить маршрутизируемую IP-сеть

Маршрутизатор (Router):

- IP маршрутизация;
- NAT;
- VPN;
- Межсетевой экран.

Рассмотрим два примера (рис. 22).

Для начала рассмотрим случай (рис. 22, а):

1. Запускаем Cisco Packet Tracer;
2. Создадим три компьютера, один коммутатор 2960 и маршрутизатор (рис. 22, а). Пусть будет три сегмента VLAN2, VLAN3 и VLAN4.

3. Настроим коммутатор в режиме глобального конфигурирования.

- 3.1. Создадим VLAN2, VLAN3 и VLAN4 и назначим им имена;

- 3.2. Определяем компьютеры в соответствующий интерфейс.

Компьютер PC0 подключен к интерфейсу fastEthernet 0/1, PC1 к fastEthernet 0/2, PC1 к fastEthernet 0/3. Настройте интерфейсы с помощью команд interface fastEthernet 0/1, switchport mode access, switchport access vlan 2. Аналогично для оставшихся VLAN3 и VLAN4;

- 3.3. Настройте trunk порт, который идет до маршрутизатора (в нашем случае порт коммутатора fastEthernet 0/4).

4. Настроим маршрутизатор:

- 4.1. Заходим в CLI;

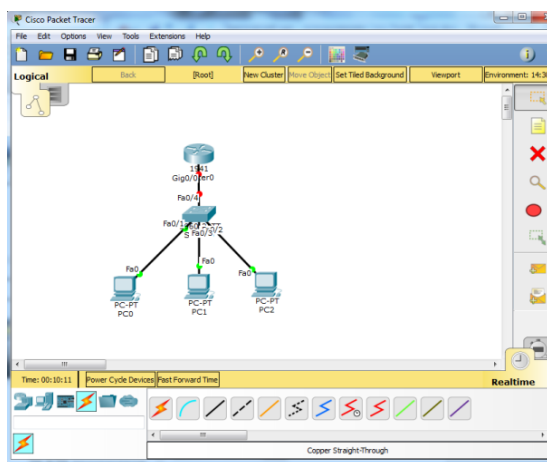
- 4.2. Режим глобального конфигурирования;

- 4.3. Необходимо поднять физический порт (в нашем случае gigabitEthernet 0/0) с помощью команд interface gigabitEthernet 0/0, no shutdown.

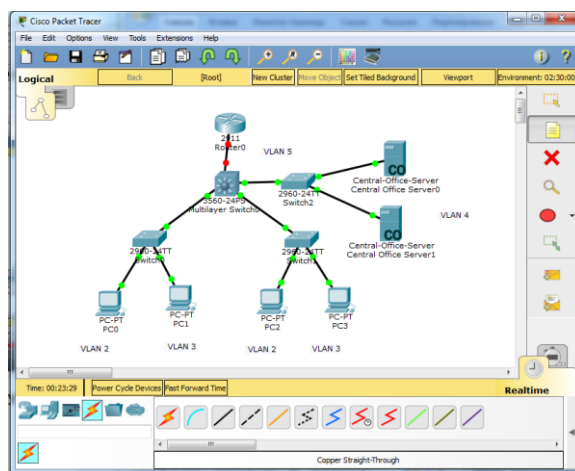
5. Т.к. на маршрутизатор приходит три VLAN, необходимо создать подинтерфейсы, которым будут соответствовать свой VLAN с помощью команд `interface gigabitEthernet 0/0.2`, `encapsulation dot1Q 2`, и зададим IP адрес `192.168.2.1 255.255.255.0`, но `shutdown`. Аналогично сделайте для VLAN 3 и 4. Сохраните.

6. Настройте компьютеры. Например, в нашем случае для PC0 IP адрес `192.168.2.2`, маска `255.255.255.0` и шлюз `192.168.2.1`. Аналогично для остальных компьютеров.

7. Проверьте соединение.



а) Пример 1



б) Пример 2

Рис. 22. Маршрутизатор

Рассмотрим пример (рис. 22, б):

1. Добавим 4 компьютера, 3 коммутатора 2960, один коммутатор третьего уровня, один маршрутизатор и 2 сервера;
2. Наши компьютеры PC0 и PC2 находятся в VLAN 2, PC1 и PC3 в VLAN 3, сервера находятся в своем выделенном VLAN 4;
3. Настройте коммутаторы Switch0, Switch1 и Switch3.
4. Для компьютеров присвойте IP адреса: PC0 – `192.168.22.2`, PC2 – `192.168.22.3`, PC1 – `192.168.33.2`, PC3 – `192.168.33.3`, для серверов `192.168.44.2` и `192.168.44.3`;
5. Настройте коммутатор L3;
6. Создайте VLAN 5;

7. Настройте коммутатор L3 для данного сегмента. Поднимите виртуальный интерфейс с помощью команд `ip address 192.168.55.2 255.255.255.0, no shutdown`;
8. Порт `gigabitEthernet 0/1` определите как access порт;
9. Настроим маршрутизатор:
  - 9.1. Режим глобального конфигурирования.
  - 9.2. Поднимите физический интерфейс (в нашем случае `gigabitEthernet 0/0`). И задаем IP адрес `ip address 192.168.55.1 255.255.255.0`;
10. Проверьте сеть.



## Лабораторная работа № 9. СТАТИЧЕСКАЯ МАРШРУТИЗАЦИЯ

**Цель работы:** настроить маршрутизацию в составной сети небольшого размера

1. Рассмотрим пример из лабораторной работы № 8. И настроим связь между двумя офисами (рис. 22, *а* (филиал 1)); (рис. 22, *б* (филиал 2));
2. В филиале 1 у нас есть VLAN 2,3 и 4, которые маршрутизируются на маршрутизаторе;
3. В филиале 2 у нас VLAN 2,3 для пользователей, VLAN 4 для серверов;
4. Настройки были произведены в прошлой лабораторной работе;
5. Проверим связь между маршрутизатором и конечными пользователями с помощью команд `ip address 192.168.22.0 255.255.255.0 192.168.55.2`, `ip address 192.168.33.0 255.255.255.0 192.168.55.2`, `ip address 192.168.44.0 255.255.255.0 192.168.55.2` в режиме глобальной конфигурации. Проверьте `ping` (например, `ping 192.168.22.2`);
6. Соединим два маршрутизатора.
  - 6.1. В нашем случае для маршрутизатора (рис. 22, *б*) необходимо настроить интерфейс `gigabitEthernet 0/1` с помощью команд `interface gigabitEthernet 0/1`, `no shutdown`. Присвоим IP адрес `ip address 192.168.70.1 255.255.255.252`. Выходим и сохраняем;
  - 6.2. Для маршрутизатора (рис. 22, *а*) необходимо настроить интерфейс `fastEthernet 0/1` с IP адресом `192.168.70.2`;
  - 6.3. Проверьте связь.
7. Создадим необходимые маршруты.
  - 7.1. Для роутера на рис. 22, *а* прописываем в режиме глобального конфигурирования `ip route 0.0.0.0 0.0.0.0 192.168.70.1`. Выходим и сохраняем;
  - 7.2. Можно посмотреть таблицы маршрутизации с помощью команды `show ip route`;

8. Пропишем маршруты для L3 с помощью команд `ip route 0.0.0.0 0.0.0.0 192.168.55.1`;

9. Пропишем маршруты на роутер (рис. 22, б) с помощью команд `ip route 192.168.2.0 255.255.255.0 192.168.70.2`, `ip route 192.168.3.0 255.255.255.0 192.168.70.2` и `ip route 192.168.4.0 255.255.255.0 192.168.70.2`. Сохраните;

10. Проверьте связь.

Теперь рассмотрим схему на рис. 23:

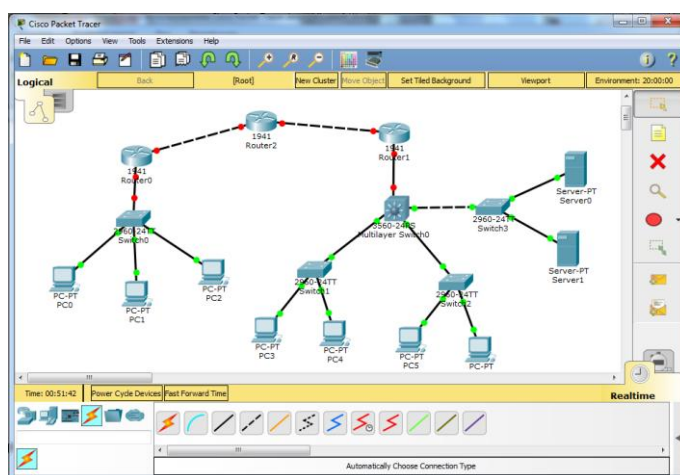


Рис. 23. Пример статической маршрутизации

1. Создадим связь между роутерами.

2. Настроим интерфейс портов `fastEthernet 0/0` и `fastEthernet 0/1` маршрутизатора, с которым связаны маршрутизаторы с филиалов 1 и 2:

2.1. Режим глобального конфигурирования. Interface `fastEthernet 0/0`, `no shutdown`, `ip address 192.168.70.1 255.255.255.0`. Аналогично настройте интерфейс для `fastEthernet 0/1` с IP адресом `192.168.80.1`. Выходим и сохраняем.

3. Проверьте настройки для роутера с филиала 1. В нашем случае необходимо поправить маску с помощью команды `ip address 192.16.70.2 255.255.255.0`. Сохраните.

4. Изменим настройки на роутере с филиала 2. Необходимо изменить IP адрес на `gigabitEthernet 0/1` с помощью команд `gigabitEthernet`

0/1, ip address 192.168.80.2 255.255.255.0, no shutdown. Изменим маршруты с помощью команд no ip route 192.168.2.0 255.255.255.0 192.168.70.2, no ip route 192.168.3.0 255.255.255.0 192.168.70.2, no ip route 192.168.4.0 255.255.255.0 192.168.70.2. Маршруты во внутреннюю сеть оставляем прежними. Теперь пишем новый маршрут ip route 0.0.0.0 0.0.0.0 192.168.80.1. Сохраняем.

5. Создадим маршруты на роутере 2:

5.1. Маршруты для сети с филиалом 1 с помощью команд ip route 192.168.2.0 255.255.255.2 192.168.70.2, ip route 192.168.3.0 255.255.255.2 192.168.70.2, ip route 192.168.4.0 255.255.255.2 192.168.70.2;

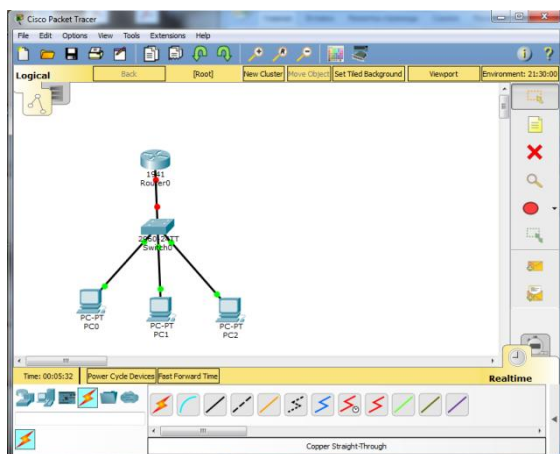
5.2. Маршруты для сети с филиалом 2 с помощью команд ip route 192.168.22.0 255.255.255.2 192.168.80.2, ip route 192.168.33.0 255.255.255.2 192.168.80.2, ip route 192.168.44.0 255.255.255.2 192.168.80.2. Сохраните

6. Проверьте связь.

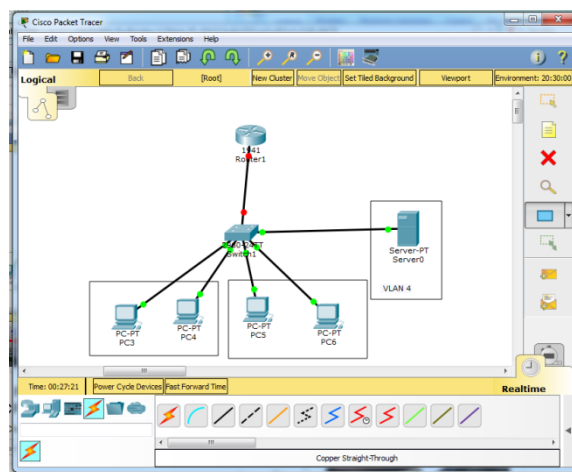
## Лабораторная работа № 10. DHCP ПРОТОКОЛ

**Цель работы:** обеспечить корректное автоматическое присвоение IP-адресов узлам сети

Рассмотрим два примера (рис. 24)



а) Пример 1



б) Пример 2

Рис. 24. Использование DHCP протокола

Рассмотрим пример (рис. 24, а):

1. Запускаем Cisco Packet Tracer;
2. Настроим маршрутизатор:
  - 2.1. Подключение осуществляется к порту fastEthernet 0/1. Настройте интерфейс и присвойте IP адрес 192.168.1.1 255.255.255.0;
  - 2.2. Создадим пространство IP адресов с помощью команд `ip dhcp pool DHCP, network 192.168.1.0 255.255.255.0;`
  - 2.3. Выдаем компьютеру IP адрес и маршрут default-router 192.168.1.1, `dns -server 0.0.0.0;`
  - 2.4. Исклучим некоторые IP адреса и DHCP протокола (например, при подключении к сети сервера) с помощью команд `ip dhcp excluded-addresses 192.168.1.99` и исключим IP адрес роутера `ip dhcp excluded-addresses 192.168.1.1;`
3. Настроим компьютеры. Ставим галочку на DHCP вместо Static. IP адрес присвоится автоматически.

#### 4. Проверьте сеть.

Рассмотрим пример (рис. 24, б):

1. Настроим коммутатор.
  - 1.1. Создайте VLAN 2,3 и 4;
  - 1.2. Настройте порты, к которым подключены компьютеры;
  - 1.3. Настройте порт, к которому подключен сервер;
  - 1.4. Соединим все VLAN с маршрутизатором с помощью команд (в нашем случае порт fastEthernet 0/1) `interface fastEthernet 0/1, switchport mode trunk, switchport trunk allowed vlan 2, 3, 4`. Сохраните.
2. Настроим маршрутизатор:
  - 2.1. Настройте порт и задайте IP адрес (например, с VLAN 2 IP адрес 192.168.2.1, с VLAN 3 IP адрес 192.168.3.1, с VLAN 4 IP адрес 192.168.4.1);
  - 2.2. Проверьте.
3. Настроим DHCP сервер:
  - 3.1. Зададим статический IP адрес 192.168.4.2 и шлюз 192.168.4.1;
  - 3.2. Проверьте взаимодействие с маршрутизатором;
  - 3.3. Перейдите во вкладку Config/DHCP. Создадим сервер с именем DHCPvlan2, IP адрес 192.168.2.0. Шлюз 192.168.2.1 и DNS Server 0.0.0.0. Включаем его (On) и добавляем (Add); Аналогично создайте для VLAN 3.
4. Переадресуем запросы с компьютеров на DHCP сервер:
  - 4.1. Заходим в настройки маршрутизатора. С помощью команд `interface gigabitEthernet 0/0.2, ip helper-address 192.168.1.2`. Аналогично выполните для VLAN 3. Сохраните.
5. Попробуйте получить IP адреса компьютеров (IP Configuration).
6. Проверьте взаимодействие.

## Лабораторная работа № 11. NETWORK ADDRESS TRANCLATION (NAT)

**Цель работы:** Настроить адресацию локальной сети на основе частных IP-адресов

Рассмотрим пример на рис. 25.

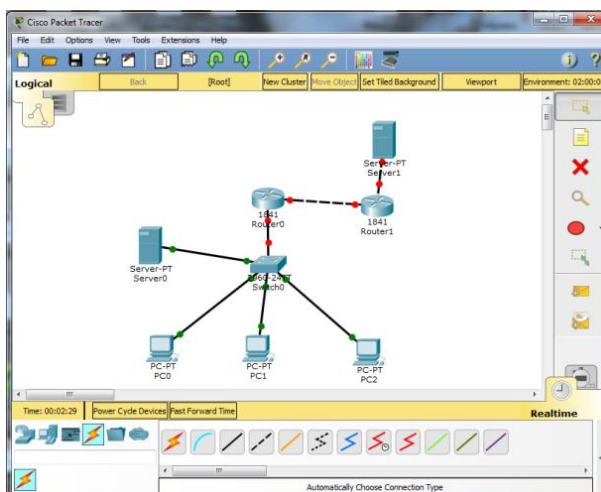


Рис. 25. Network Address Translation

1. Запускаем Cisco Packet Tracer;
2. Рассмотрим пример небольшого офиса, который состоит из трех компьютеров, одного локального сервера.
3. Настройте компьютеры (например, с IP адресами 192.168.2.2, 192.168.2.3, 192.168.2.4), у сервера IP адрес 192.168.3.2;
4. Создайте сегменты посредством VLAN на коммутаторе (VLAN 2, 3);
5. Настройте порты на коммутаторе. Например, порт с сервером fastEthernet 0/4 будет на VLAN 3, а порты fastEthernet 0/1, 0/2 и 0/3 на VLAN 3, а порт fastEthernet 0/5 будет trunk;
6. Проверьте;
7. Настройте роутер. В нашем случае роутер подключается к интерфейсу fastEthernet 0/0. Создайте sub-интерфейсы;
8. Локальная сеть настроена. Проверьте соединение;
9. Подключим локальную сеть к сети интернет:

9.1. Настройте роутер Router1 (в нашем случае подключен к интерфейсу fastEthernet 0/0). IP адрес из белого диапазона 213.234.10.1 с маской 255.255.255.252;

9.2. За роутером провайдера находится сервер Server1 (интерфейс fastEthernet 0/1), который имеет белый IP адрес 213.234.20.1 с маской 255.255.255.252;

9.3. Настройте сервер. IP адрес 213.234.20.2 с маской 255.255.255.252, шлюзом укажем IP адрес 213.234.20.1;

9.4. На Router0 в нашем случае на интерфейсе fastEthernet 0/1 создайте IP адрес 213.234.10.2 с маской 255.255.255.252 и необходимо создать ip route 0.0.0.0 0.0.0.0 213.234.10.1. Сохраните.

10. Настроим доступ пользователей PC0, PC1 и PC 2 в сеть интернет (в нашем случае к Server1) с помощью NAT. Настроим Router0:

10.1. В нашем случае интерфейс fastEthernet 0/1 внешний (команда ip nat outside), а интерфейс fastEthernet 0/0.2 внутренний (команда ip nat inside);

10.2. Аналогично необходимо сделать на интерфейсе Server0, если необходим доступ к сети интернет.

10.3. Необходимо создать access листы с помощью команды ip access-list standard FOR-NAT, permit 192.168.2.0 0.0.0.255, permit 192.168.3.0 0.0.0.255. Проверьте;

10.4. Настроим NAT с помощью команды ip nat inside source list FOR-NAT interface fastEthernet 0/1 over;

11. Проверьте связь компьютера и сервера Server0 на сервер Server1 с белым IP адресом;

12. Настроим доступ к локальному серверу из внешней сети:

12.1. Перейдем в настройки Server0. Вкладка Config/HTTP доступ к сайту, например NetSkill;

12.2. Настроим Static NAT на Route0 с помощью команды ip nat inside source static tcp 192.168.3.2 80 213.234.10.2 80;

12.3. Попробуйте с помощью Web Brouse Server1 обратиться на IP адрес 213.234.10.2.

## Лабораторная работа № 12. ДИНАМИЧЕСКАЯ МАРШРУТИЗАЦИЯ (ПРОТОКОЛ OSPF)

**Цель работы:** настроить автоматическое построение таблиц маршрутизации в составной сети по протоколу OSPF

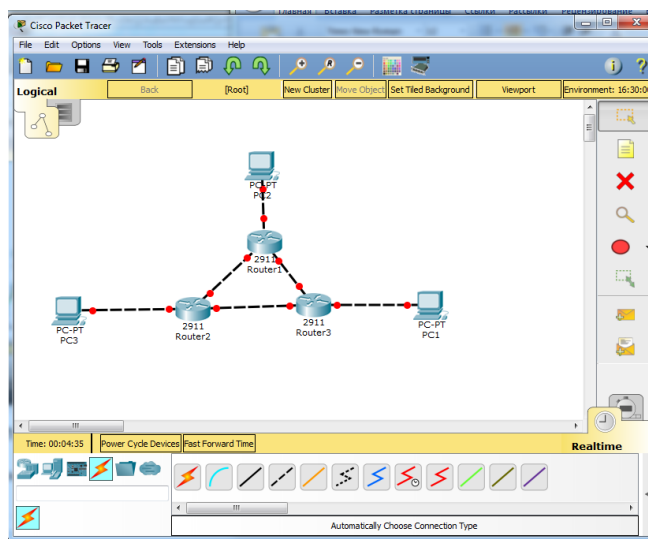


Рис. 26. Пример динамической маршрутизации

Рассмотрим пример динамической маршрутизации на рис. 26. В рассматриваемом примере необходимо установить, чтобы с сетей компьютеров были доступны все IP адреса, не прописывая статически маршруты на роутерах:

1. Запускаем Cisco Packet Tracer;
2. Добавьте три роутера и три сети;
3. Настройте роутеры.
  - 3.1. IP адрес для Router2 192.168.1.1 на интерфейсе gigabitEthernet 0/2, куда подключен PC3 с IP адресом 192.168.1.2. На интерфейсах gigabitEthernet 0/0 – 10.10.10.1/30, gigabitEthernet 0/1 – 10.10.11.1/30, которые связаны с Router1 и 3.
  - 3.2. IP адрес для Router1 192.168.2.1 на интерфейсе gigabitEthernet 0/2. На интерфейсах gigabitEthernet 0/0 – 10.10.10.2/30, gigabitEthernet 0/1 – 10.10.12.1/30, которые связаны с Router2 и 3.



3.3. IP адрес для Router3 192.168.3.1 на интерфейсе gigabitEthernet 0/2. На интерфейсах gigabitEthernet 0/0 – 10.10.12.2/30, gigabitEthernet 0/1 – 10.10.11.2/30, которые связаны с Router1 и 2.

4. Настроим роутер Router2:

4.1. Настроим адрес на логическом интерфейсе loopback с помощью команд `interface loopback 0`, `ip address 192.168.100.1 255.255.255.255`, по `shutdown`;

4.2. Настроим OSPF.

- Заходим в режим конфигурирования роутера `router ospf 1`;
- Укажем все сети, которые подключены к рассматриваемому роутеру (в нашем случае 10.10.10.0/30, 10.10.11.0/30 и 192.168.1.0), с помощью команд `network 192.168.1.0 0.0.0.255 area 0`, `network 10.10.10.0 0.0.0.3 area 0`. Аналогично укажите для оставшейся сети;

5. Аналогично настройте роутер Router1 и Router3;

6. Сеть настроена;

7. Для проверки настроек можно набрать команду `show ip ospf neighbor`;

8. Для проверки маршрутизации с помощью протокола OSPF `show ip route`;

9. Проверьте связь.

10. Проверим реализацию отказоустойчивость системы. Для этого потушите связь на Router2 (в нашем случае интерфейс gigabitEthernet 0/1) и увидите, что 192.168.1.0 доступна через маршрутизатор Router1.

## Лабораторная работа № 13. ДИНАМИЧЕСКАЯ МАРШРУТИЗАЦИЯ (ПРОТОКОЛ EIGRP)

**Цель работы:** настроить автоматическое построение таблиц маршрутизации в составной сети по протоколу EIGRP

Рассмотрим пример из лабораторной работы № 12. Настройки маршрутизаторов и компьютеров аналогичные.

1. Запускаем Cisco Packet Tracer;
2. Настройте Router2 аналогично п.4.1.
  - 2.1. Настройка EIGRP.
    - Заходим в режим конфигурирования роутера `router eigrp 1`;
    - Укажем все сети, которые подключены к рассматриваемому роутеру (в нашем случае `10.10.10.0/30`, `10.10.11.0/30` и `192.168.1.0`), с помощью команд `network 192.168.1.0 0.0.0.255`, `network 10.10.10.0 0.0.0.3`. Аналогично укажите для оставшейся сети;
    - Отключим суммирование маршрутов с помощью команды `no auto-summary`;
3. Аналогично настройте роутер Router1 и Router3;
4. Проверьте настройки;
5. Проверьте таблицы маршрутизации;
6. Проверьте `ping` с компьютера;
7. Проверим реализацию отказоустойчивость системы.
8. Распространим дефолтный маршрут на другие маршрутизаторы, чтобы не прописывать их статически.
  - 8.1. Пусть Router3 имеет дефолтный маршрут `ip route 0.0.0.0 0.0.0.0 192.168.3.2`;
  - 8.2. Зайдем в настройку EIGRP `router eigrp 1` и распространим информацию о дефолтном маршруте с помощью команды `redistribute static`. Сохраните;
  - 8.3. Проверьте, например на Router1, таблицу маршрутизации.

## Лабораторная работа № 14. СПИСКИ ДОСТУПА (ACCESS LIST)

**Цель работы:** настроить безопасную сеть на основе фильтрации IP-пакетов

Рассмотрим пример, который состоит из четырех сегментов (рис. 27): VLAN 2 – технологи, VLAN 3 – менеджеры, VLAN 4 – руководство, VLAN 5 – сегмент сервера. Интернет моделируют маршрутизатор Router1 и сервер Server1.

1. На коммутаторе настройте соответствующие порты в соответствующие VLAN 2-5;

2. Настройте маршрутизатор Router0. Создайте 4 sub интерфейса и физический интерфейс с белым IP адресом для выхода в интернет.

3. Настроим NAT (согласно лабораторной работе № 11) с акцентом на access list:

3.1. Заходим в настройки Router0. Определим интерфейсы, которые будут внутренними и внешними для NAT. (в рассматриваемом примере fa0/0 – внешний, fa0/1.2, fa0/1.3, fa0/1.4 - внутренний). Server0 изолируем от сети интернет;

3.2. Создаем стандартный access list с помощью команды `ip access-list standard FOR-NAT`. Перечисляем сети `permit 192.168.2.0 0.0.0.255`, аналогично для 192.168.3.0 и 192.168.4.0;

3.3. Указываем название access list с помощью команды `ip nat inside list FOR-NAT interface fa0/0 overload`;

3.4. Проверьте доступ компьютеров и Server0 к сети интернет;

4. Для ограничения доступа к внутренней сети воспользуемся расширенными access list на входящий трафик:

4.1. Зайдите в настройки Router0;

4.2. Создадим расширенный access list с помощью `ip access-list extended FROM-OUTSIDE`;

4.3. Запретим трафик во внутреннюю сеть deny ip any 192.168.2.0 0.0.0.255, аналогично для 192.168.3.0, 192.168.4.0 и 192.168.5.0;

4.4. Созданный access list привяжем к внешнему интерфейсу (в нашем случае fa0/0) с помощью команды ip access-group FROM-OUTSIDE in;

5. Проверьте. Как можно заметить пропал доступ компьютеров к сети интернет. Для того чтобы решить данную проблему зайдём в конфигурацию access list и добавим permit ip any host 210.210.0.2. Сохраните и проверьте;

6. Т.к. в конце любого листа доступа присутствует запрещающее правило deny ip any , целесообразнее разрешить единственный access list, а остальное было бы запрещено, что привело бы к сокращению access list. Для этого:

6.1. Удалим access list – no ip access-list extended FROM-OUTSIDE;

6.2. Укажем permit ip any host 210.210.0.2. Проверьте с помощью show run.

7. Проверьте доступ к сети интернет.

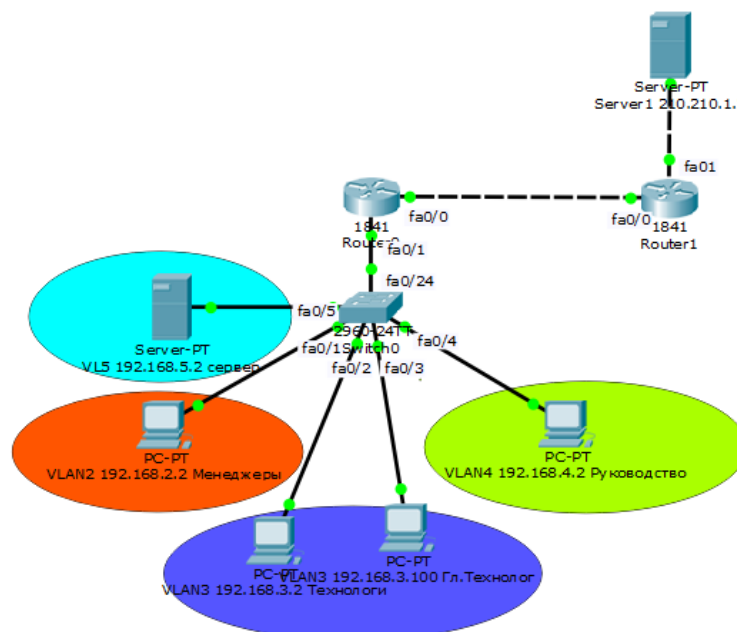


Рис. 27. Списки доступа

8. Создадим на Router0 доступ по TELNET username admin privilege 15 password 1111. Создадим пароль на enable enable password 1111. Включим доступ line vty 0 4, login local. Проверьте удаленный доступ с Server1 на Router0. Доступ есть. Для его запрета необходимо:

8.1. Возвращаемся к access list с помощью команды ip access-list extended FROM-OUTSIDE, добавим запрещающее правило на TELNET deny tcp any host 210.210.0.2 eq telnet;

8.2. Запрещающее правило должно быть выше разрешающего. Для этого удалим access list no ip access-list extended FROM-OUTSIDE и создадим заново ip access-list extended FROM-OUTSIDE, deny tcp any host 210.210.0.2 eq telnet, permit ip any host 210.210.0.2;

8.3. Проверьте access list и удаленный доступ с Server1.

9. Применение стандартных access list на исходящий трафик на примере Server0 с доступом только для менеджеров:

9.1. Настройка Router0. Создайте стандартный access list с именем TO-MENEGERS. Разрешим только одну сеть 192.168.2.0;

9.2. Привяжите access list к соответствующему интерфейсу fa0/1.5 ip access-group TO-MENEGERS out. Проверьте.

## Лабораторная работа № 15. CISCO ADAPTIVE SECURITY APPLIANCE

**Цель работы:** Настроить безопасную сеть при помощи специализированного устройства Cisco ASA

В данной лабораторной работе на примере рис. 28 необходимо сделать следующее:

- Подключение к Cisco Adaptive Security Appliance;
- Проверка лицензии;
- Настройка удаленного доступа к МЭ;
- Настройка Security Level;
- Настройка маршрута по умолчанию;
- Настройка инспектирования трафика;
- Настройка NAT.

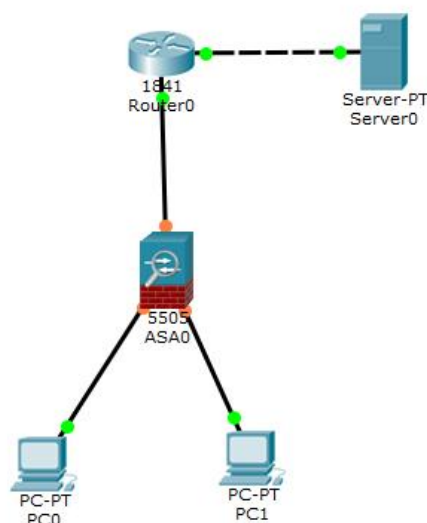


Рис. 28. Пример Cisco Adaptive Security Appliance

1. Запускаем Cisco Packet Tracer 6.2;
2. Добавьте элементы согласно рис. 28;
3. Заходим в настройки ASA0. Заходим в привилегированный режим, show version. Можно увидеть, что установлена базовая лицензия.
4. Соедините оборудование (рис. 28);

5. Посмотрим, что предустановленно на ASA0 с помощью «show run», в нашем случае по умолчанию Ethernet0/0 настроен на VLAN 2, остальные в VLAN 1. По умолчанию настроен DHCP сервер, следовательно, PC0 и PC1 должны получить IP адреса. Проверьте.

6. **Настройка удаленного доступа к МЭ.** Пусть на PC0 администратор хочет удаленно администрировать Cisco ASA:

- Заходим в настройки ASA0. Режим глобального конфигурирования. Задаем пароль enable password 1111, создадим пользователя username admin password 1111.
- Выберем протокол, по которому хотим осуществлять удаленное подключение ssh 192.168.1.0 255.255.255.0 inside;
- Зададим параметры authentication ssh console LOCAL;
- Проверьте доступ с компьютера.

#### 7. **Настроим Security Level:**

7.1. Заходим в ASA0. Конфигурацию интерфейса и изменим интерфейс Security Level с помощью команды int vlan 1, security-level 95;

7.2. Донастроим внешний интерфейс с помощью команд interface vlan 2, ip address 210.210.0.2 255.255.255.255, no shutdown;

7.3. Проверьте;

7.4. На Router0 настроим интерфейс fa0/0 int fa0/0, ip address 210.210.0.1 255.255.255.255, no shutdown;

7.5. На Router0 настроим интерфейс fa0/1 int fa0/1, ip address 210.210.1.1 255.255.255.255, no shutdown;

7.6. Настройте сервер Server0 (210.210.1.2, шлюз 210.210.1.1);

7.7. Проверьте с ASA0 пингуется ли интернет провайдер.

#### 8. **Настройка маршрута**

8.1. Пропишем маршрут на ASA0 с помощью route outside 0.0.0.0 0.0.0.0 210.210.0.1. Проверьте;

8.2. Пропишем маршрут на ASA0 для локальной сети с помощью `ip route 192.168.1.0 255.255.255.0 210.210.0.2`;

## **9. Настройка инспектирования трафика**

9.1. Настройки ASA0. Режим глобального конфигурирования;

9.2. Определим `class map` с помощью команды `class-map inspection_default, match default-inspection-traffic`;

9.3. Определяем действия над трафиком с помощью команд (в нашем случае инспектирование) `policy-map global_policy, class inspection_default, inspect icmp, inspect http`;

9.4. Определяем направление действия с помощью команды `service-policy global_policy global`. Сохраните;

9.5. Проверьте связь.

## **10. Настройка NAT**

10.1. Заходим в настройки Router0, удалим созданный маршрут в локальную сеть по `ip route 192.168.1.0 255.255.255.0 210.210.0.2`;

10.2. Настроим NAT в ASA0:

- `object network FOR-NAT`, определим сеть `subnet 192.168.1.0 255.255.255.0, nat (inside, outside) dynamic interface`. Сохраните;
- Проверьте пинг.



## Лабораторная работа № 16. DEMILITARIZED ZONE (DMZ)

**Цель работы:** Обеспечить безопасный доступ из внешнего мира к ресурсам локальной сети

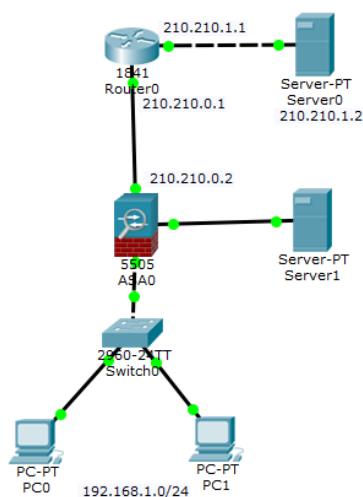


Рис. 29. Пример DMZ

Рассмотрим пример из лабораторной работы № 15.

1. Запускаем Cisco Packet Tracer;
2. Добавьте коммутатор между PC0 и PC1 (рис. 29);
3. Настройте внутреннюю и внешнюю сеть, Router0, Server0;
4. Настройте пароль ASA0, 2 интерфейса VLAN1 и 2, настройте маршрутизацию, NAT и настройте инспектирование трафика (согласно лабораторной работе № 15);
5. Настроим DMZ:
  - 5.1. Добавьте Server1 (рис. 29), на который установите белый IP адрес 210.210.3.2 255.255.255.252 и шлюз 210.210.3.1;
  - 5.2. Пропишем маршрут в Router0 на Server1 через внешний интерфейс ASA `ip route 210.210.3.0 255.255.255.252 210.210.0.2`;
  - 5.3. Настроим ASA0:
    - Создадим сегмент DMZ `int eth0/2, switchport access vlan 3, int vlan 3, no forward interface vlan 1, nameif dmz, security-level 50, ip address 210.210.3.1 255.255.255.252, no shutdown`.

- Пропингуйте Server1;
- 6. Создадим access list, чтобы разрешить трафик до DMZ:
  - Настройка ASA0;
  - Создайте расширенный access list с именем FROM-OUTSIDE  
access-list FROM-OUTSIDE extended permit icmp any host  
210.210.3.2 и разрешим web трафик access-list FROM-OUTSIDE  
extended permit tcp any host 210.210.3.2 eq www;
  - Создадим access группы access-group FROM-OUTSIDE in interface  
outside;
  - Проверьте.

## Лабораторная работа № 17. VIRTUAL PRIVATE NETWORK (VPN)

**Цель работы:** Обеспечить безопасное соединение двух локальных сетей по каналу, проходящему через Internet

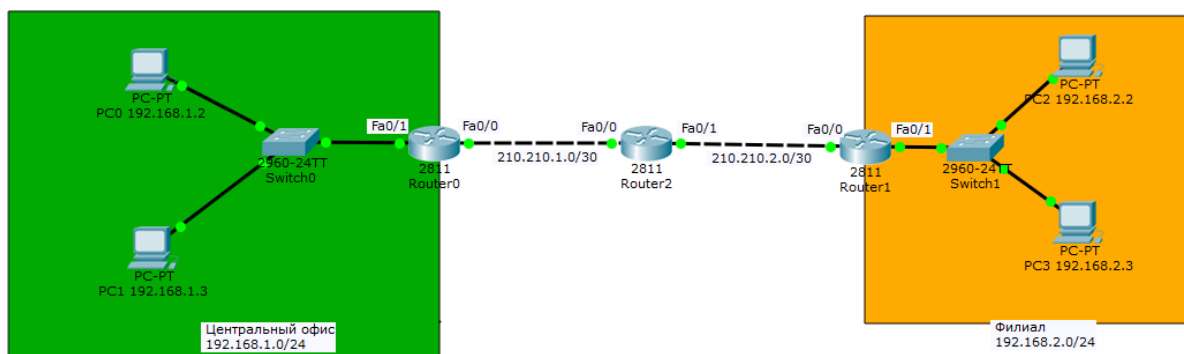


Рис. 30. Организация Virtual Private Network (VPN)

Рассмотрим пример на рис. 30. Настроим связь через VPN от центрального офиса до филиала и наоборот:

1. Запускаем Cisco Packet Tracer;
2. На Router0 настройте 2 IP адреса и дефолтный маршрут;
  - 2.1. Настройте NAT (fa0/0 - внешний, fa0/1 - внутренний);
  - 2.2. Создайте access list с помощью команд: `ip access-list extended FOR-NAT`, `deny ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255`, `permit ip 192.168.1.0 0.0.0.255 any`;
  - 2.3. `ip nat inside list FOR-NAT interface fa0/0 overload`;
  - 2.4. Сохраните и проверьте пинг с компьютера до интернет провайдера;
3. Аналогично настройте на Router1;
4. Настроим VPN:
  - 4.1. Настройки Router0;
  - 4.2. Настроим с помощью команд `crypto isakmp policy 1`, `encryption 3des`, `hash md5`, `authentication pre-share`, `group 2`;
  - 4.3. Настроим ключ аутентификации и пира с помощью команд `crypto isakmp key cisco address 210.210.2.2`;

4.4. На втором этапе настроим с помощью команд `crypto ipsec transform-set TS esp-3des esp-md5-hmac`;

4.5. Создадим access list `ip access-list standard FOR-VPN, permit 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255`;

4.6. Создадим криптокарту с помощью команд `crypto map CMAP 10 ipsec-isakmp, set peer 210.210.2.2, set transform-set TS, match address FOR-VPN`;

4.7. Привяжем криптокарту к внешнему интерфейсу с помощью `interface fa0/0, crypto map CMAP`;

4.8. Аналогично настройте VPN для Router1 с изменением IP адресов;

4.9. Проверьте работоспособность сети

## Лабораторная работа № 18. ПРОТОКОЛ SYSLOG И NTP

**Цель работы:** Обеспечить журналирование работы активных сетевых устройств

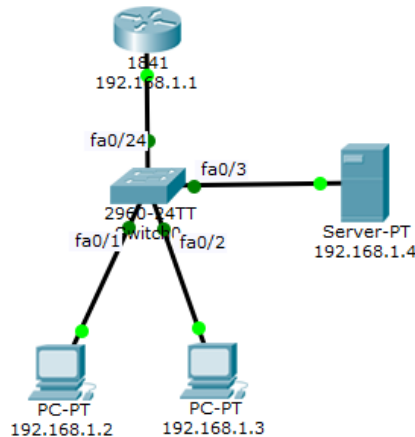


Рис. 31. Пример применения протоколов Syslog и NTP

Рассмотрим пример на рис. 31:

1. Запускаем Cisco Packet Tracer;
2. Добавьте два компьютера, коммутатор, сервер, который будем использовать в качестве Syslog сервера, и роутер (рис. 31);
3. Пропишите IP адреса для компьютеров, сервера и роутера;
4. Настроим Switch0:
  - 4.1. Соберем логи в буфер маршрутизатора с помощью команд `logging on`, `logging buffered 4096`;
  - 4.2. Syslog:
    - Настроим уровень логирования с помощью команд `logging trap debugging`;
    - Укажем IP адрес Syslog сервера `logging 192.168.1.4`;
    - Укажем IP адрес на коммутаторе `int vlan 1`, `ip address 192.168.1.5`, `255.255.255.0`, `no shutdown`;

- Проверьте. Как можно заметить на Server0 в Syslog время задается в «не читаемом» виде исправим это с помощью команды `service timestamps log datetime msec`. Однако полученные значения времени и даты не верны, воспользуемся NTP для решения данной проблемы;
- 5. Настроим NTP на Router0.
  - 5.1. Настройте IP адрес на fa0/0;
  - 5.2. Настроим NTP и синхронизируем время с помощью команд `ntp server 192.168.1.4`. Проверьте;
  - 5.3. Настроим Syslog `logging on, logging trap debugging, logging 192.168.1.4, service timestamps log datetime msec`. Проверьте.

## Лабораторная работа № 19. AAA СЕРВЕР

**Цель работы:** Настроить централизованную авторизацию активных сетевых устройств

Рассмотрим схему из лабораторной работы №18 (рис. 31). Server0 будет выступать в качестве AAA сервера.

1. Запускаем Cisco Packet Tracer;
2. Настройте IP адреса на роутере (в нашем случае fa0/1 192.168.1.1/24), у PC0 192.168.1.2, PC1 - 192.168.1.3, у Server0 - 192.168.1.4;
3. Настроим роутер:
  - 3.1. Настройте пароль на привилегированный режим;
  - 3.2. Создайте пользователя для локальной базы и пароль;
  - 3.3. `aaa new model`. Создадим список методов подключения к маршрутизатору - `aaa authentication login default local`;
4. Настроим Server0.
  - 4.1. Настройки, Services, вкладка AAA, включаем. Задаем имя, IP адрес 192.168.1.1, пароль и добавьте клиента;
  - 4.2. Заполните базу пользователей и введите пароль.
5. Настроим роутер:
  - 5.1. Откорректируем список методов по `aaa authentication login default local` и создадим новый `aaa authentication login default group radius local`;
  - 5.2. Настроим radius сервер `radius-server host 192.168.1.4 key` (созданный пароль). Сохраните и проверьте.

## Лабораторная работа № 20. TRIVIAL FILE TRANSFER PROTOCOL (TFTP)

**Цель работы:** Настроить обновление конфигурации и программного обеспечения активного сетевого оборудования

Рассмотрим схему из лабораторной работы № 18 (рис. 31). Server0 будет выступать в качестве TFTP сервера.

1. Запускаем Cisco Packet Tracer;
2. Настроим коммутатор. Проверьте версию прошивки с помощью команды `show ver`. Проверьте наличие файла прошивка `show flash`;
3. Обновим прошивку:
  - Проверьте наличие свежей прошивки для TFTP сервера;
  - Задайте IP адрес 192.168.1.5 для связи с TFTP сервером, проверьте;
  - Загрузим прошивку с TFTP сервера `copy tftp: flash: 192.168.1.4` и пропишите имя файла из TFTP сервера. Проверьте `show flash`;
  - `boot system flash/(имя прошивки)`. Сохраните и перезагрузите.



## Лабораторная работа № 21. WIFI

**Цель работы:** Настроить беспроводной доступ доверенных конечных устройств в локальную сеть

Рассмотрим схему на рис. 32.

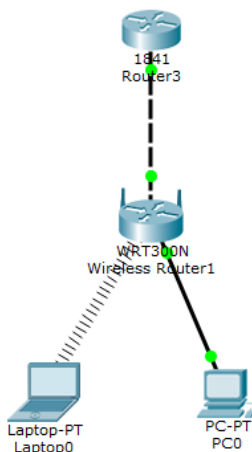


Рис. 32. Пример для организации WiFi роутер

**Рассмотрим пример WiFi роутера (рис. 32):**

1. На интерфейсе Router3 настройте IP адрес 210.210. 0.1;
2. Настроим WiFi Router1:
  - 2.1. Во вкладке GUI настроим IP адрес, используя Static IP 210.210.0.2, 255.255.255.252, маршрутом будет 210.210.0.1;
  - 2.2. Во вкладке Wireless можно выбрать настройки WiFi;
  - 2.3. Во вкладке Wireless Security можно выбрать режим, выбрать режим шифрования и задать ключевое слово. Сохраните
3. Настроим ноутбук. Wireless, вкладка Desktop, вкладка Connect, где видим доступные сети. Подключитесь к созданному нами WiFi и введите пароль. На рис. 32 видно, что подключение успешное (пунктирная линия). Проверьте выход в интернет;
4. В настройках компьютера проверьте IP адрес, выход в интернет и доступность ноутбука.

### Рассмотрим пример WiFi точка доступа (рис. 33):

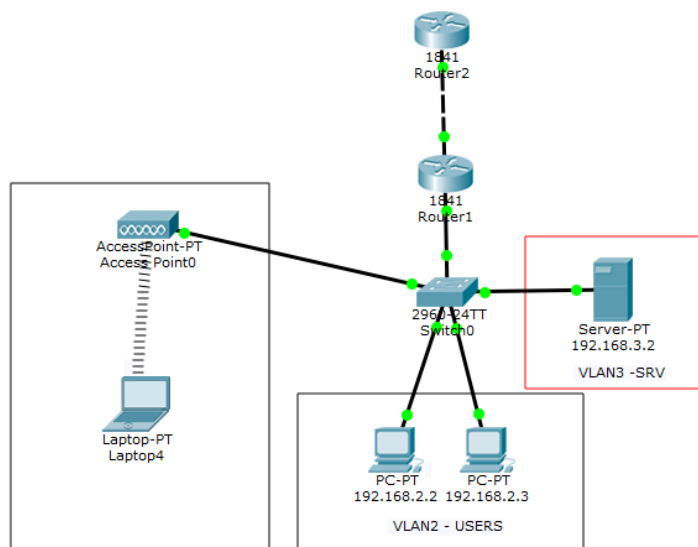


Рис. 33. Пример для организации WiFi точка доступа

1. Настройте порты на коммутаторе Switch0 в соответствующие VLAN;
2. На Router1 настройте интерфейс на подключение к интернет провайдеру, настройте sub интерфейсы, которые соответствуют VLAN 2 и 3, настройте NAT;
3. Проверьте сеть;
4. Настроим точку доступа, вкладка Config, вкладка Port 1, задайте идентификатор сети, тип аутентификации и задайте пароль;
5. Пусть WiFi сегмент будет во VLAN 4. Создайте VLAN 4 и настройте интерфейс в Switch0;
6. Создайте sub интерфейсы на Router1 и добавьте IP адрес 192.168.4.1 255.255.255.0;
7. Настроим раздачу IP адресов пользователям на Router1:
  - 7.1. Создадим ip dhcp pool WiFi-pool, network 192.168.4.0. 255.255.255.0, default router 192.168.4.1;
  - 7.2. Необходимо исключить IP адрес маршрутизатора из DHCP с помощью команды ip dhsp excluded-addresses 192.168.4.1;

7.3. Настроим NAT, отредактировав созданный access list - `ip access-list standard FOR-NAT, permit 192.168.4.0 0.0.0.255`.

7.4. В нашем случае fa0/1.4 определим как `ip nat inside`. Сохраните;

8. Настроим ноутбук аналогично предыдущей схеме (рис. 32) и определим точку доступа в VLAN 4 на маршрутизаторе с помощью команд `switchport mode access, switchport access vlan 4 description WiFi-AP`.

9. Проверьте работоспособность сети