**Лабораторная работа 13.**

**Обновление DHCP-сервера в Cisco Packet Tracer - 2**

**Цель работы:** научиться работать с протоколом DHCP в Cisco Packet Tracer

**Теоретическая часть**

Протокол DHCP (Dynamic Host Configuration Protocol) относится к числу основных служб, формирующих инфраструктуру сетей. Он применяется для автоматического выполнения конфигурации сетевых параметров.

*Обновление адреса*

Одной из важных функций, для чего предназначен протокол DHCP, можно назвать функцию обновления сетевых адресов. IP предоставляется клиенту на установленный период, называемый *временем аренды*. Его продолжительность в зависимости от установленных настроек сервера изменяется в пределах от минут до месяцев. После завершения половины этого периода клиент предпринимает попытку обновить аренду. При неудаче предпринимаются повторные попытки обновления, которые будут следовать до завершения срока. Если не одна попытка не завершится успешным обновлением, клиент приступит к поиску нового сервера.

В процессе обновления аренды клиент проходит два состояния:

RENEWING — обновление адреса.

REBINDING — обновление конфигурации.

Наступление состояния RENEWING предусмотрено на половине времени аренды (T1), а состояние REBINDING — после прохождения 87,5 этого периода (T2). Чтобы исключить синхронизацию различных клиентов, используется случайная величина отклонения при определении T1 и T2.

*Работа при RENEWING*

В этом состоянии клиентом запускается процесс обновления аренды. Для этого он направляет запрос DHCPREQUEST на собственный DHCP-сервер. При согласии сервера на продление клиенту возвращается ответ DHCPACK, в котором прописано новое время аренды и обновленные параметры. Клиент отмечает полученные значения, сбрасывает отсчет времени T1 и T2, после чего переходит в нормальное рабочее состояние.

В случае отказа сервер возвращает сообщение DHCPNACK. В результате клиент снова начинает инициализацию и повторно запускает процедуру обновления времени аренды.

*Работа при REBINDING*

При неполучении от ответа на запрос, направленный для обновления аренды, клиент ожидает его в течение определенного времени. После этого серверу направляется повторный запрос. Клиент продолжает поддерживать состояние RENEWING и периодически отправляет запросы DHCPREQUEST до получения ответа со стороны сервера. Весь этот период он нормально работает на своем текущем IP-адресе.

Если до наступления T2 не поступает серверный ответ, сетевой протокол DHCP предусматривает перевод клиента в состояние REBINDING, после чего при помощи широковещания направляется запрос DHCPREQUEST с указанием текущего адреса. Такие запросы посылаются через определенное время.

Если серверный ответ не поступает до окончания времени аренды, клиент прекращает отправку запроса и переходит в состояние инициализации. При получении ответа после окончания времени аренды клиент сможет снова работать со своим прежним IP-адресом.

*Освобождение адреса*

Для отказа от аренды IP клиент передает серверу специальный запрос DHCPRELEASE. В ответ сервер помечает соответствующий IP-адрес свободным. При этом резервируется запись с клиентскими сетевыми параметрами. Это необходимо для того, чтобы возобновить действие адреса при поступлении такого запроса. При простом выключении клиент не прекращает аренду, а сохраняет локально все установленные настройки. Запрос DHCPRELEASE направляется клиентом только при возникновении потребности в отказе от аренды. Например, такая необходимость может возникнуть при переходе в новую подсеть. Кроме того, существует возможность отказа от аренды вручную. Для этого можно использовать команду *ipconfig/release*.

*Особенности работы DHCP*

Сетевой протокол DHCP работает посредством UDP. Обмен данными между клиентом и сервером осуществляется через порты 67 UDP и UDP 68. Для передачи информации от клиента к серверу DHCP протокол задействует порт 67 UDP, а в обратном направлении — 68 UDP.

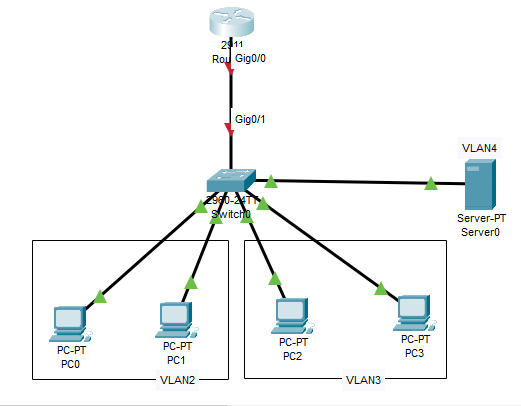
По умолчанию запросы протокола DHCP передаются в пределах текущей подсети. Это объясняется использованием широковещания, не пропускаемого маршрутизаторами за границы широковещательного домена. Такой домен обычно ограничен пределами логической или физической подсети.

При расположении в разных широковещательных доменах общение клиентов и серверов производится через специальный ретранслятор DHCP *relay agent*. Он выполняет функцию посредника, который обеспечивает обмен сообщениями между клиентом и сервером в формате адресных пакетов. Таким ретранслятором может служить маршрутизатор или специальный сервер, например, Windows Server.

Для нормальной работы и исполнения назначения протокола DHCP необходимо удостовериться, что необходимые порты не блокируются брандмауэром. В случае, расположения клиентов и сервера в разных подсетях, важно проверить наличие ретранслятора DHCP *relay agent*.

Спроектируем и настроим сеть.

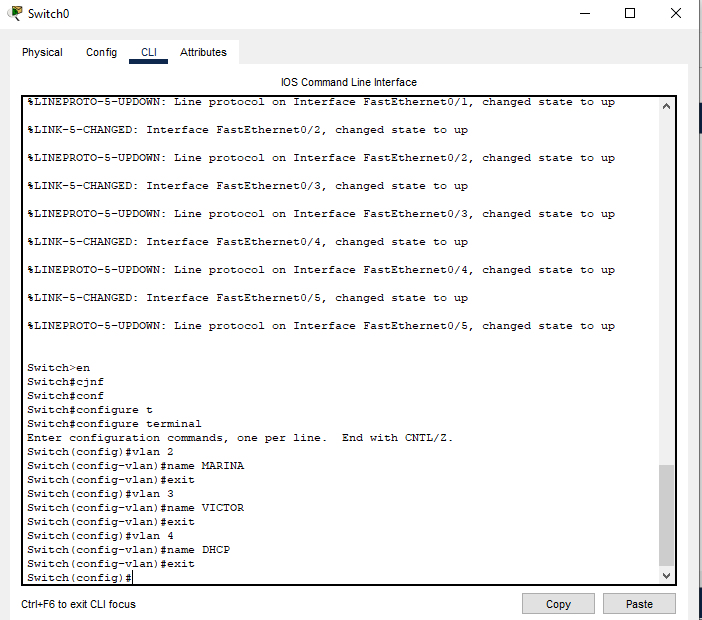
Используем 4 компьютера, 1 сервер, 1 коммутатор и 1 маршрутизатор.



Компьютеры PC0 и PC1 объединены во VLAN2. PC2 и PC3 во VLAN3. Сервер находится во VLAN4.

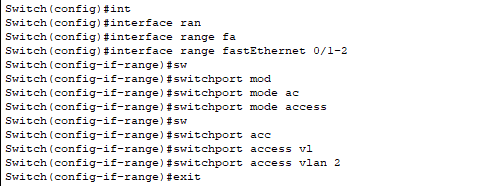
Сделаем настройки.

Настройки коммутатора. Необходимо создать VLAN. Имена VLAN2 и VLAN3 дать по своему имени и фамилии. VLAN4 дать имя DHCP.



Настройка портов

VLAN2 на порты Fa0/1 и Fa0/2 (проверить на какие порты сделано подключение). Команда ***range*** сразу настраивает несколько портов.



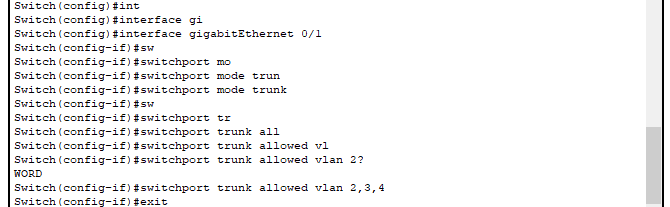
Аналогично настраиваются порты Fa0/3 и Fa0/4 на VLAN3.

Настройка порта до сервера.

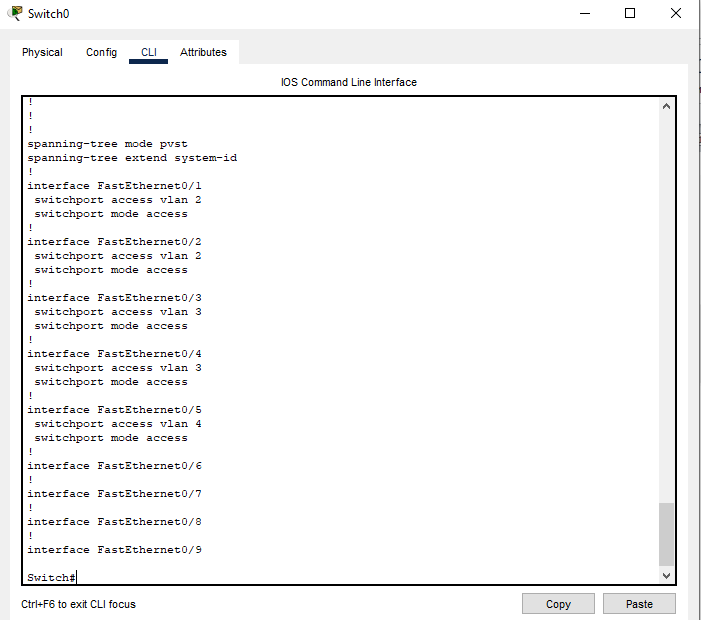
VLAN4 на порт Fa0/5 (проверить на какой порт сделано подключение). Все порты определить как access порты.

Настройка порта до роутера

Проверить на какой порт сделано подключение. Порт Gig0/1 определить как trunk порт.

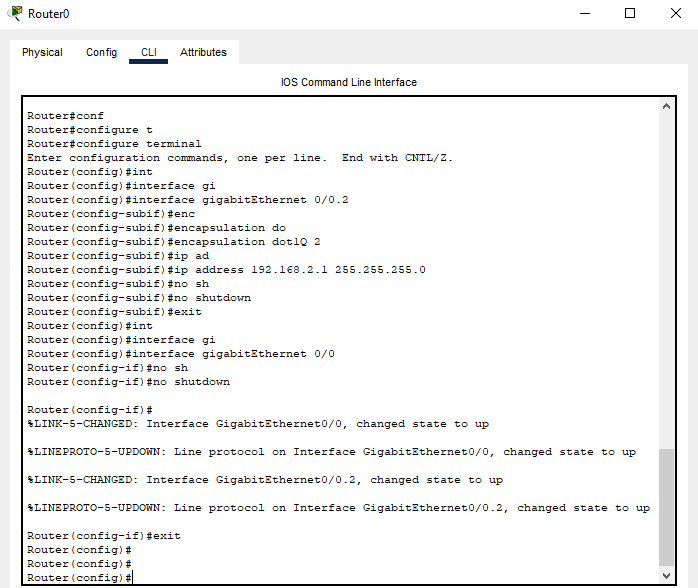


Посмотреть командой ***show run*** все настройки.

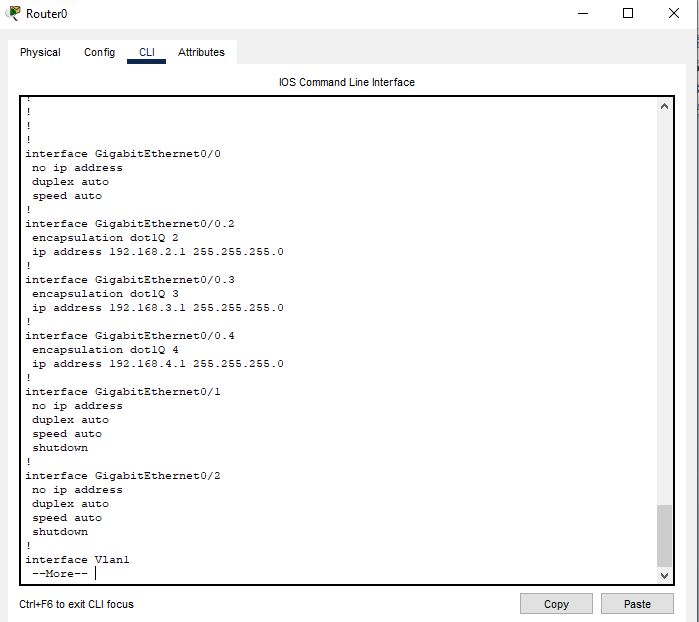


Настройка маршрутизатора

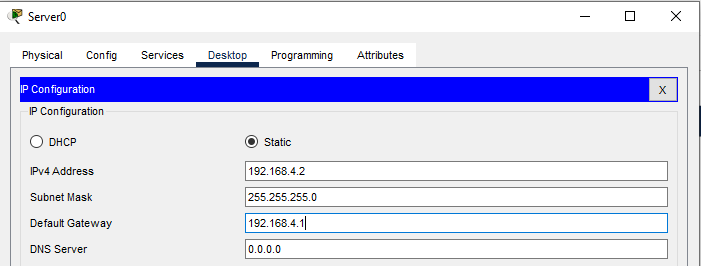
Необходимо настроить sub-interface для VLAN2 (проверить подключение порта). Задать IP-адрес 192.168.2.1 255.255.255.0 и включить sub-interface. Нужно включить порт.



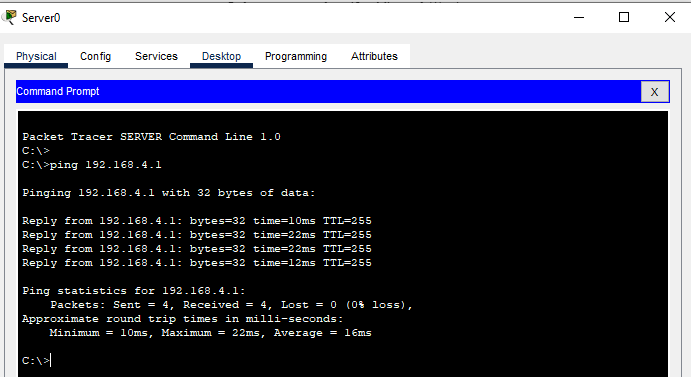
Такие же настройки сделать для VLAN3. Задать IP-адрес 192.168.3.1 255.255.255.0 и включить sub-interface. Для VLAN4 задать IP-адрес 192.168.4.1 255.255.255.0 и включить sub-interface. Проверить все настройки командой ***show run***.



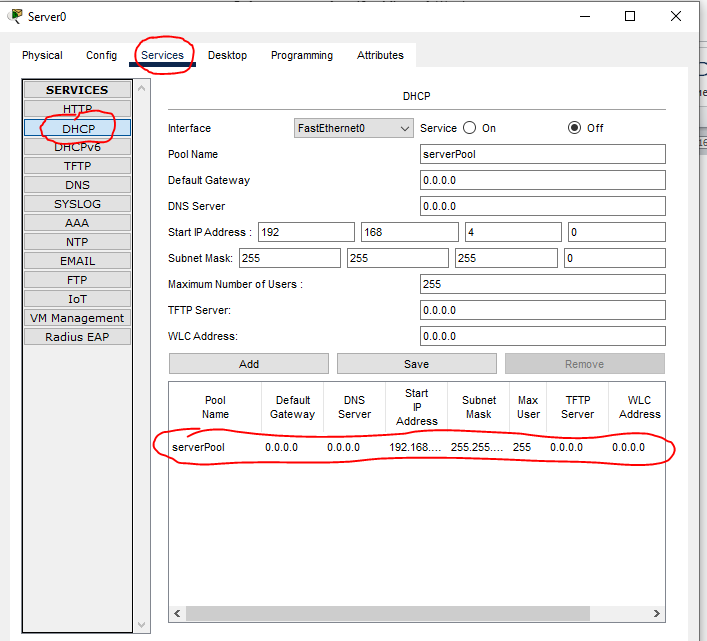
Настройка DHCP-сервера. Статический IP-адрес 192.168.4.2 255.255.255.0 и шлюз 192.168.4.1



Проверить взаимодействие с роутером.



Проверить создание pool (пула).



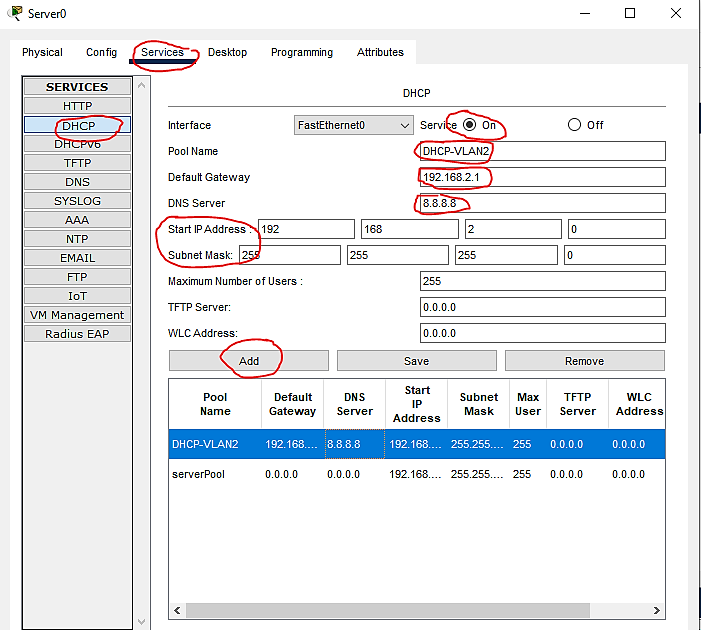
Создать новый pool для VLAN2. Имя DHCP-VLAN2

Шлюз 192.168.2.1

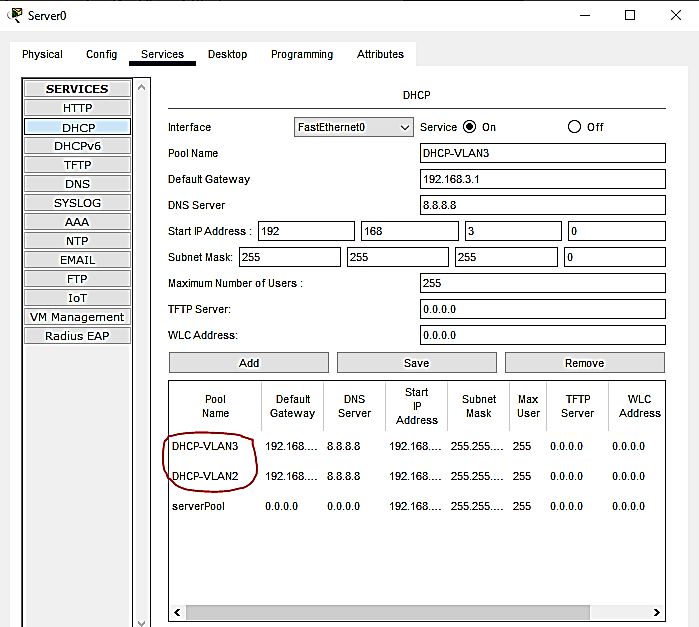
DNS 8.8.8.8

IP-адрес 192.168.2.0

Включить ON Добавить Add



Таким же образом создать для VLAN3.



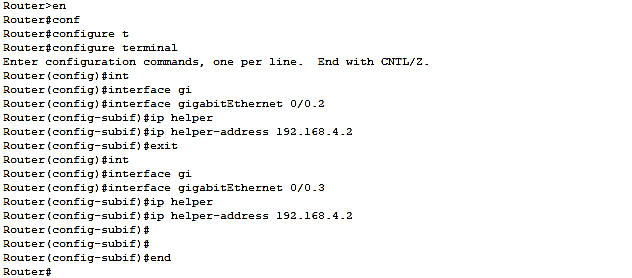
Эти pool будут раздавать IP-адреса соответствующим сегментам.

Необходимо переадресовать запросы компьютеров на DHCP-сервер.

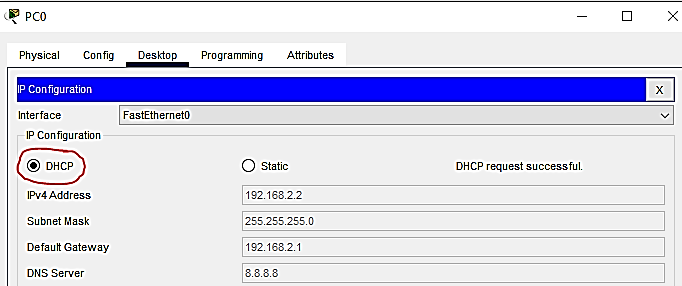
Для этого используется функция перенаправления DHCP-запросов на DHCP-сервер.

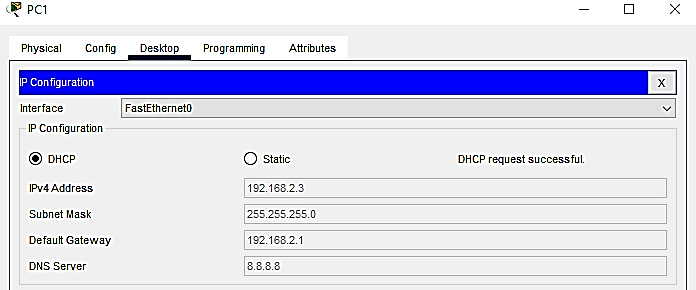
***ip helper-address***

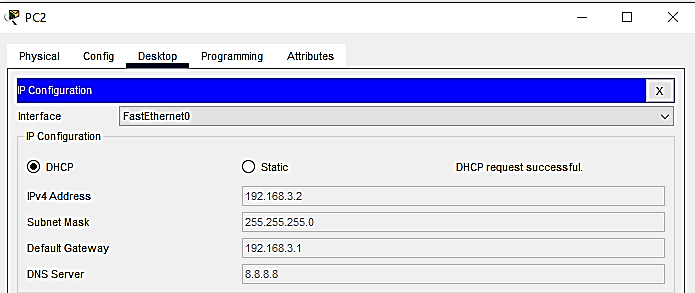
Необходимо настроить эту функцию на роутере для каждого VLAN.

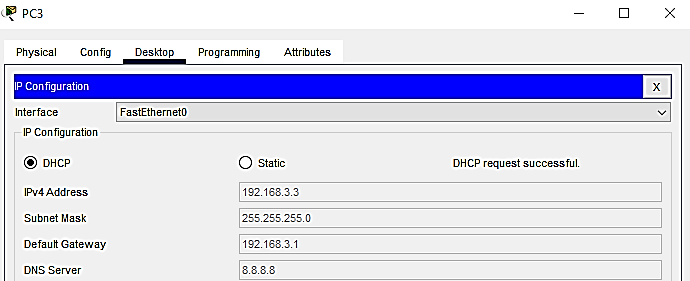


Получаем IP-адреса на компьютерах.

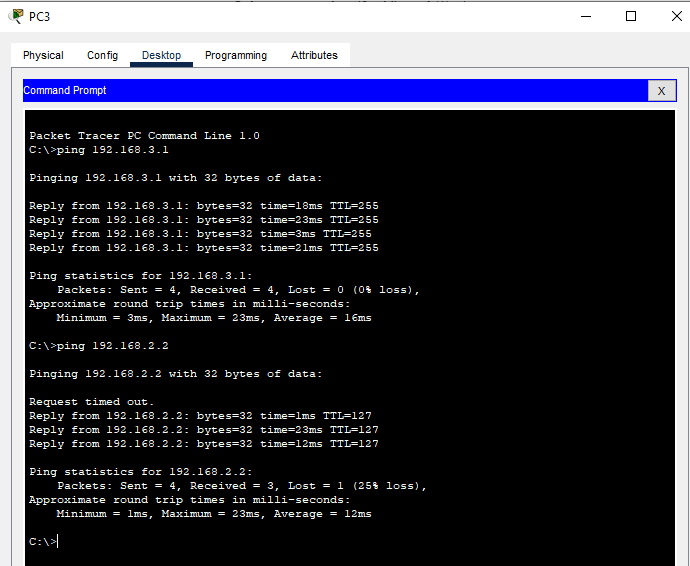








Проверить взаимодействие до шлюза и с компьютерами соседнего сегмента.



Ping проходит. Было настроено автоматическое получение IP-адресов для двух сегментов посредством выделенного DHCP-сервера.

**Задание на лабораторную работу:**

1. Настроить протокол DHCP в Cisco Packet Tracer. Имена VLAN дать по своему имени и фамилии. Скриншоты всех действий поместить в отчет.
2. Ответить письменно на контрольные вопросы к лекциям 25 и 26.