**Лабораторная работа 12.**

**Обновление DHCP-сервера в Cisco Packet Tracer - 1**

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

**Теоретическая часть**

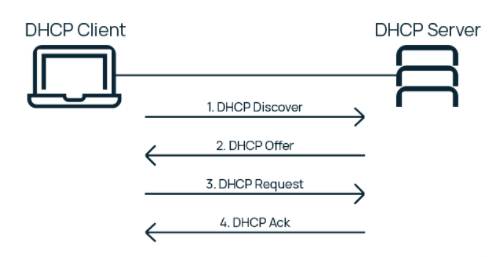
DHCP — протокол автоматизации назначения IP-адреса клиенту. Он широко используется в современных сетях.

DHCP — протокол прикладного уровня модели TCP/IP, служит для назначения IP-адреса клиенту — Dynamic Host Configuration Protocol. IP-адрес можно назначать вручную каждому клиенту, то есть компьютеру в локальной сети. Но в больших сетях это очень трудозатратно, поэтому для автоматизации назначения IP был создан протокол DHCP.

Впервые протокол был описан в 1993 году в документе RFC 1531, но с тех пор в описание вносились правки. На сегодняшний день основным документом, регламентирующим протокол, является RFC 2131.

Принцип работы DHCP

Получение адреса проходит в четыре шага. Этот процесс называют DORA по первым буквам каждого шага: Discovery, Offer, Request, Acknowledgement.



*Discovery, или поиск*

Изначально клиент находится в состоянии инициализации (INIT) и не имеет своего IP-адреса. Поэтому он отправляет широковещательное (broadcast) сообщение DHCPDISCOVER на все устройства в локальной сети. В той же локальной сети находится DHCP-сервер. DHCP-сервер — это, например, маршрутизатор или коммутатор, существуют также выделенные DHCP-серверы.

Не всегда одну сеть обслуживает один DHCP-сервер, нередко организации устанавливают сразу несколько. Сервер всегда слушает 67 порт, ожидает широковещательное сообщение от клиента, а после его получения отправляет ответное предложение — DHCPOFFER. Клиент принимает сообщение на 68 порту.

*Offer, или предложение*

DHCP-сервер отвечает на поиск предложением, он сообщает IP, который может подойти клиенту. IP выделяются из области (SCOPE) доступных адресов, которая задается администратором. Если имеются адреса, которые не должны быть назначены DHCP-сервером, область можно ограничить, указав только разрешенные адреса. Например, администратор может задать диапазон используемых IP-адресов от 192.0.0.10 до 192.0.0.255.

Бывает и так, что не все доступные адреса должны быть назначены клиентам. Например, администратор может исключить (exclude) диапазон 192.0.0.100 — 192.0.0.200 из используемой области. Такое ограничение называется исключением.

*Request, или запрос*

Клиент получает DHCPOFFER, а затем отправляет на сервер сообщение DHCPREQUEST. Этим сообщением он принимает предлагаемый адрес и уведомляет DHCP-сервер об этом. Широковещательное сообщение почти полностью дублирует DHCPDISCOVER, но содержит в себе уникальный IP, выделенный сервером, а сервера помечают IP как занятый.

*Acknowledgement, или подтверждение*

Сервер получает от клиента DHCPREQUEST и окончательно подтверждает передачу IP-адреса клиенту сообщением DHCPACK. Это широковещательное или прямое сообщение утверждает не только владельца IP, но и срок, в течение которого клиент может использовать этот адрес.

*Срок аренды*

Когда DHCP-сервер выделяет IP из области, он оставляет запись о том, что этот адрес зарезервирован за клиентом с указанием срока действия IP. Этот срок действия называется срок аренды (lease time). Срок аренды может составлять от 24 часов до нескольких дней, недель или даже месяцев, он задается в настройках самого сервера.

*Недостатки протокола DHCP*

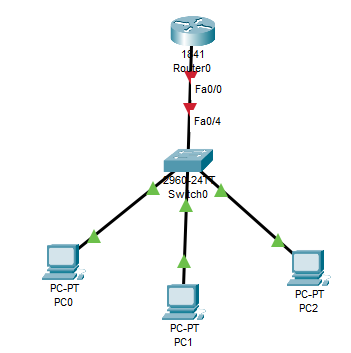
DHCP имеет свои уязвимости. Основная заключается в четырех шагах, необходимых для получения IP. Процесс DORA подразумевает рассылку сообщений широковещательного типа, когда первый откликнувшийся DHCP-сервер получает возможность предложить IP из своей области. Если злоумышленник сможет использовать свой сервер, который даст самый быстрый ответ клиенту, то у него откроется возможность получить контроль над действиями пользователя в сети и нанести существенный ущерб.

Еще одна брешь в безопасности — в том, что DHCP использует UDP-протокол. UDP — протокол обмена датаграммами без установления соединения, а значит, и без шифрования. Передаваемая по UDP информация не защищена и может быть «подслушана», что также может быть использовано злоумышленниками.

Третий недостаток — UDP не обеспечивает гарантию доставки информации. Этот протокол допускает потери и ошибки, которые могут сказаться и на работе DHCP.

Спроектируем и настроим сеть.

Используем 3 компьютера, 1 коммутатор и 1 маршрутизатор.



Настройка роутера

Заходим на роутер. Выбираем CLI(консоль)

***en*** – вход в привелигерованный режим (появится #).

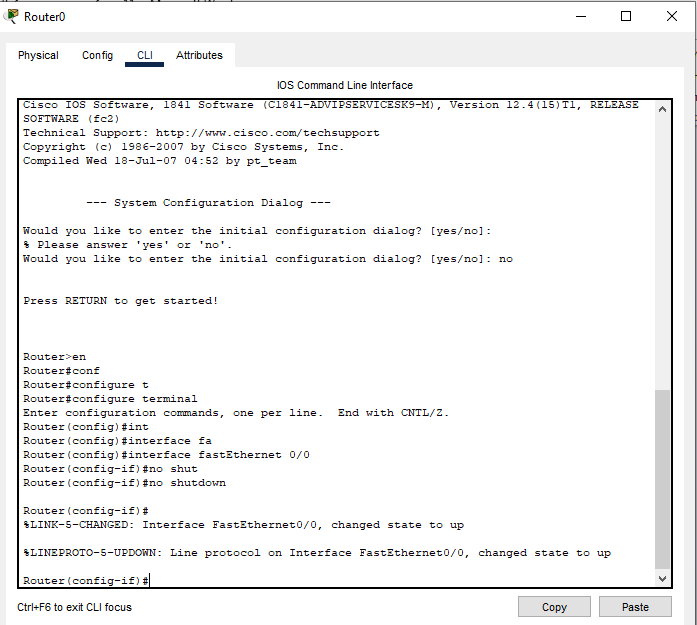
***conf t*** – режим глобального конфигурирования.

***int*** – настройка интерфейса.

***fa***  – FastEthernet.

***0/0*** – порт 0/0.

***no shut*** – включить порт.



***ip address 192.168.1.1 255.255.255.0*** – присвоить IP-адрес роутеру.

***exit*** – выход.

Необходимо создать DHCP пул – это пространство IP-адресов.

***ip dhcp pool DHCP*** – создание DHCP пула (имя пула DHCP).

Нужно задать из какой сети будут раздаваться IP-адреса. В данной сети в качестве DHCP сервера выступает роутер.

***network 192.168.1.0 255.255.255.0***

Компьютерам нужен не только IP-адрес, но и маршрут.

***defa*** – по умолчанию маршрут проходит через роутер.

***192.168.1.1*** – адрес роутера.

Необходимо указать DNS-сервер для выхода в сеть Интернет.

***dns-server*** –DNS-сервер

***8.8.8.8*** – в качестве примера берем IP-адрес DNS Google.

***exit*** – выход.

Можно исключить определенные IP-адреса из выдачи в DHCP (например, IP-адрес 192.168.1.100)

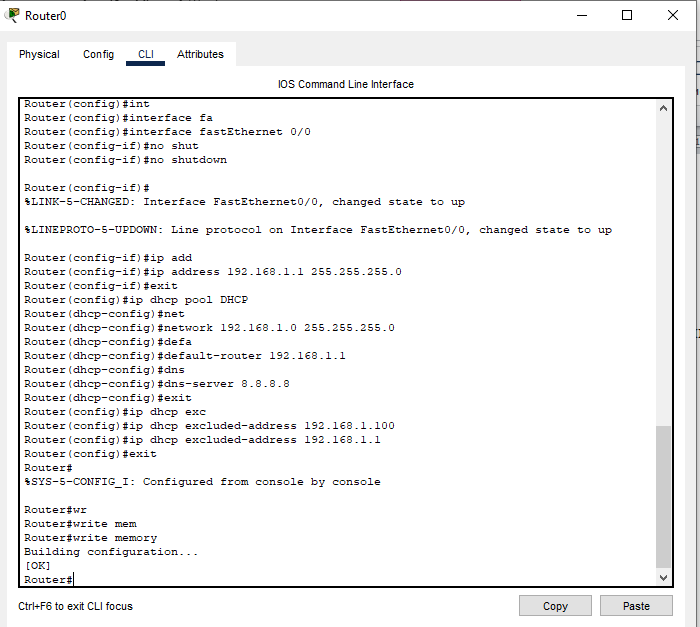
***ip dhcp excluded-address 192.168.1.100*** – исключение IP-адреса 192.168.1.100

Нужно исключить из выдачи DHCP IP-адрес роутера.

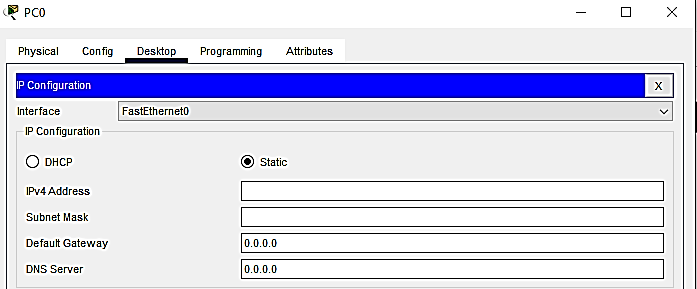
***ip dhcp excluded-address 192.168.1.1*** – исключение IP-адреса роутера

***exit*** – выход.

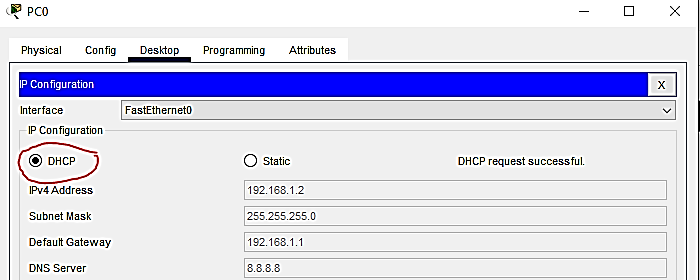
***write memory*** – сохранение настроек.



Посмотреть настройки компьютеров.

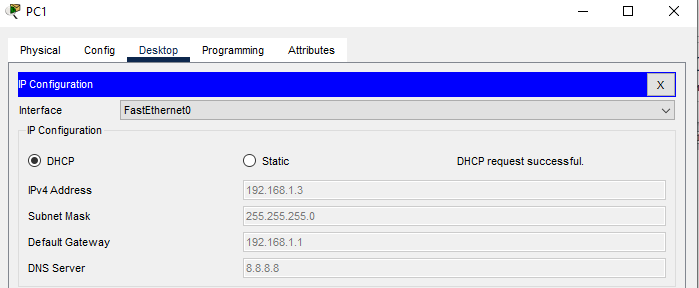


По умолчанию стоит параметр Static. Изменяем на DHCP (на реальных компьютерах всегда по умолчанию выставлен параметр DHCP).



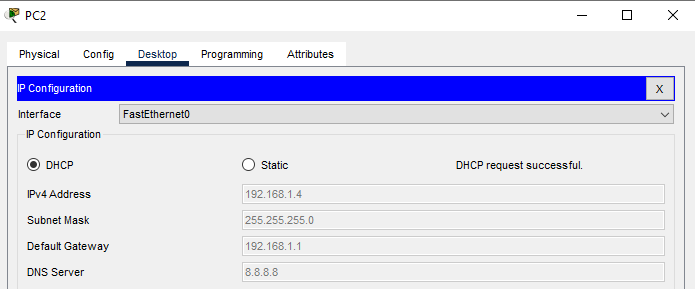
Компьютер получил IP-адрес и адрес шлюза.

Изменим параметр на компьютере PC1.

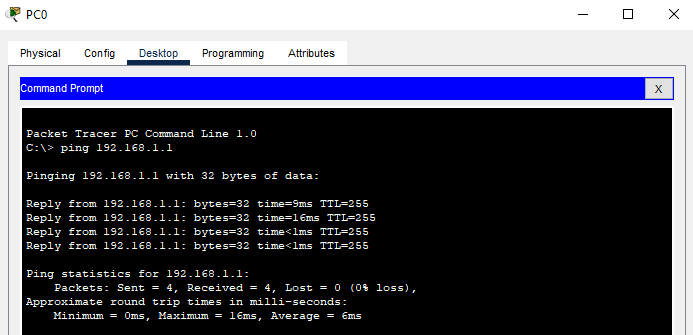


Компьютер получил IP-адрес и адрес шлюза.

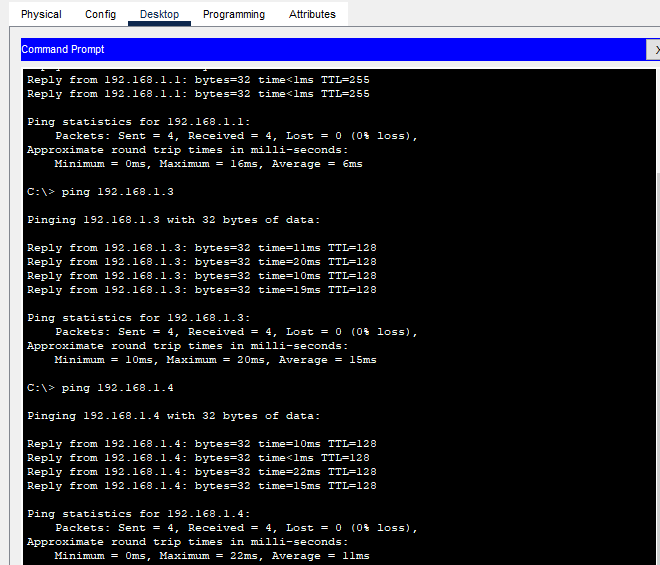
Изменим параметр на компьютере PC2. Компьютер получил IP-адрес и адрес шлюза.



Проверим взаимодействие. Пропингуем до шлюза.

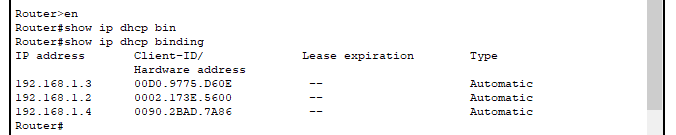


Пропингуем компьютеры между собой.



Можно посмотреть какие IP-адреса каким компьютерам были выданы:

***show ip dhcp binding***



**Задание на лабораторную работу:**

1. Настроить протокол DHCP в Cisco Packet Tracer. Скриншоты всех действий поместить в отчет.
2. Ответить письменно на контрольные вопросы к лекциям 23 и 24.