

**МИНОБРНАУКИ РОССИИ**

**федеральное государственное бюджетное образовательное учреждение**

**высшего образования**

**«Московский государственный технологический университет «СТАНКИН»**

**(ФГБОУ ВО «МГТУ «СТАНКИН»)**

Институт цифровых интеллектуальных систем  
Кафедра компьютерных систем управления

Образовательная программа 15.03.04

«Автоматизация технологических процессов и производств»

Дисциплина «Вычислительные машины, системы и сети»

**Отчет**

**Лабораторная работа №4**

**«**Разработка проекта компьютерной сети c реализацией VLAN**»**

Выполнил:

студент

гр. АДБ-18-08 \_\_\_\_\_\_\_\_\_\_\_\_\_ Пискунов М.П.

(дата) (подпись)

Принял:

Преподаватель \_\_\_\_\_\_\_\_\_\_\_\_\_ Путинцева Е.В.

(дата) (подпись)

**Оглавление**

[Введение: 3](#_Toc69161677)

[Практическая часть: 3](#_Toc69161678)

[Добавление оборудования 3](#_Toc69161679)

[Настройка ПК первого и второго отдела 4](#_Toc69161680)

[Настройка третьего отдела 5](#_Toc69161681)

[Настройка беспроводных ПК. 7](#_Toc69161682)

[Настройка сервера: 13](#_Toc69161683)

[Вывод 15](#_Toc69161684)

# **Введение:**

Компания арендовала 3 помещения в бизнес-центре. В этих помещениях есть только голые стены и розетки. Вы - сетевой и системный администратор. Вас попросили разработать схему сети.

В сети должна быть реализована возможность связываться с любым из трёх помещений в компании, но при этом каждое помещение (отдел) должны быть изолированы. Также в третьем помещении необходимо создать беспроводную точку доступа. Эта точка должна иметь пароль junior17, должны автоматически выдаваться первые 20 адресов, SSID должен быть скрыт.

Во втором отделе стоит ненастроенный web-сервер. Это тоже необходимо исправить. От Вас требуется реализовать в каждом помещении возможность получать доступ к серверу по url имени.

В первом отделе 4 рабочих места, во втором — 2 рабочих места и сервер, третье помещение нужно для отдыха персонала (10 рабочих мест, в том числе 4 беспроводных). К сетевому оборудованию вам необходимо предоставить безопасный удаленный доступ (SSH).

Всю работу необходимо выполнить в Cisco Packet Tracer.

Использовать 3 коммутатора Cisco 2960, маршрутизатор Cisco 1941 и роутер Cisco WRT300N.

# **Практическая часть:**

# **Добавление оборудования**

Открыть Packet Tracer и создать на рабочем поле: a. 16 компьютеров b. Сервер c. 3 коммутатора Cisco 2960 d. Маршрутизатор Cisco 1941 e. Роутер Cisco WRT300N

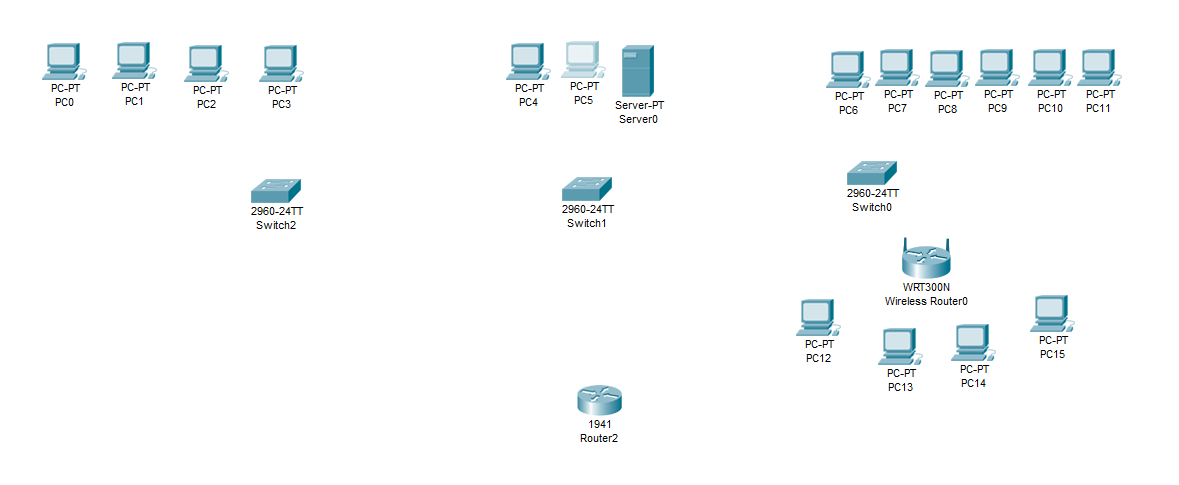


Рис1. Общий вид устройств сети

Настройка беспроводного подключения

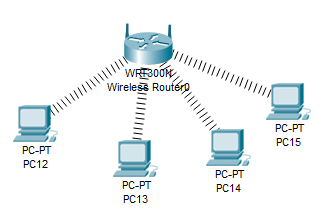


Рис.2 Результат настройки

# **Настройка ПК первого и второго отдела**

Каждому компьютеру в первом и втором отделе, а также серверу присвоим значения по формуле: N0.0.0.n, где N – номер отдела, а n – номер устройства (например, 10.0.0.2 – второй компьютер на первом этаже). Сервер, так как он третье устройство на втором этаже будет иметь адрес 20.0.0.3.

Маску подсети выставим на 255.255.255.0. Default Gateway выставим N0.0.0.254. DNS Server выставляем на 20.0.0.3.

Пример правильно настроенного ПК в первом отделе:

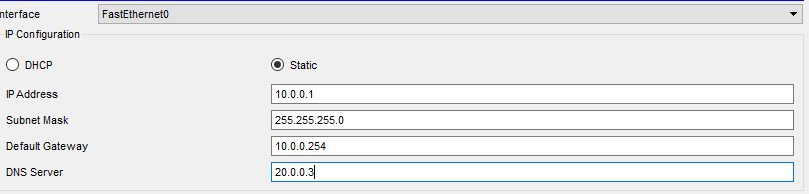


Рис.3.1 Настройка ПК в первом (левом по схеме) отделе

Пример правильно настроенного ПК во втором (среднем) отделе:

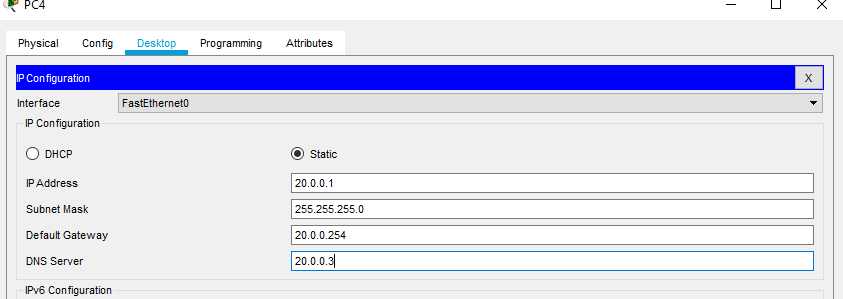


Рис.3.2 Настройка ПК во втором (среднем) отделе

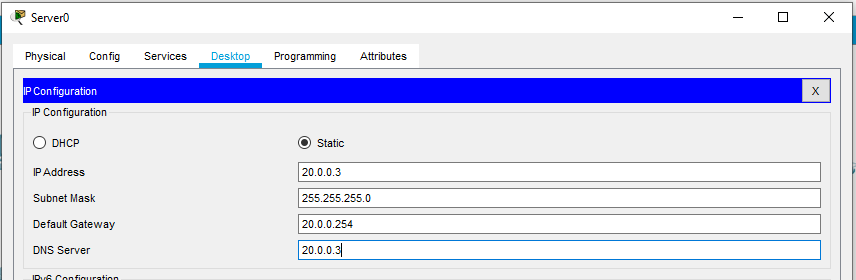


Рис. 4 Настройка сервера

# **Настройка третьего отдела**

Выставим IP по формуле 30.0.0.10n, где n – номер ПК. Пример правильно настроенного ПК в третьем отделе:

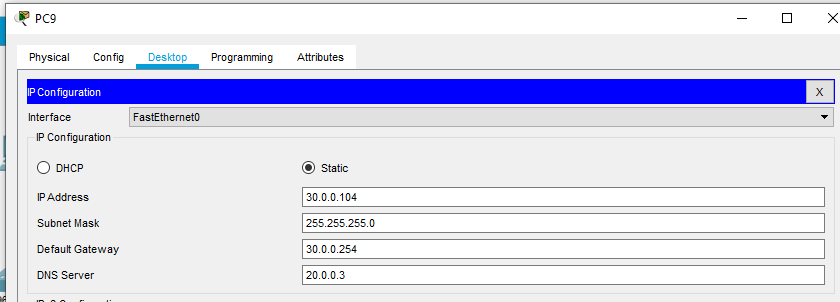


Рис. 5 Настройка ПК в третьем (правом по схеме) отделе

Настройка беспроводного роутера Выставим настройки:

DHCP вкл. IP - 30.0.0.253

Маска - 255.255.255.0

Start IP Address - 30.0.0.1

Maximum number of Users – 20

Static DNS 1 - 20.0.0.3

Network Name - Cisco2107

SSID Broadcast – Disabled

Security Mode - WPA2-Personal

Passphrase - junior17

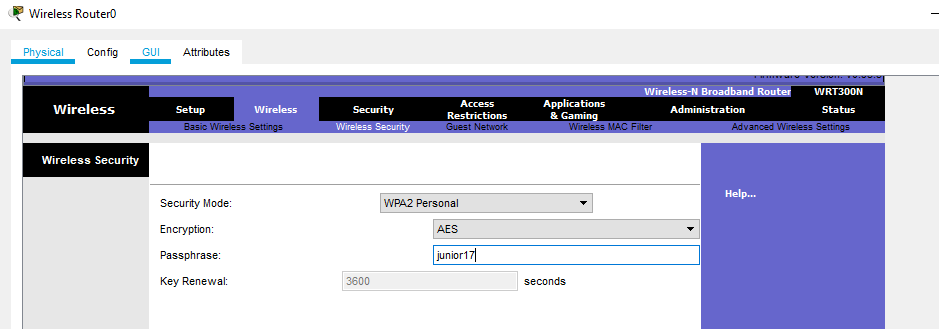
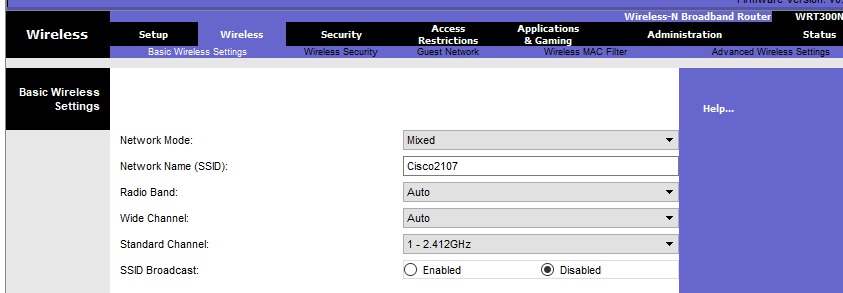
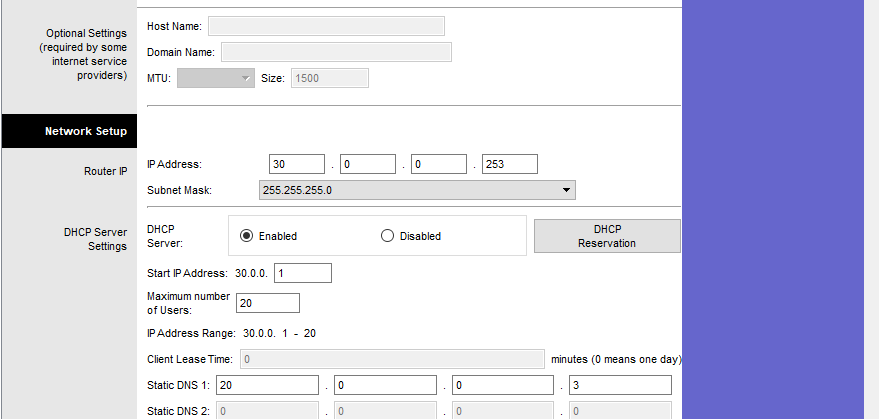


Рис.6 Основные настройки беспроводного роутера

# **Настройка беспроводных ПК.**

Задаём имя сети **Cisco2107** и WPA2-Personal пароль – **junior17** Пример настроек одного из ПК:

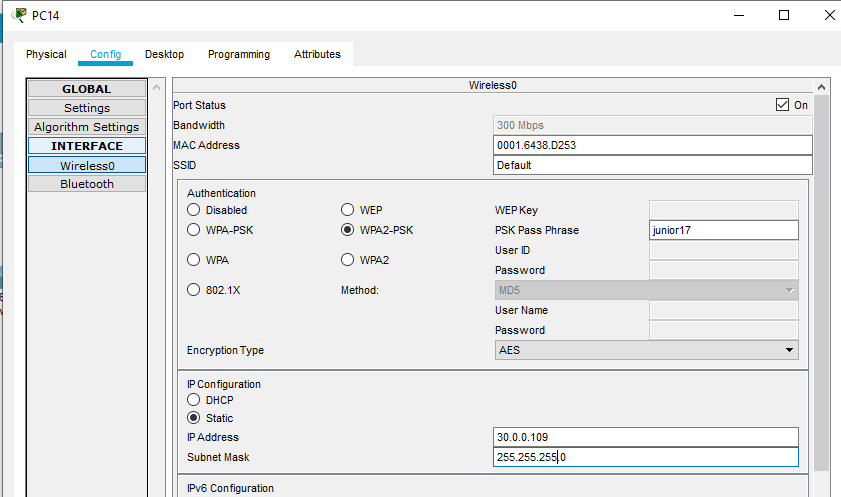


Рис.7 Настройки беспроводной связи ПК

Вид сети после добавления кабельных подключений

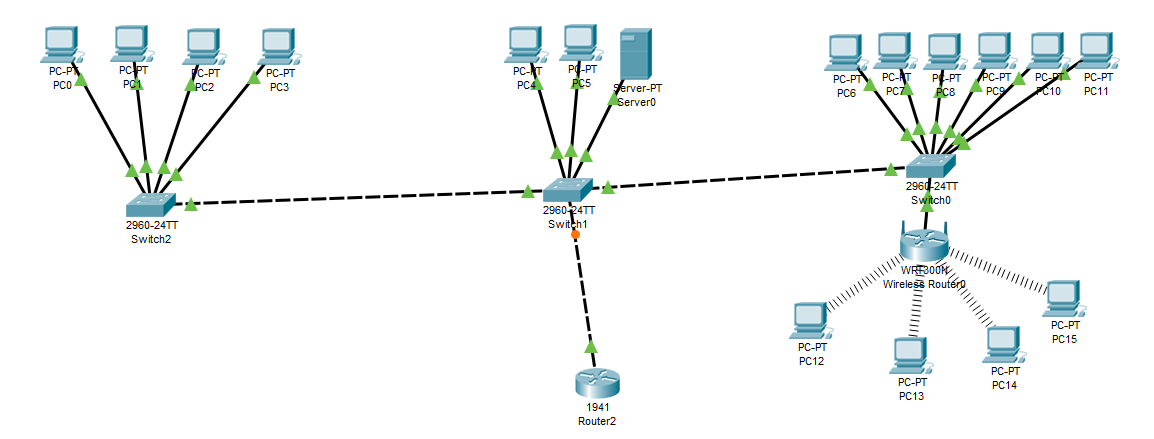
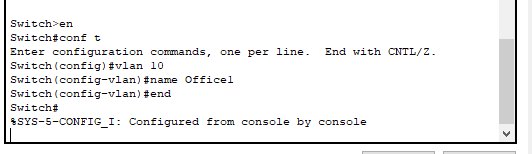


Рис. 8 Схема сети со всеми подключениями

Настройка VLAN коммутатора 1



Рассмотрим все команды:

**en** – enable. Расширенный доступ к конфигурации

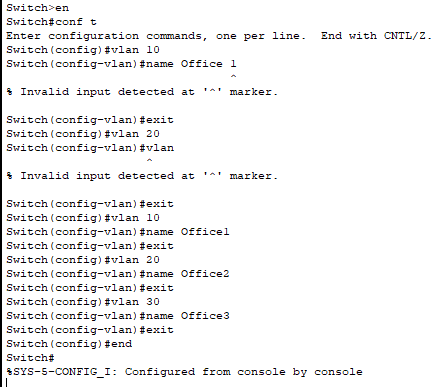
**conf t** – configuration terminal. Открывает терминал настройки

**vlan 10** – создаёт виртуальную сеть с индексом 10

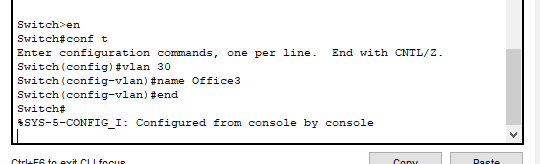
**name Office1** – задаётся имя VLAN. Имя – Office1.

**end** – завершения настройки.

Настройка VLAN коммутатора 2



Настройка VLAN коммутатора 3



Выставляем на первом коммутаторе VLAN 10 на все порты, к которым есть подключение. Это делается на вкладке Config выбором VLAN из выпадающего списка.

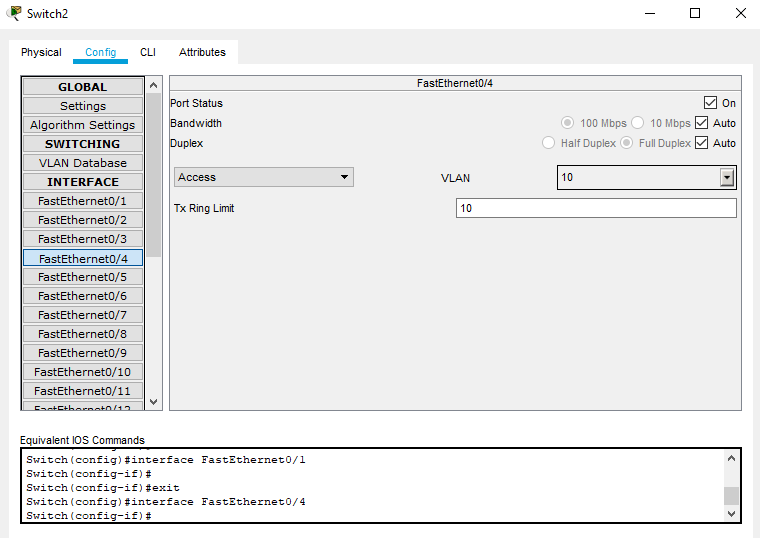


Рис.9 Установка VLAN на порт коммутатора

На втором коммутаторе нужно выставить порт, к которому подключен коммутатор из первого отдела VLAN 10, из третьего VLAN 30, а порты с подключениями к 2 ПК и серверу второго отдела - VLAN 20.

Порт, соединяющий коммутатор и маршрутизатор выставляем в Trunk режим:

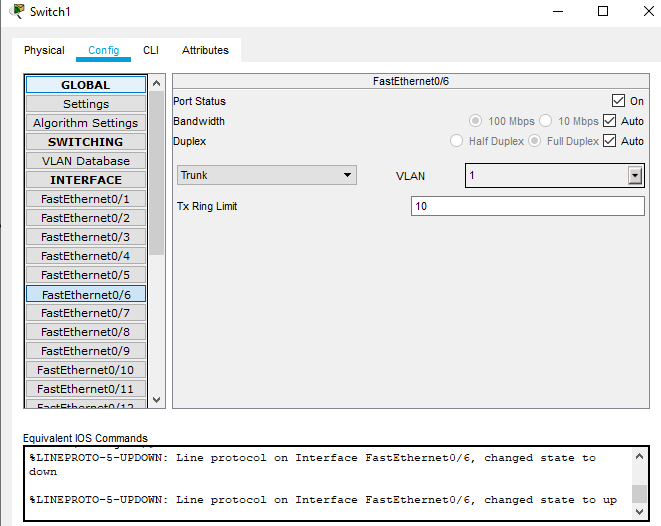
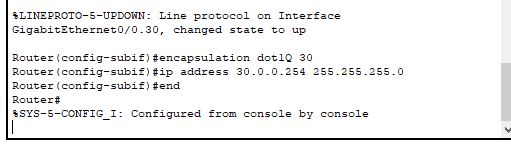
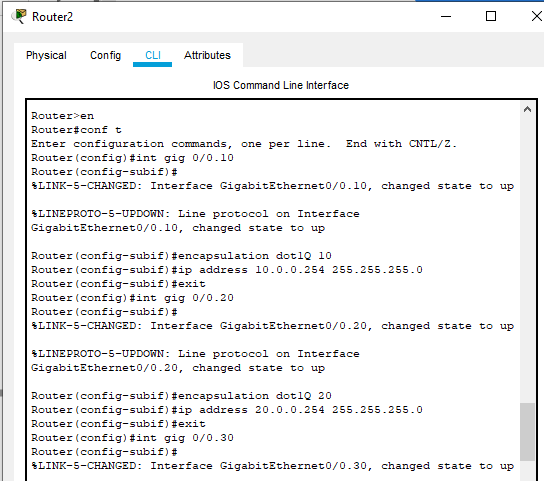


Рис.10 Установка порта в режим Trunk

На третьем коммутаторе нужно выставить на все порты VLAN 30.

Производим настройку маршрутизатора для работы с VLAN.



Разберём команды:

**int gig 0/0.10** - команда подключает виртуальный интерфейс для работы с VLAN. Цифра после точки – номер VLAN.

**encapsulation dot1Q 10** - команда настройки виртуального интерфейса для VLAN. Номер после dot1Q – номер VLAN.

**ip address 10.0.0.254 255.255.255.0** - IP адрес выхода пакетов информации для текущей настраиваемой VLAN.

Пропингуем компьютеры

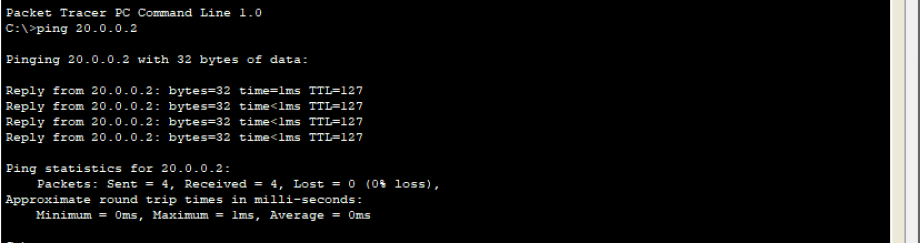


Рис.11 Пинг машины из другого отдела

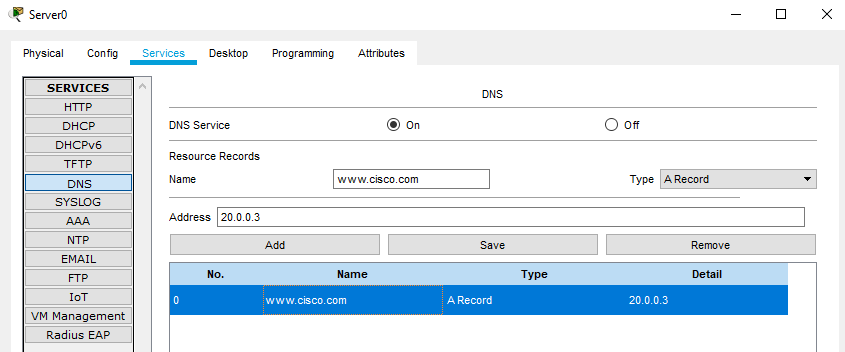


Рис.12 Параметры DNS сервера

# **Настройка сервера:**

Включаем DNS (вкладка Services -> DNS).

Name — www.cisco.com Address – 20.0.0.3

Проверим возможность выхода на сайт из любого отдела. Вводим URL имя в браузере (находим его во вкладке Desktop) и нажимаем Go:

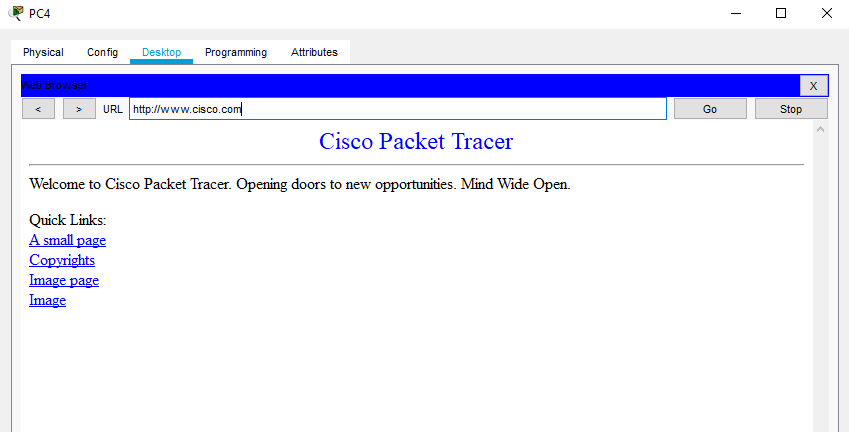


Рис.13 Проверка DNS

Настроим SSH. Для этого заходим в маршрутизатор, во вкладку CLI и вводим команды:

Router>en

Router#clock set 10:10:00 24 Feb 2019

Router#conf t

Router(config)#hostname ncsrouter

ncsrouter(config)#ip domain name ncs.dom

ncsrouter(config)#crypto key generate rsa

Ввести длину ключа (512)

ncsrouter(config)#service password-encryption

ncsrouter(config)#username Alex privilege 15 password junior17

ncsrouter(config)#aaa new-model

ncsrouter(config)#line vty 0 4

ncsrouter(config-line)#transport input ssh

ncsrouter(config-line)#logging synchronous

ncsrouter(config-line)#exec-timeout 60 0

ncsrouter(config-line)#exit

ncsrouter(config)#exit

ncsrouter#copy running-config startup-config

Ввести «startup-config»

Проверим работу соединения. На любом компьютере запустим Telnet / SSH Client (на вкладке Desktop). Введем данные роутера и имя пользователя. После этого нажимаем кнопку Connect и в открывшемся терминале вводим пароль. Соединение открывается, следовательно все настроено верно:

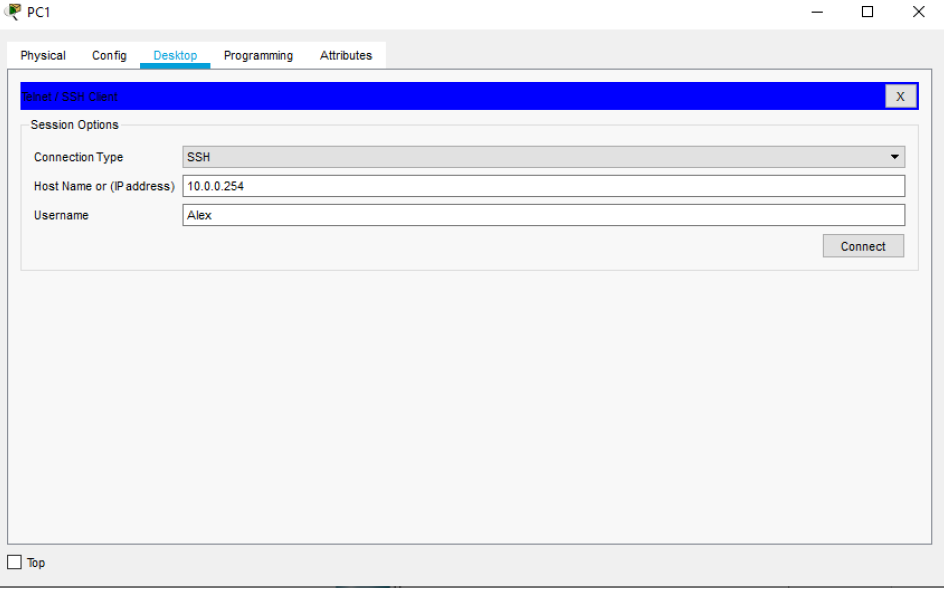


Рис.14 Подключение по SSH

# **Вывод**

Был разработан проект компьютерной сети c реализацией VLAN и успешно протестирован.