

Задание лабораторной работы

Компания арендовала 3 помещения в бизнес центре. В этих помещениях есть только голые стены и розетки. Вы друг основателя фирмы и по совместительству 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 не настроенный web сервер. Это тоже необходимо исправить. От Вас требуется реализовать в каждом помещении возможность получить 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).

Обеспечить защиту портов доступа на коммутаторах (не более 2 адресов на интерфейсе, адреса должны быть динамически сохранены в текущей конфигурации, при попытке подключения устройства с адресом, нарушающим политику, на консоль должно быть выведено уведомление, порт должен быть отключен).

Так как Вы давно дружны с директором он попросил Вас создать административную виртуальную сеть и задать ей имя KingMan.

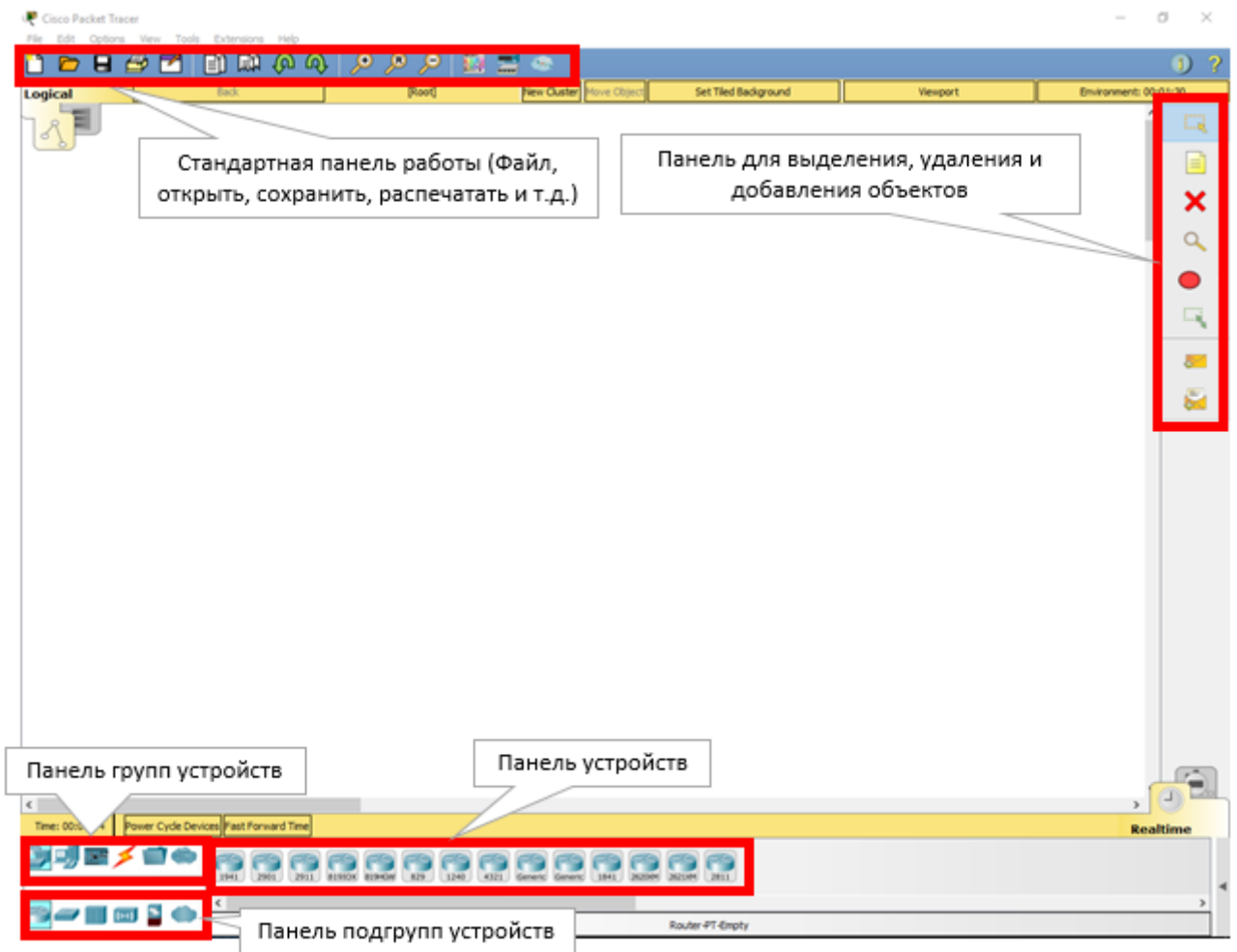
В средствах Вы ограничены. У Вас осталось с прошлой работы 3 коммутатора Cisco 2960, маршрутизатор Cisco 1941 и роутер Cisco WRT300N.

Всю работу необходимо выполнить в бесплатной программе Packet Tracer.

Инструкция по работе в Packet Tracer

Cisco Packet Tracer — это мощная программа моделирования сетей, которая позволяет системным администраторам экспериментировать с поведением сети и оценивать возможные сценарии развития событий. Этот инструмент дополняет физическое оборудование, позволяя создавать сети с практически неограниченным количеством устройств, и помогает получить практические навыки конфигурирования, поиска и устранения проблем и обнаружения устройств.

Окно программы и его структура представлены ниже.



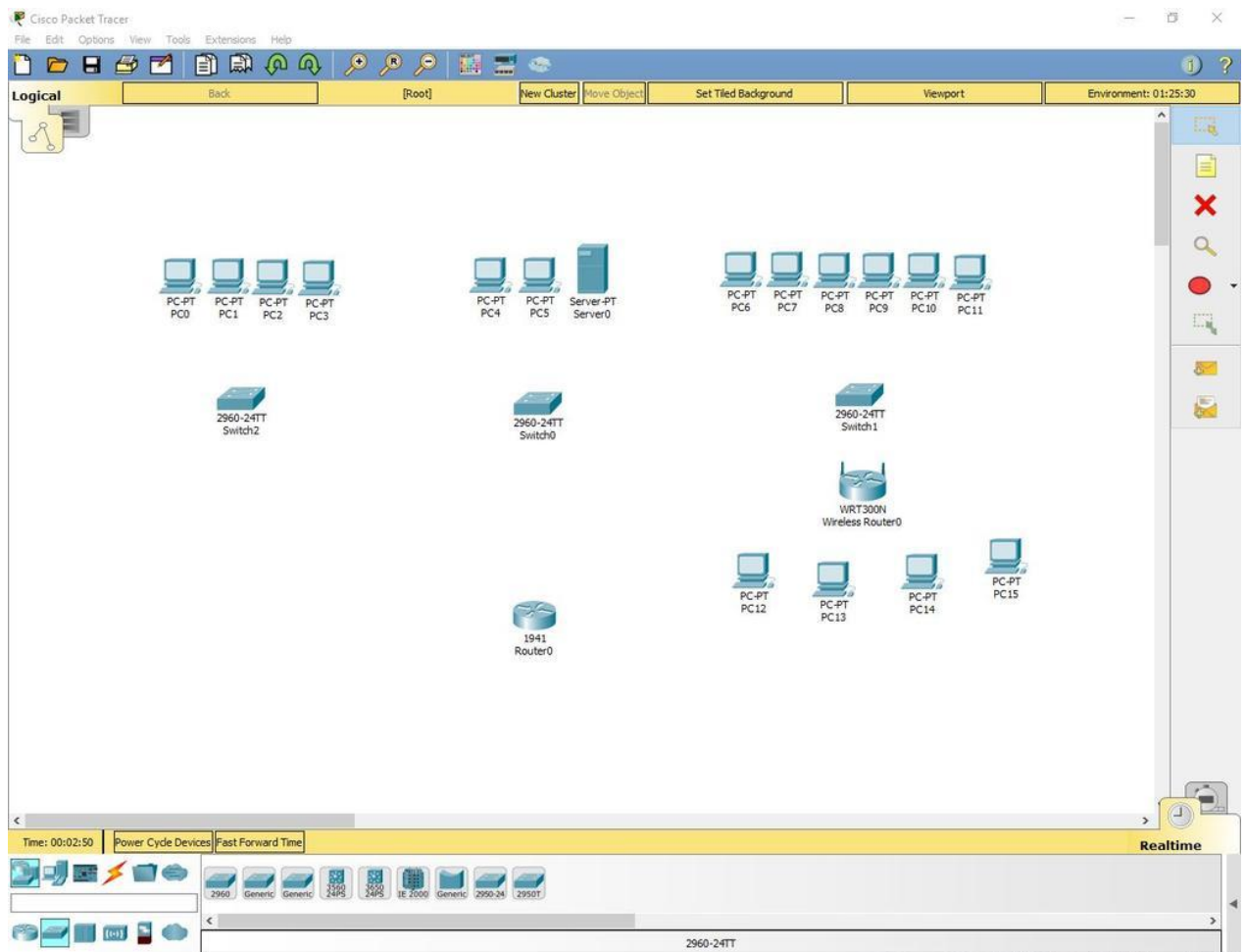
Инструкция по выполнению лабораторной работы в Packet Tracer

1. Добавление оборудования.

Открыть Packet Tracer и создать на рабочем поле:

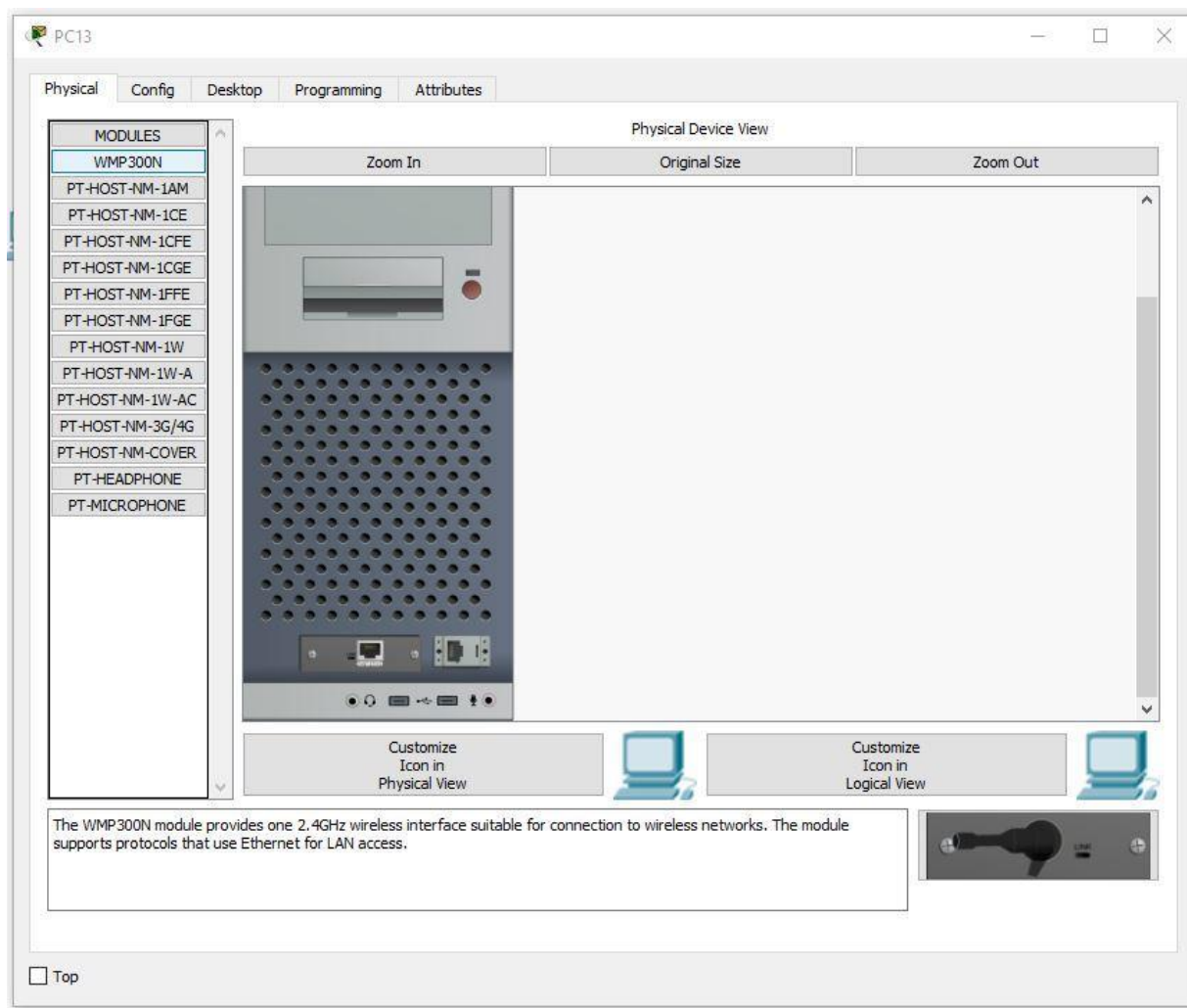
- a. 16 компьютеров
- b. Сервер
- c. 3 коммутатора Cisco 2960
- d. Маршрутизатор Cisco 1941
- e. Роутер Cisco WRT300N

Итого: 22 устройства



2. Установка Wi-Fi модуля в ПК.

У четырёх компьютеров в третьем отделе заменить LAN разъём на Wi-Fi антенну. Для этого открываем устройство, выключаем его, вынимаем старый модуль, меняем его на Wi-Fi (WMP300N) антенну. Включаем компьютер.



3. 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:

PC0

Physical Config Desktop Programming Attributes

IP Configuration

IP Configuration

☐ DHCP ☒ Static

IP Address 10.0.0.1

Subnet Mask 255.255.255.0

Default Gateway 10.0.0.254

DNS Server 20.0.0.3

IPv6 Configuration

☐ DHCP ☐ Auto Config ☒ Static

IPv6 Address /

Link Local Address FE80::2D0:BCFF:FEDE:B113

IPv6 Gateway

IPv6 DNS Server

☐ Top

Пример правильно настроенного ПК во втором отделе:

PC4

Physical Config Desktop Programming Attributes

IP Configuration

IP Configuration

☐ DHCP ☒ Static

IP Address 20.0.0.1

Subnet Mask 255.255.255.0

Default Gateway 20.0.0.254

DNS Server 20.0.0.3

IPv6 Configuration

☐ DHCP ☐ Auto Config ☒ Static

IPv6 Address /

Link Local Address FE80::2E0:F7FF:FE6C:CCA0

IPv6 Gateway

IPv6 DNS Server

☐ Top

На сервере выставим такие настройки:

Server0

Physical Config Services Desktop Programming Attributes

IP Configuration

IP Configuration

☐ DHCP ☒ Static

IP Address 20.0.0.3

Subnet Mask 255.255.255.0

Default Gateway 20.0.0.254

DNS Server 20.0.0.3

IPv6 Configuration

☐ DHCP ☐ Auto Config ☒ Static

IPv6 Address /

Link Local Address FE80::20C:CFFF:FE85:6364

IPv6 Gateway

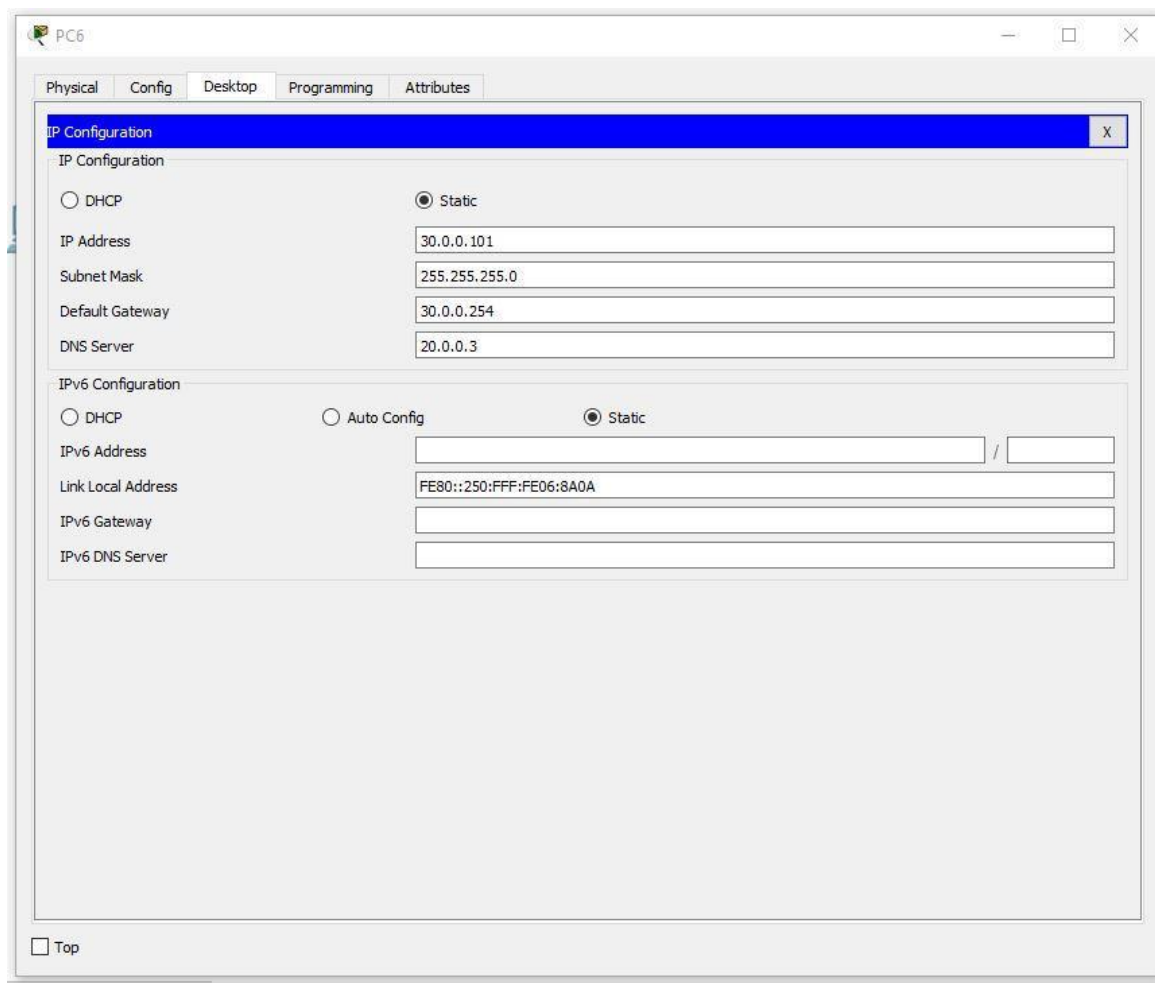
IPv6 DNS Server

☐ Top

4. Настройка третьего отдела.

Выставим IP по формуле $30.0.0.10n$, где n – номер ПК.

Пример правильно настроенного ПК в третьем отделе:



Продолжим настройку ПК. Первый IP – 30.0.0.101, а последний – 30.0.0.110

5. Настройка роутера.

Выставим настройки:

```
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
```

Скриншоты всех настраиваемых вкладок роутера:

Wireless Router0

PhysicalConfigGUIAttributes

Wireless-N Broadband Router

Firmware Version: v0.93.3

Wireless-N Broadband RouterWRT300N

SetupSetupWirelessSecurityAccess RestrictionsApplications & GamingAdministrationStatus

Basic SetupDDNSMAC Address CloneAdvanced Routing

Internet Setup

Internet Connection typeAutomatic Configuration - DHCP

Optional Settings (required by some internet service providers)

Host Name:

Domain Name:

MTU:Size: 1500

Network Setup

Router IP

IP Address:3000253

Subnet Mask:255.255.255.0

DHCP Server Settings

DHCP Server:EnabledDisabledDHCP Reservation

Start IP Address: 30.0.0.1

Maximum number of Users:20

IP Address Range: 30.0.0.1 - 20

Client Lease Time:0 minutes (0 means one day)

Static DNS 1:20003

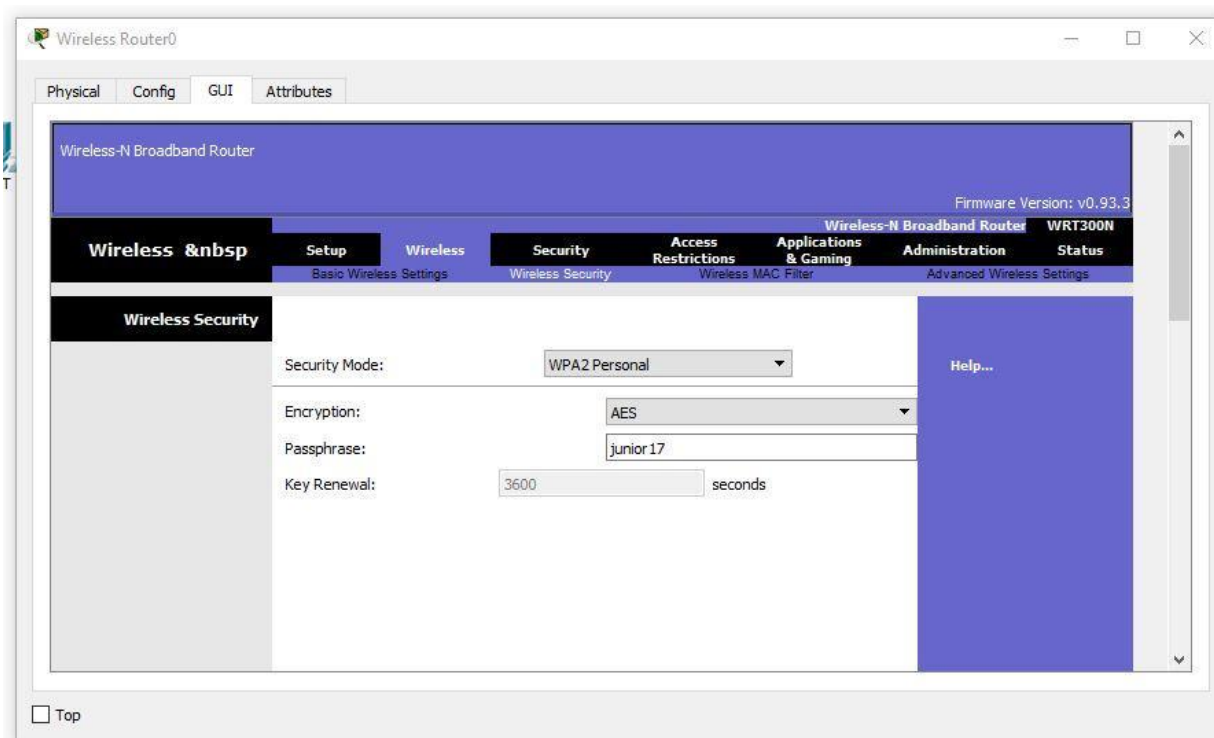
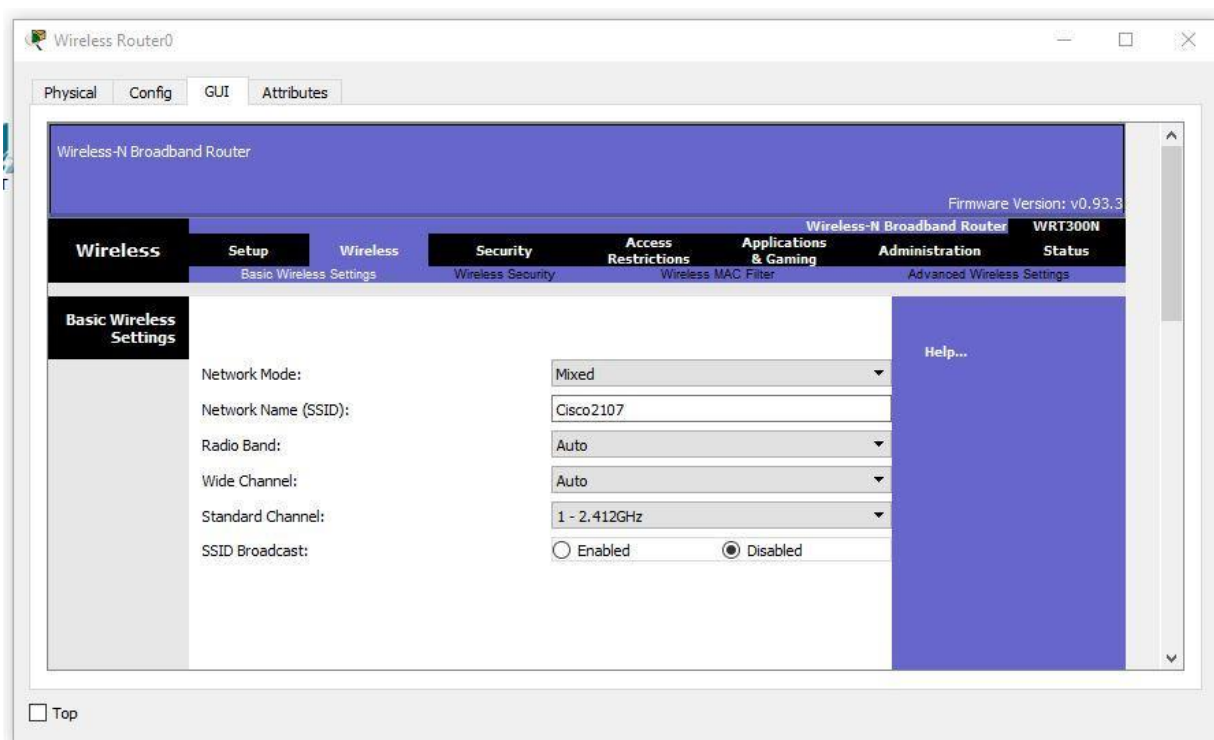
Static DNS 2:0000

Static DNS 3:0000

WINS:0000

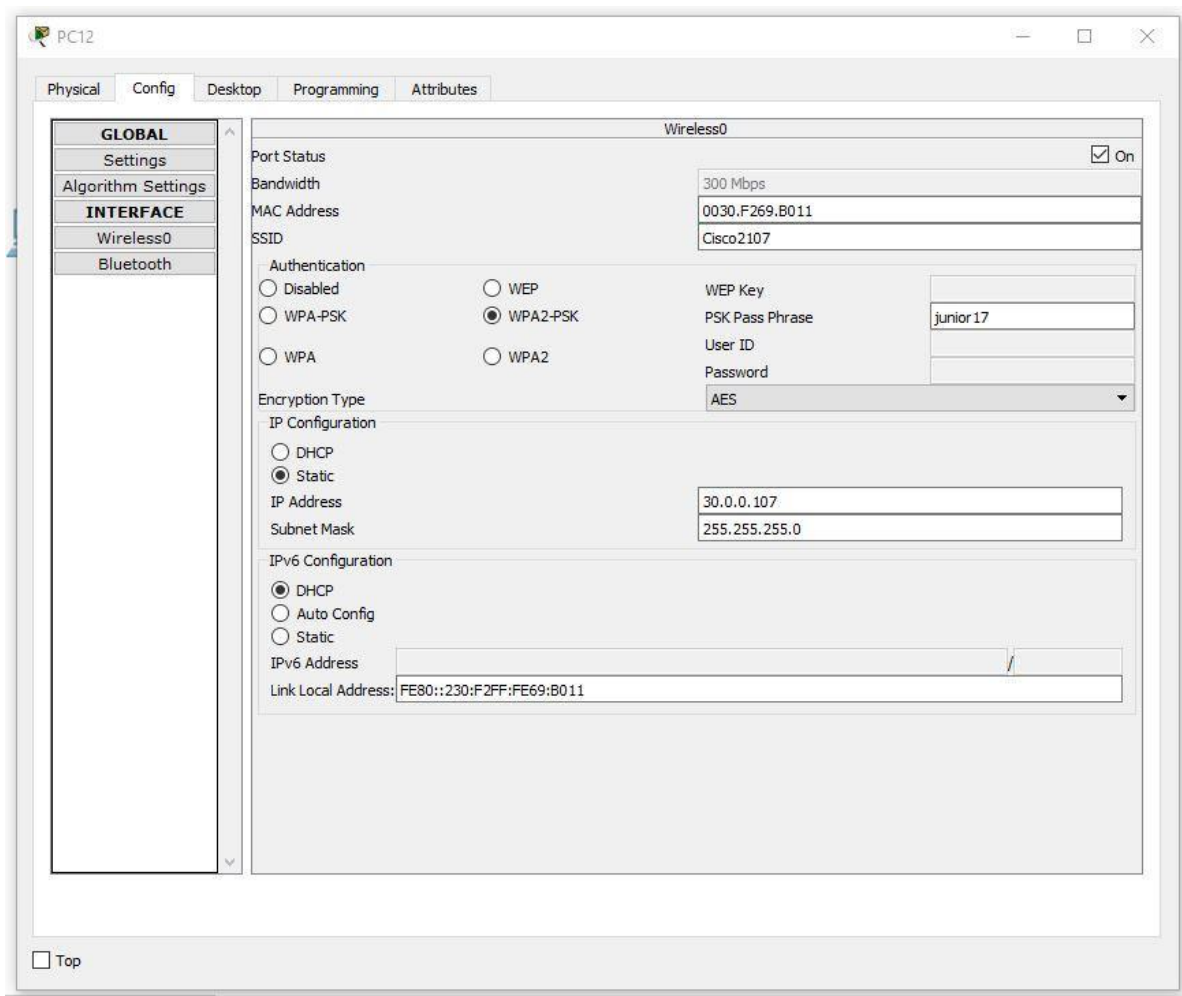
Help...

Top



Настройка беспроводных ПК. Задаём имя сети **Cisco2107** и WPA2-Personal пароль – **junior17**

Пример настроек одного из ПК:



6. Подключаем кабели и соединяем отделы.

Соединяем ПК витой парой.

Во всех коммутаторах подключаем кабели к FastEthernet по часовой стрелке. В маршрутизаторе подключимся к гигабитному разъёму, предварительно его включив.

Настраиваем VLAN на всех коммутаторах. Для этого открываем коммутатор в первом отделе. Переходим в интерфейс командной строки и вводим команды:

```
Switch>en
Switch#conf t
Switch(config)#vlan 10
Switch(config-vlan)#name Office1
Switch(config-vlan)#end
```

Рассмотрим все команды.

1. En – enable. Расширенный доступ к конфигурации
2. Conf t – Configuration terminal. Открывает терминал настройки

3. Vlan 10 – создаёт виртуальную сеть с индексом 10
4. Name Office1 – задаётся имя VLAN. Имя – Office1.
5. End – завершения настройки.

Открываем коммутатор во втором отделе и прописываем следующие команды:

```
Switch>en
Switch#conf t
Switch(config)#vlan 10
Switch(config-vlan)#name Office1
Switch(config-vlan)#exit
Switch(config)#vlan 20
Switch(config-vlan)#name Office2
Switch(config-vlan)#exit
Switch(config)#vlan 30
Switch(config-vlan)#name Office3
Switch(config-vlan)#exit
Switch(config)#end
```

Открываем коммутатор в третьем отделе и прописываем следующие команды:

```
Switch>en
Switch#conf t
Switch(config)#vlan 30
Switch(config-vlan)#name Office3
Switch(config-vlan)#end
```

Выставляем на первом коммутаторе VLAN 10 на все порты, к которым есть подключение (Fa0/1-Fa0/5).

На втором коммутаторе нужно выставить порт, к которому подключен коммутатор из первого отдела VLAN – 10, из третьего VLAN – 30, а 2 ПК и сервер второго отдела VLAN – 20. То есть Fa0/1 – VLAN 10, Fa0/2- Fa0/4 – VLAN 20, Fa0/5 – VLAN 30. Fa0/6, соединяющий коммутатор и маршрутизатор выставляем в Trunk режим.

На третьем коммутаторе нужно выставить на все порты VLAN 30 (Fa0/1-Fa0/8). Затем, производим настройку маршрутизатора для работы с VLAN.

Также, переходим во вкладку CLI и прописывает там команды:

```
Router>en
Router#conf t
Router(config)#int gig 0/0.10
Router(config-subif)#encapsulation dot1Q 10
Router(config-subif)#ip address 10.0.0.254 255.255.255.0
Router(config-subif)#exit
```

```
Router(config)#int gig 0/0.20
Router(config-subif)#encapsulation dot1Q 20
Router(config-subif)#ip address 20.0.0.254 255.255.255.0
Router(config-subif)#exit
Router(config)#int gig 0/0.30
Router(config-subif)#encapsulation dot1Q 30
Router(config-subif)#ip address 30.0.0.254 255.255.255.0
Router(config-subif)#end
```

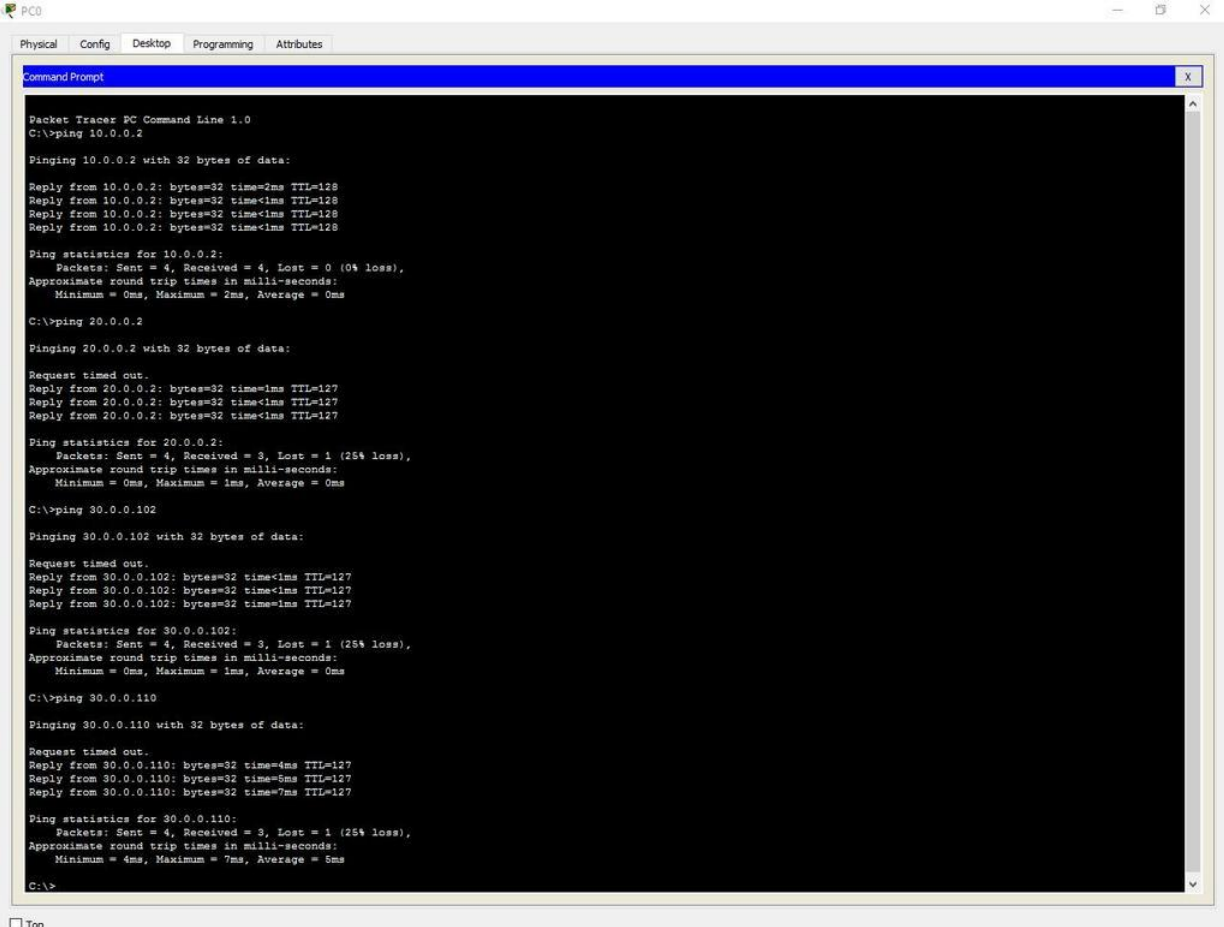
Теперь разберём команды:

1. int gig 0/0.10. Команда подключает виртуальный интерфейс для работы с разными VLAN. Цифра после точки – номер VLAN.
2. Encapsulation dot1Q 10. Команда настройки VLAN в sub. Номер после dot1Q – номер VLAN.
3. ip address 10.0.0.254 255.255.255.0. IP адрес выхода пакетов информации.

Теперь протестируем сеть командой **ping**.

Возьмём любой компьютер в каждом отделе и пропингуем все отделы (в третьем отделе проверим и проводную сеть и беспроводную).

Первый отдел



```
PC0
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 10.0.0.2

Pinging 10.0.0.2 with 32 bytes of data:

Reply from 10.0.0.2: bytes=32 time=2ms TTL=128
Reply from 10.0.0.2: bytes=32 time<1ms TTL=128
Reply from 10.0.0.2: bytes=32 time<1ms TTL=128
Reply from 10.0.0.2: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 2ms, Average = 0ms

C:\>ping 20.0.0.2

Pinging 20.0.0.2 with 32 bytes of data:

Request timed out.
Reply from 20.0.0.2: bytes=32 time<1ms TTL=127
Reply from 20.0.0.2: bytes=32 time<1ms TTL=127
Reply from 20.0.0.2: bytes=32 time<1ms TTL=127

Ping statistics for 20.0.0.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 30.0.0.102

Pinging 30.0.0.102 with 32 bytes of data:

Request timed out.
Reply from 30.0.0.102: bytes=32 time<1ms TTL=127
Reply from 30.0.0.102: bytes=32 time<1ms TTL=127
Reply from 30.0.0.102: bytes=32 time<1ms TTL=127

Ping statistics for 30.0.0.102:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 30.0.0.110

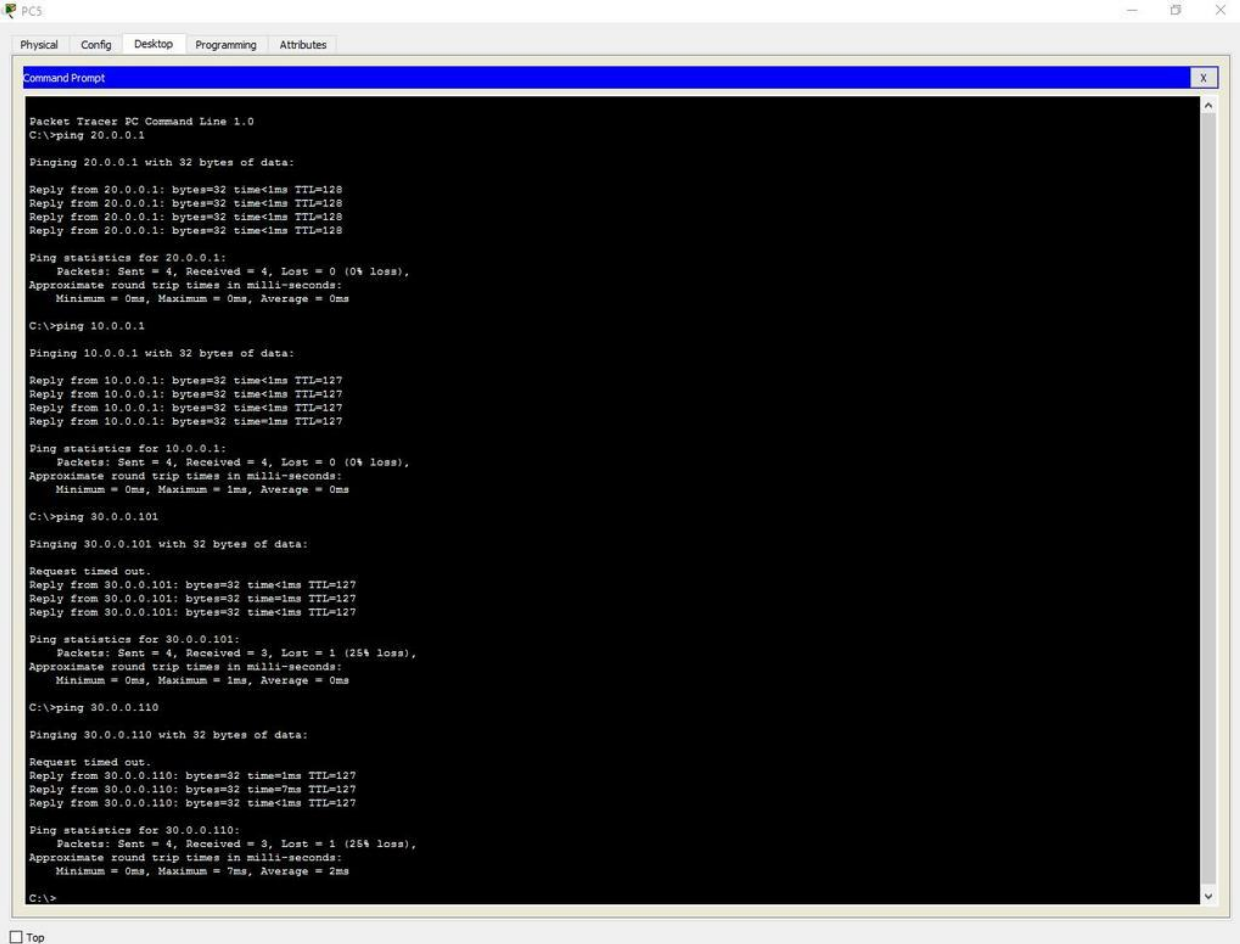
Pinging 30.0.0.110 with 32 bytes of data:

Request timed out.
Reply from 30.0.0.110: bytes=32 time=4ms TTL=127
Reply from 30.0.0.110: bytes=32 time=5ms TTL=127
Reply from 30.0.0.110: bytes=32 time=7ms TTL=127

Ping statistics for 30.0.0.110:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 4ms, Maximum = 7ms, Average = 5ms

C:\>
```

Второй отдел



Packet Tracer PC Command Line 1.0
C:\>ping 20.0.0.1

Pinging 20.0.0.1 with 32 bytes of data:

Reply from 20.0.0.1: bytes=32 time<1ms TTL=128
Reply from 20.0.0.1: bytes=32 time<1ms TTL=128
Reply from 20.0.0.1: bytes=32 time<1ms TTL=128
Reply from 20.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 20.0.0.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 10.0.0.1

Pinging 10.0.0.1 with 32 bytes of data:

Reply from 10.0.0.1: bytes=32 time<1ms TTL=127
Reply from 10.0.0.1: bytes=32 time<1ms TTL=127
Reply from 10.0.0.1: bytes=32 time<1ms TTL=127
Reply from 10.0.0.1: bytes=32 time<1ms TTL=127

Ping statistics for 10.0.0.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 30.0.0.101

Pinging 30.0.0.101 with 32 bytes of data:

Request timed out.
Reply from 30.0.0.101: bytes=32 time<1ms TTL=127
Reply from 30.0.0.101: bytes=32 time<1ms TTL=127
Reply from 30.0.0.101: bytes=32 time<1ms TTL=127

Ping statistics for 30.0.0.101:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 30.0.0.110

Pinging 30.0.0.110 with 32 bytes of data:

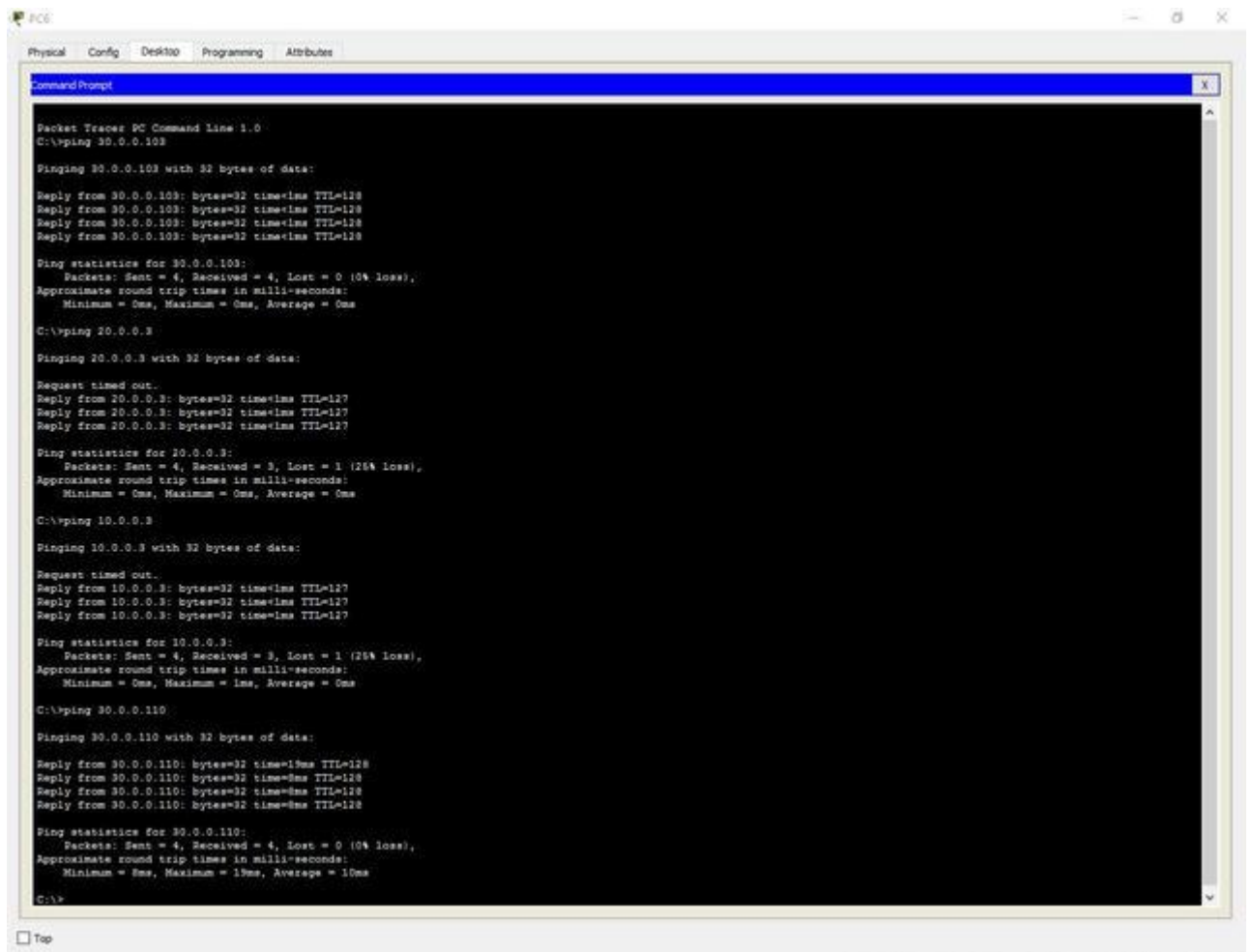
Request timed out.
Reply from 30.0.0.110: bytes=32 time<1ms TTL=127
Reply from 30.0.0.110: bytes=32 time=7ms TTL=127
Reply from 30.0.0.110: bytes=32 time<1ms TTL=127

Ping statistics for 30.0.0.110:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 7ms, Average = 2ms

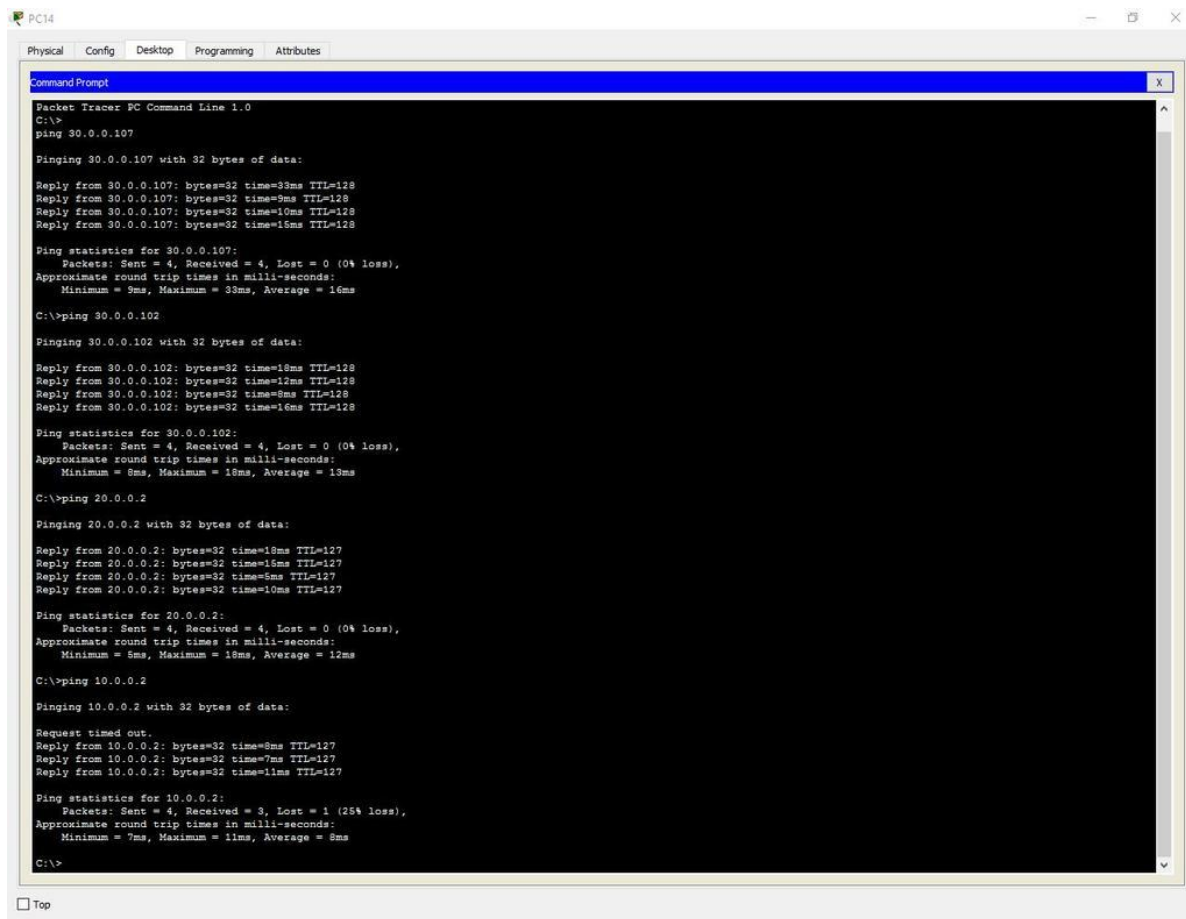
C:\>

☐ Top

Третий отдел (кабель)



Третий отдел (Wi-Fi)



```
Packet Tracer PC Command Line 1.0
C:\>
ping 30.0.0.107

Pinging 30.0.0.107 with 32 bytes of data:

Reply from 30.0.0.107: bytes=32 time=33ms TTL=128
Reply from 30.0.0.107: bytes=32 time=9ms TTL=128
Reply from 30.0.0.107: bytes=32 time=10ms TTL=128
Reply from 30.0.0.107: bytes=32 time=15ms TTL=128

Ping statistics for 30.0.0.107:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 9ms, Maximum = 33ms, Average = 16ms

C:\>ping 30.0.0.102

Pinging 30.0.0.102 with 32 bytes of data:

Reply from 30.0.0.102: bytes=32 time=18ms TTL=128
Reply from 30.0.0.102: bytes=32 time=12ms TTL=128
Reply from 30.0.0.102: bytes=32 time=8ms TTL=128
Reply from 30.0.0.102: bytes=32 time=16ms TTL=128

Ping statistics for 30.0.0.102:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 8ms, Maximum = 18ms, Average = 13ms

C:\>ping 20.0.0.2

Pinging 20.0.0.2 with 32 bytes of data:

Reply from 20.0.0.2: bytes=32 time=18ms TTL=127
Reply from 20.0.0.2: bytes=32 time=15ms TTL=127
Reply from 20.0.0.2: bytes=32 time=8ms TTL=127
Reply from 20.0.0.2: bytes=32 time=10ms TTL=127

Ping statistics for 20.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 8ms, Maximum = 18ms, Average = 12ms

C:\>ping 10.0.0.2

Pinging 10.0.0.2 with 32 bytes of data:

Request timed out.
Reply from 10.0.0.2: bytes=32 time=8ms TTL=127
Reply from 10.0.0.2: bytes=32 time=7ms TTL=127
Reply from 10.0.0.2: bytes=32 time=11ms TTL=127

Ping statistics for 10.0.0.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 7ms, Maximum = 11ms, Average = 8ms

C:\>
```

Добавляем административный VLAN (40 — Management).

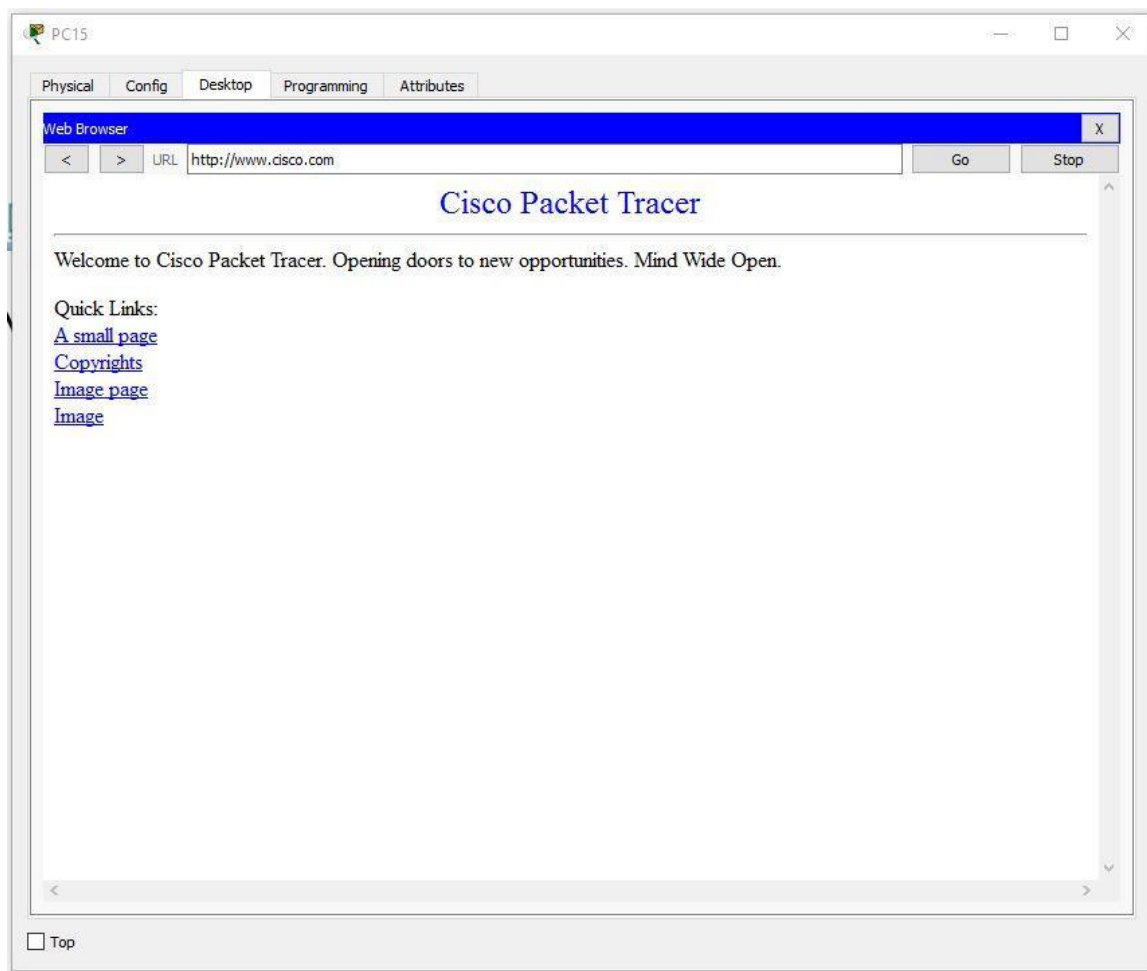
7. Настройка сервера.

Включаем DNS.

Name — www.cisco.com.

Address – 20.0.0.3.

Проверим возможность выхода на сайт из любого отдела. Вводим URL имя в браузере и нажимаем Go.



8. Настроим SSH.

Для этого заходим в маршрутизатор и пишем команды:

```
Router>en
Router#clock set 10:10:00 13 Oct 2017
Router#conf t
Router(config)#ip domain name ssh.dom
Router(config)#crypto key generate rsa
Router(config)#service password-encryption
Router(config)#username Valery privilege 15 password 8 junior17
Router(config)#aaa new-model
Router(config)#line vty 0 4
Router(config-line)#transport input ssh
Router(config-line)#logging synchronous
Router(config-line)#exec-timeout 60 0
Router(config-line)#exit
Router(config)#exit
Router#copy running-config startup-config
```

Разберём каждую команду:

1. clock set 10:10:00 13 Oct 2017. Устанавливаем точное время для генерации ключа.

2. `ip domain name ssh.dom`. Указываем имя домена (необходимо для генерации ключа).
3. `crypto key generate rsa`. Генерируем RSA ключ (необходимо будет выбрать размер ключа).
4. `service password-encryption`. Активируем шифрование паролей в конфигурационном файле.
5. `username Valery privilege 15 password 8 junior17`. Заводим пользователя с именем Valery, паролем junior17 и уровнем привилегий 15.
6. `aaa new-model`. Активируем протокол AAA (до активации AAA в системе обязательно должен быть заведен хотя бы один пользователь).
7. `line vty 0 4`. Входим в режим конфигурирования терминальных линий с 0 по 4.
8. `transport input ssh`. Указываем средой доступа через сеть по умолчанию SSH.
9. `logging synchronous`. Активируем автоматическое поднятие строки после ответа системы на сделанные изменения.
10. `exec-timeout 60 0`. Указываем время таймаута до автоматического закрытия SSH сессии в 60 минут.
11. `copy running-config startup-config`. Сохраняем конфигурационный файл в энергонезависимую память. (Здесь выведется строка «Destination filename [startup-config]?» Вводим «startup-config»).

9. Настроим защиту портов на каждом коммутаторе.

Для этого открываем коммутатор и пишем команды:

```
Switch>en
Switch#conf t
Switch(config)#interface range fastEthernet 0/X-Y
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport port-security
Switch(config-if-range)#switchport port-security maximum K
Switch(config-if-range)#switchport port-security mac-address sticky
Switch(config-if-range)#switchport port-security violation shutdown
Switch(config-if-range)#end
```

Разберём каждую команду:

1. `Interface range fastEthernet 0/X-Y`. Выбор диапазона интерфейсов (X – первый нужный порт, Y – последний).

ВНИМАНИЕ! Выбирайте порты которые **НЕ** активны в подключениях!

2. `switchport mode access`. Переводим порт в access режим.
3. `switchport port-security`. Включаем защиту портов.
4. `switchport port-security maximum K`. Ограничиваем число MAC-адресов на интерфейсе (K – число портов).

5. switchport port-security mac-address sticky. Выбираем способ изучения MAC-адресов коммутатором (есть статический (mac-address) и динамический (sticky)).
6. switchport port-security violation shutdown. Задаем тип реагирования на превышение числа разрешенных MAC-адресов (бывают protect – после переполнения все пакеты, отправленные с других MAC-адресов отбрасываются, restrict – то же самое, но с уведомлением в syslog или по SNMP, shutdown – порт выключается до автоматического или ручного его поднятия, также отправляются уведомления).

В итоге работа выполнена так:

