HDU-ITMO Joint Institute

杭州电子科技大学 圣光机联合学院

NETWORK PROTOCOLS

COURSE PROTOCOLS

A COMPLEX NETWORK MODELING

Instructors

Elena Boldyreva, Associate Professor eaboldyreva@itmo.ru

Yuriy Boldyrev, Assistant Professor

HDU-ITMO Joint Institute
杭州电子科技大学 圣光机联合学院

PREREQUISITES

1. Computer Networking: A Top-Down Approach, 7th ed., J.F. Kurose and K.W. Ross (Chapter 1 and Chapter 2)

REPORT

After completion the task the students need to submit:

- **The format of the report file is *pdf*.**
- Upload reports for the GitLab repository (to your personal project)
- Do not forget to write your name and ID inside the report

HDU-ITMO Joint Institute
杭州电子科技大学 圣光机联合学院

Task:

The company rented 3 premises in the business center. In these rooms there are only bare walls and sockets. You are a friend of the founder of the company and part-time network and system administrator. You were asked to develop a network diagram.

The network should be able to communicate with any of the three premises in the company, but each room (department) should be isolated.

It is also necessary to create a wireless access point in the third room. This point should have the password junior17, the first 20 addresses should be automatically issued, the SSID should be hidden.

In the second department there is an unconfigured web server. This also needs to be fixed. You are required to implement in each room the ability to access the server by url name.

There are 4 workstations in the first department, 2 workstations and a server in the second, the third room is needed for staff rest (10 workstations, including 4 wireless ones).

You need to provide secure remote access (SSH) to the network equipment.

Ensure the protection of access ports on switches (no more than 2 addresses on the interface, addresses must be dynamically stored in the current configuration, when trying to connect a device with an address that violates the policy, a notification must be displayed on the console, the port must be disabled).

Since you have been friends with the director for a long time, he asked you to create an administrative virtual network and give it the name “HDUMan”.

You have 3 Cisco 2960 switches, a Cisco 1941 (1841) router and a Cisco WRT300N router.

HDU-ITMO Joint Institute
杭州电子科技大学 圣光机联合学院

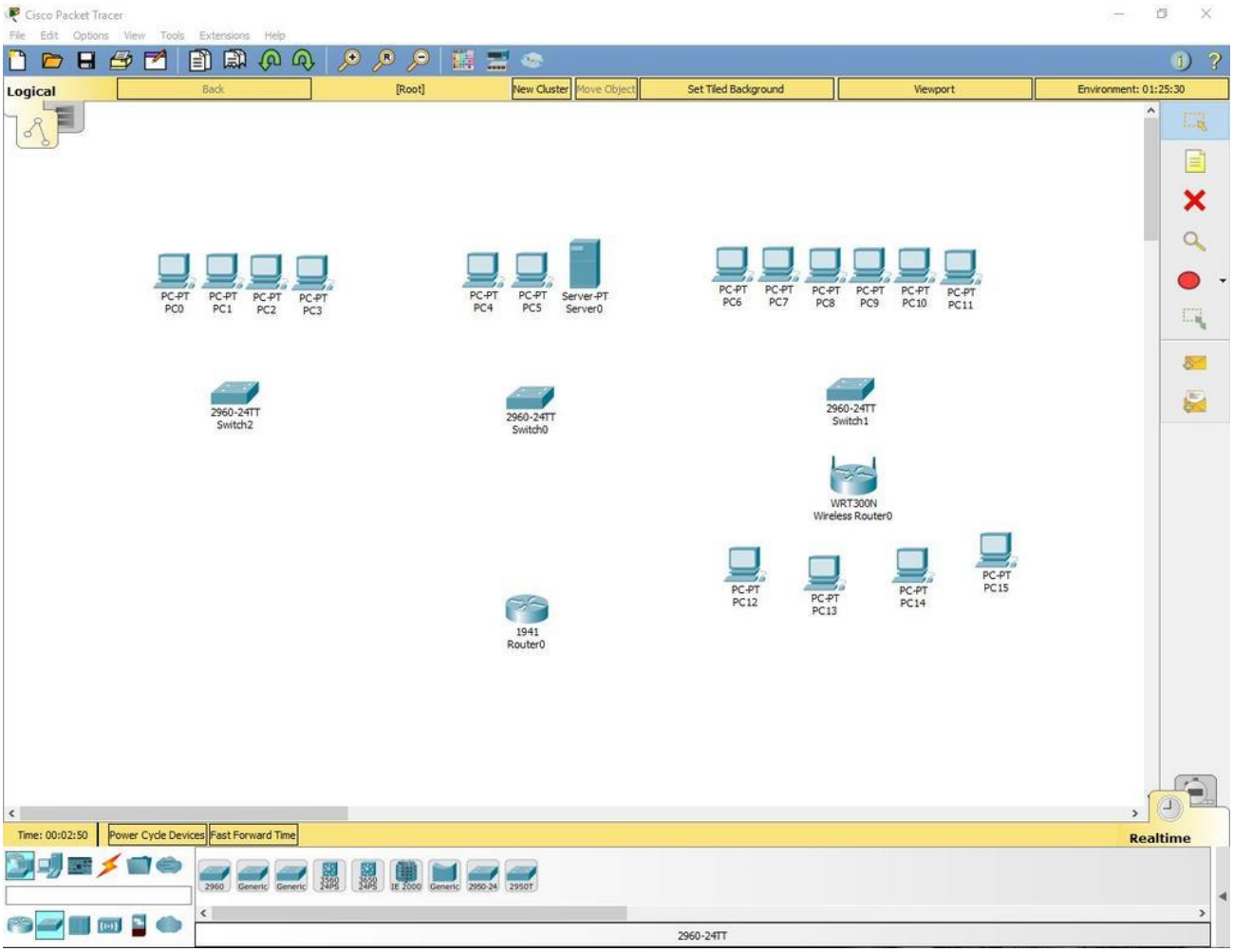
Instructions step-by-step:

1. Adding equipment.

Open Packet Tracer and create on the work field:

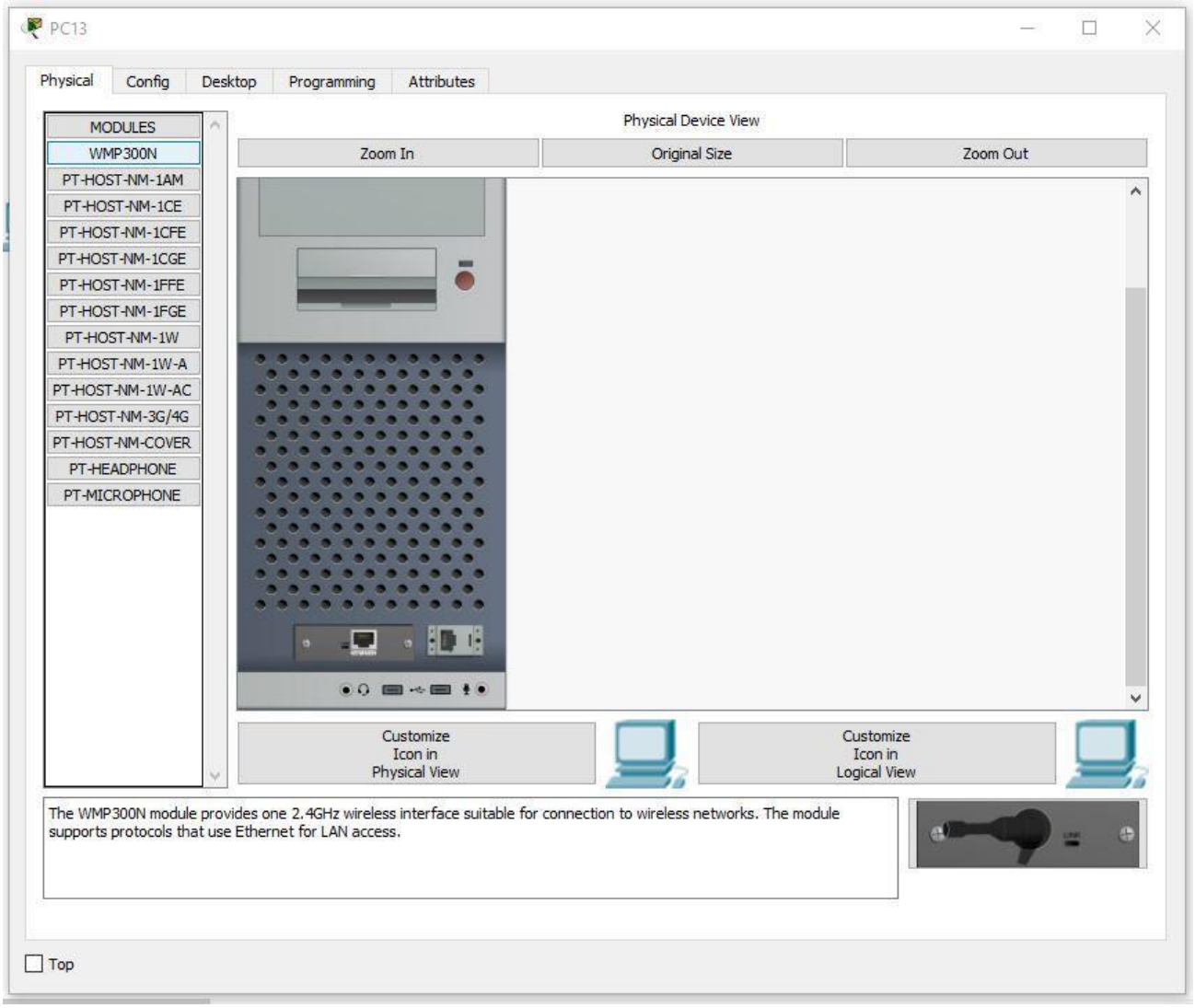
- 16 computers
- Server
- 3 Cisco 2960 switches
- Cisco 1941 Router
- Cisco WRT300N router

Total: 22 devices



2. Installing the Wi-Fi module in the PC.

Four computers in the third department have to replace the LAN connector with a Wi-Fi antenna. To do this, open the device, turn it off, take out the old module, change it to a Wi-Fi (WMP300N) antenna. Turn on the computer.

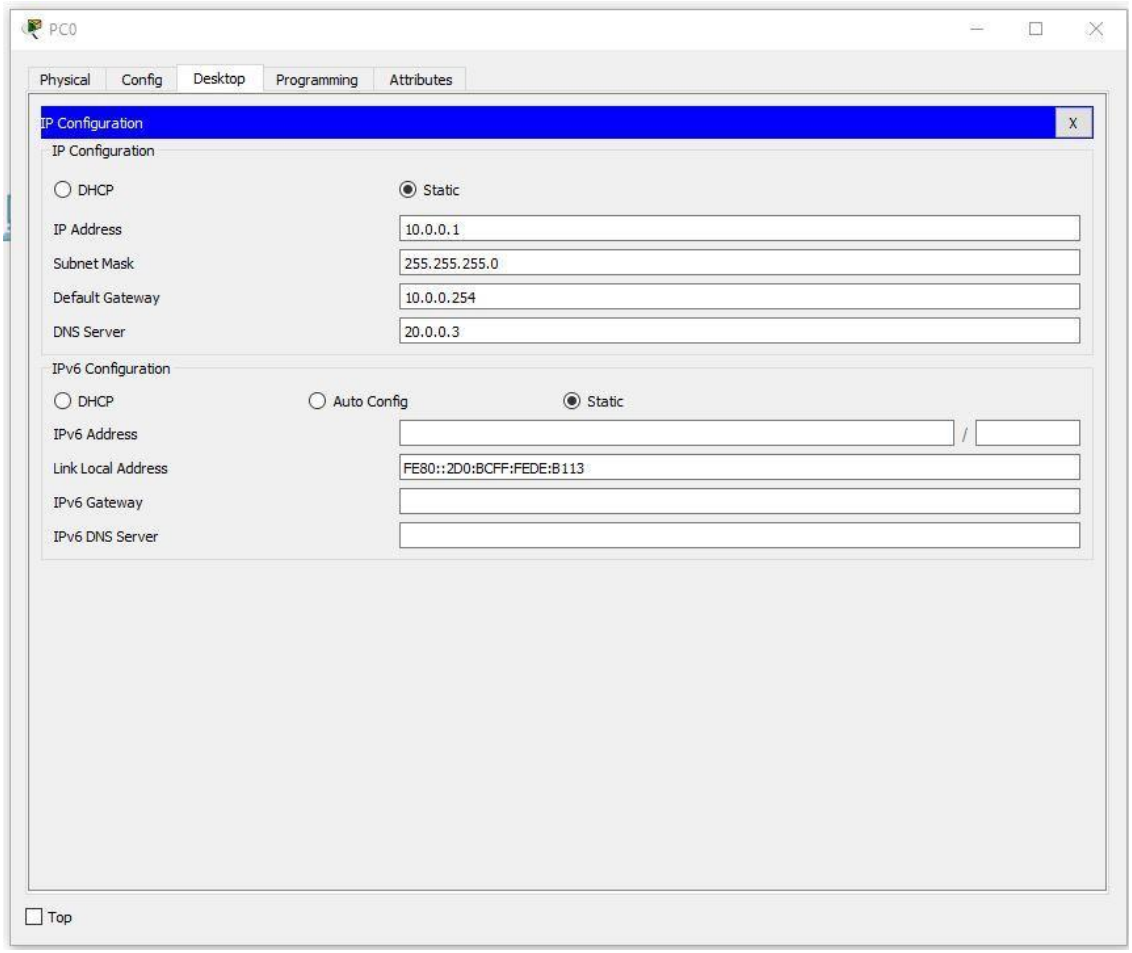


3. Setting up the PCs of the first and second departments.

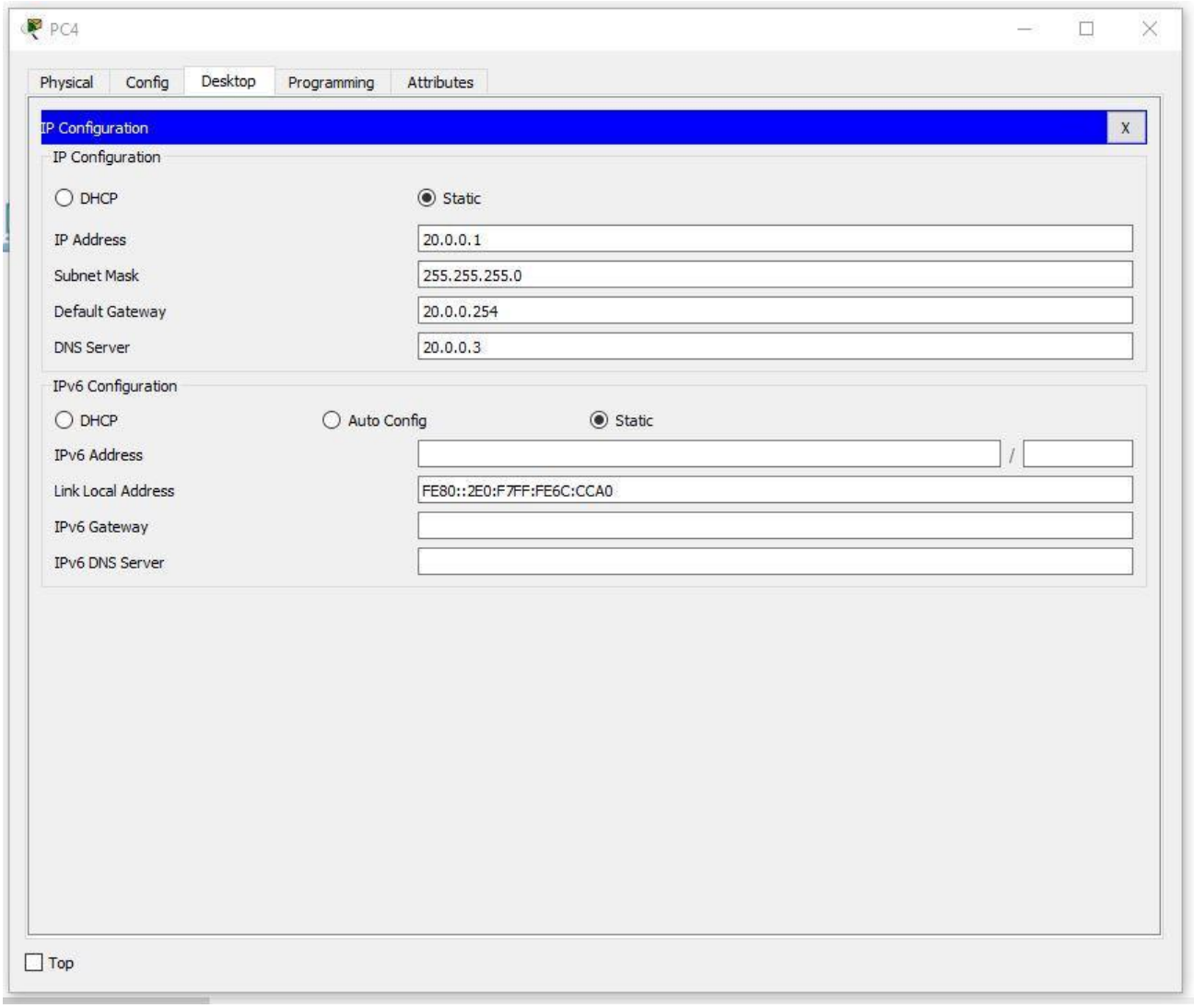
We will assign values to each computer in the first and second departments, as well as to the server, according to the formula: N0.0.0.n, where N is the department number and n is the device number (for example, 10.0.0.2 is the second computer on the first floor). The server, since it is the third device on the second floor, will have the address 20.0.0.3.

- The subnet mask will be set to 255.255.255.0.
- Default Gateway will be set to N0.0.0.254.
- DNS Server will be set to 20.0.0.3.

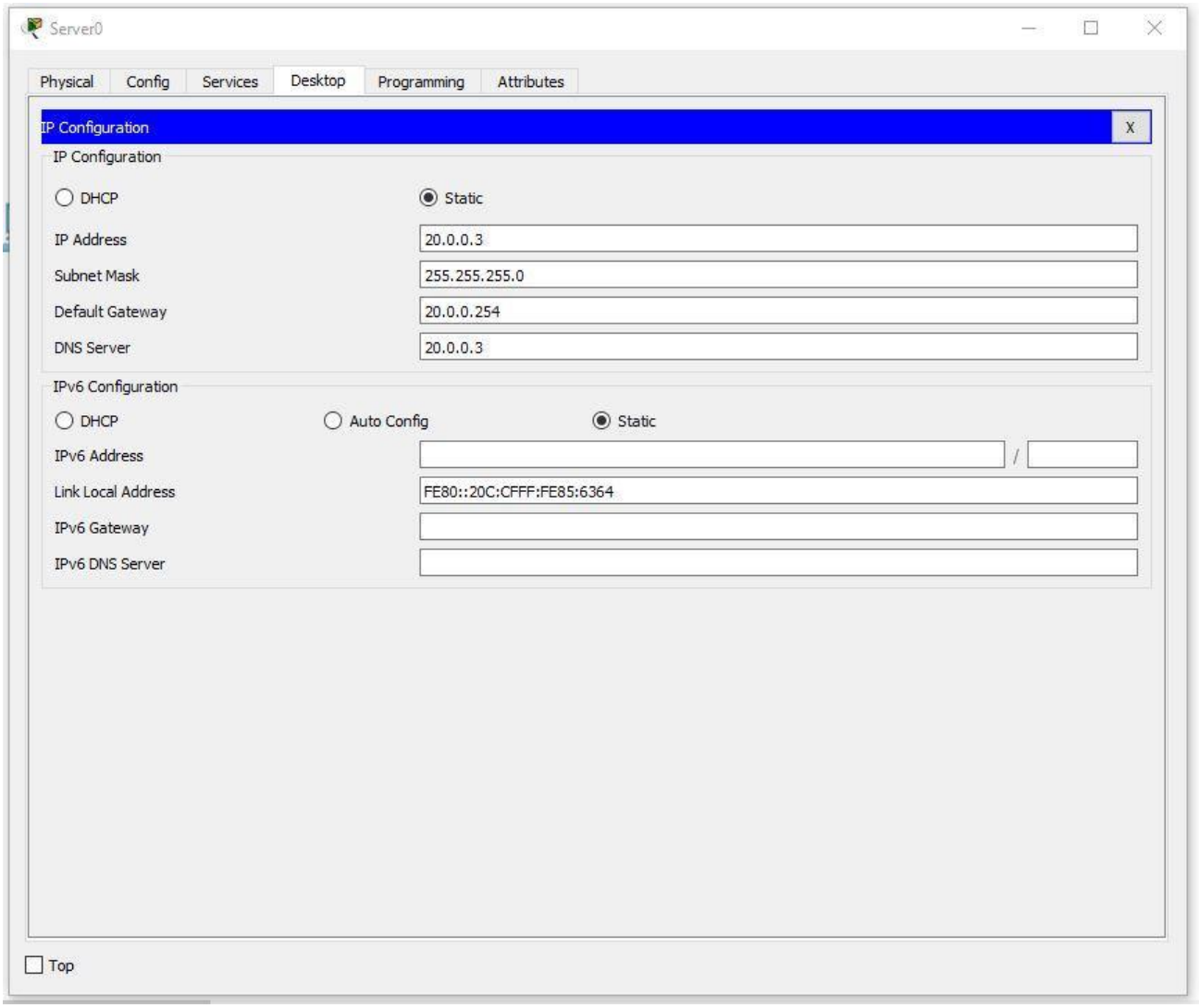
Example of a properly configured PC in the first department:



Example of a properly configured PC in the second department:


PC4
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
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

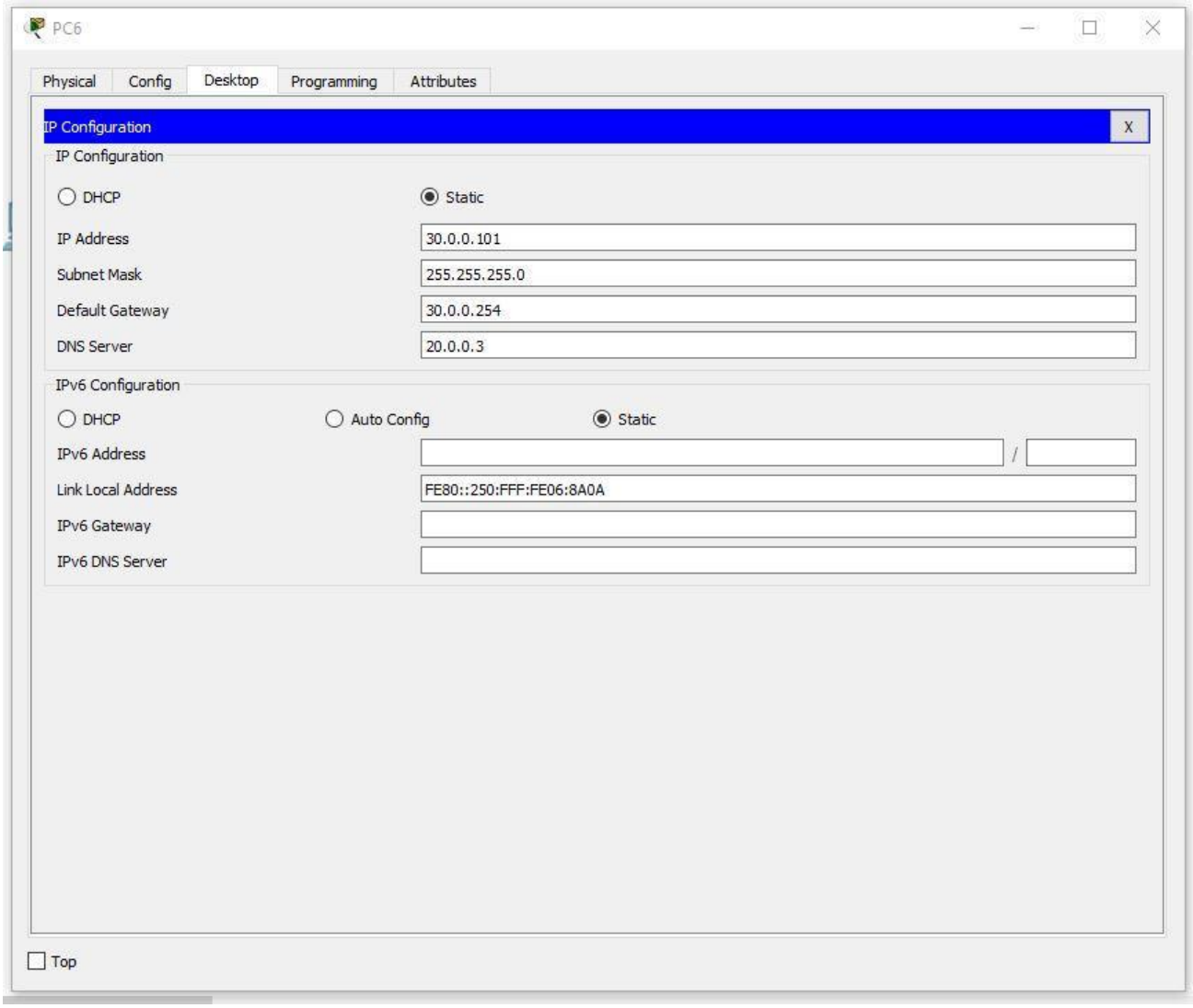
We will set the following settings on the server:



4. Setting up the third department.

We will set the IP according to the formula 30.0.0.10n, where n is the PC number.

Example of a properly configured PC in the third department:



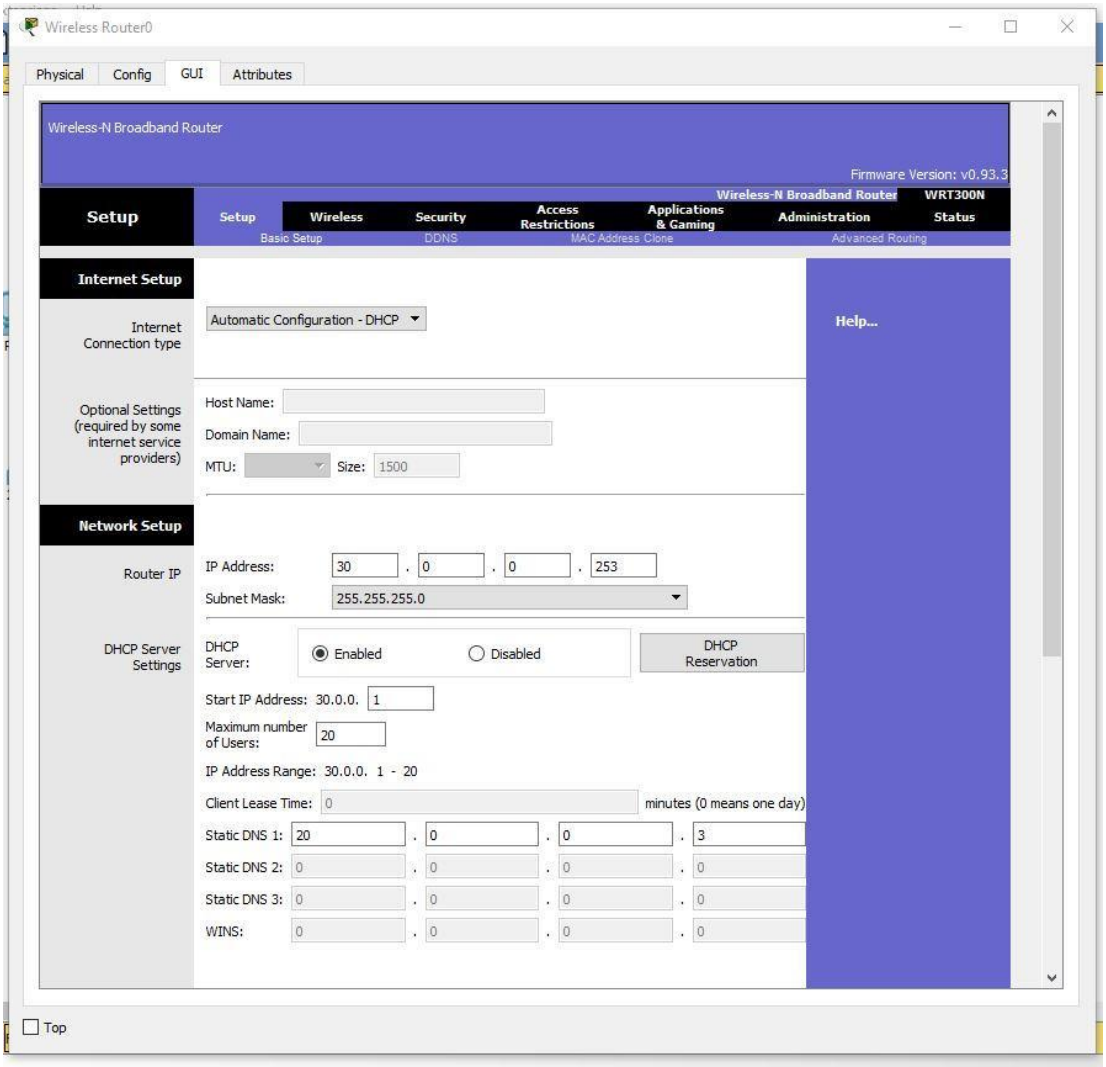
Let's continue setting up the PC. The first IP is 30.0.0.101 and the last one is 30.0.0.110.

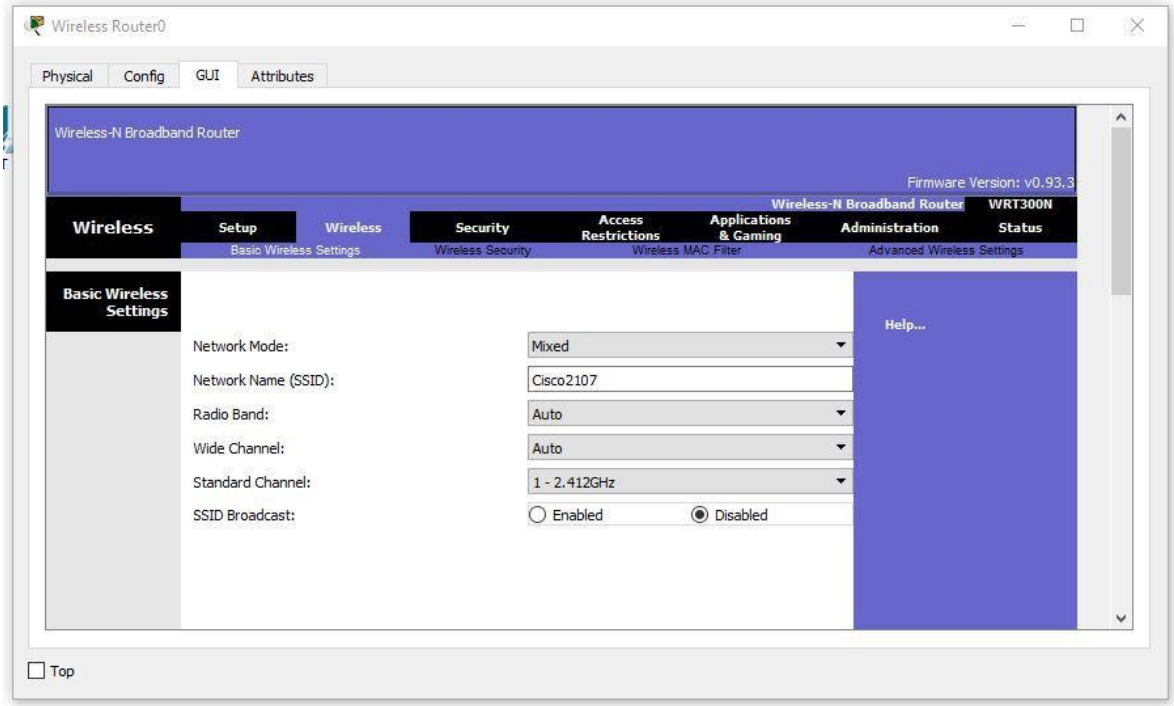
5. Configuring the router.

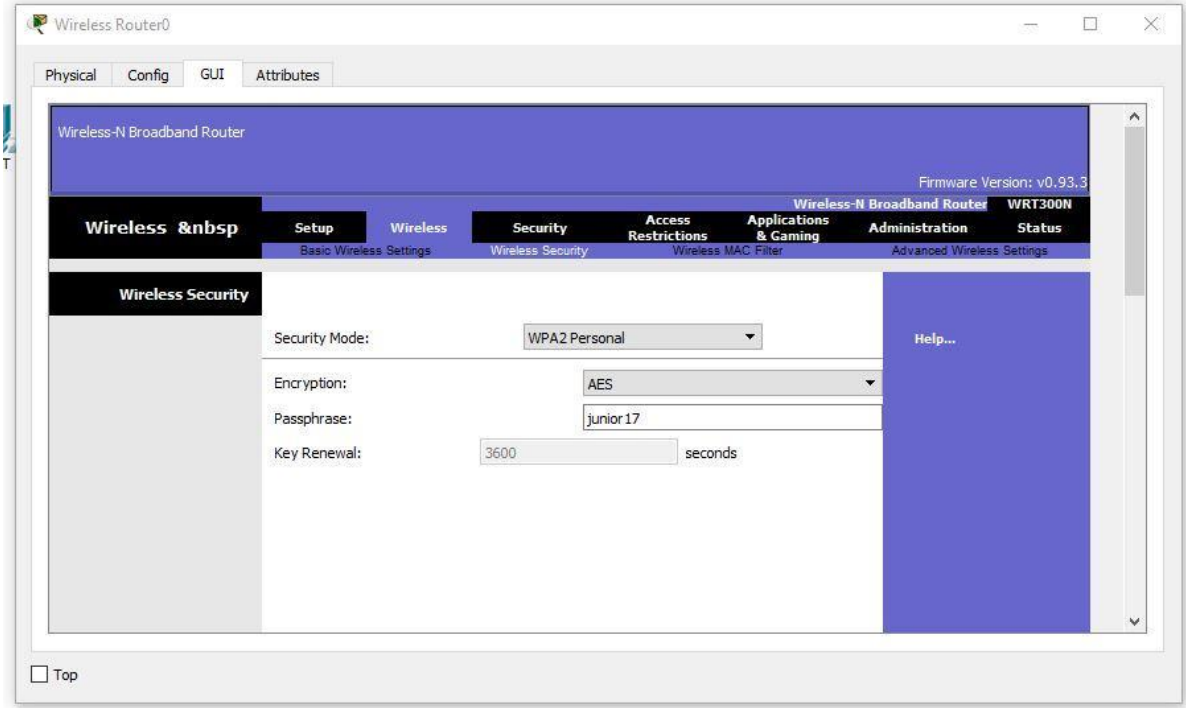
Let's set the settings:

```
IP - 30.0.0.253
Mask - 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
```

Screenshots of all configurable router tabs:

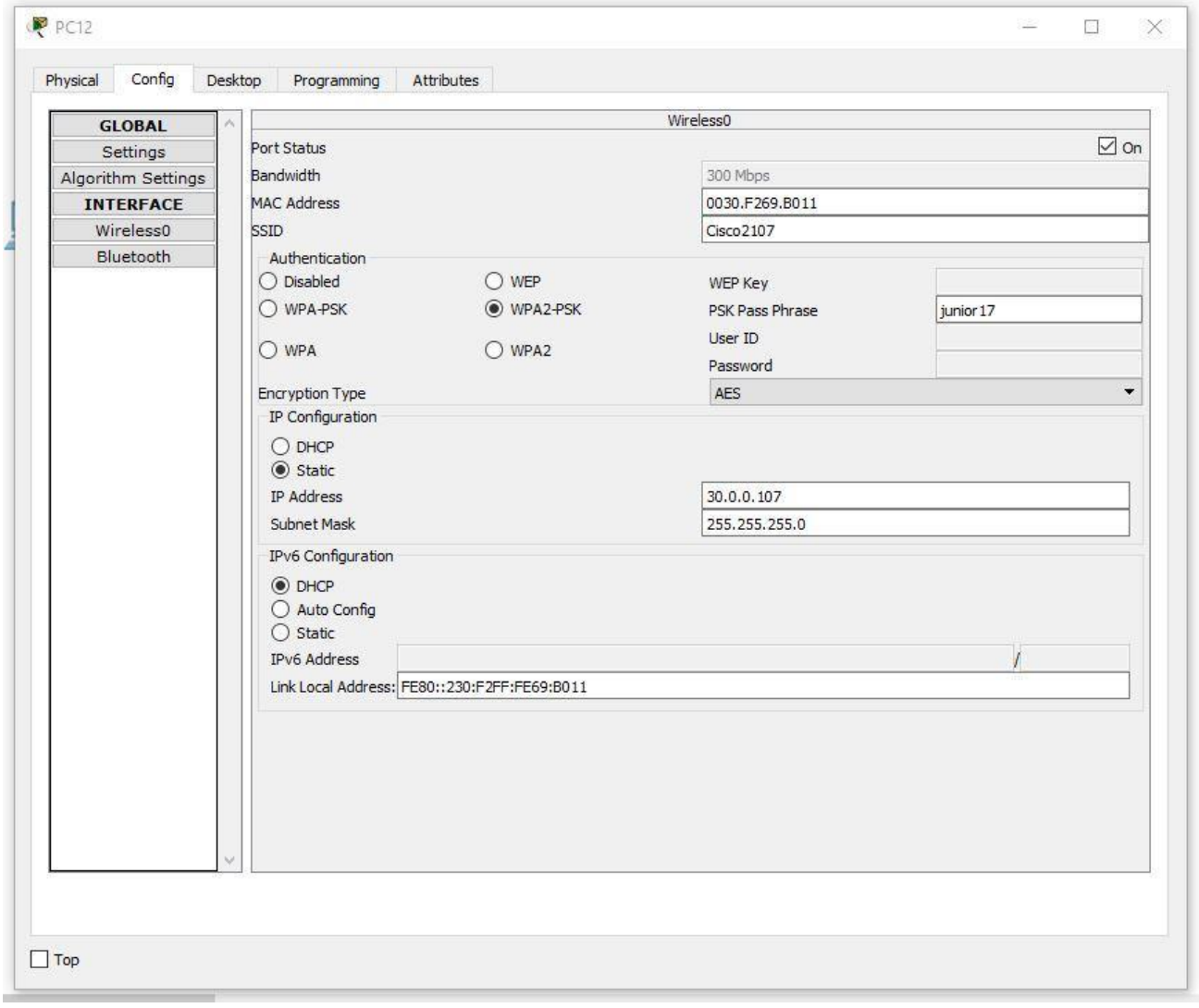

Wireless Router0
Physical
Config
GUI
Attributes
Wireless-N Broadband Router
Firmware Version: v0.93.3
Setup
Setup
Wireless
Security
Access Restrictions
Applications & Gaming
Administration
Status
Basic Setup
DDNS
MAC Address Clone
Advanced Routing
Wireless-N Broadband Router WRT300N
Internet Setup
Internet Connection type
Automatic Configuration - DHCP
Help...
Optional Settings (required by some internet service providers)
Host Name:
Domain Name:
MTU:
Size: 1500
Network Setup
Router IP
IP Address: 30 . 0 . 0 . 253
Subnet Mask: 255.255.255.0
DHCP Server Settings
DHCP Server:
Enabled
Disabled
DHCP 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: 20 . 0 . 0 . 3
Static DNS 2: 0 . 0 . 0 . 0
Static DNS 3: 0 . 0 . 0 . 0
WINS: 0 . 0 . 0 . 0
Top


Wireless Router0
Physical
Config
GUI
Attributes
Wireless-N Broadband Router
Firmware Version: v0.93.3
Wireless-N Broadband Router WRT300N
Wireless
Setup
Wireless
Security
Access Restrictions
Applications & Gaming
Administration
Status
Basic Wireless Settings
Wireless Security
Wireless MAC Filter
Advanced Wireless Settings
Basic Wireless Settings
Help...
Network Mode:
Mixed
Network Name (SSID):
Cisco2107
Radio Band:
Auto
Wide Channel:
Auto
Standard Channel:
1 - 2.412GHz
SSID Broadcast:
Enabled
Disabled
Top


Wireless Router0
Physical
Config
GUI
Attributes
Wireless-N Broadband Router
Firmware Version: v0.93.3
Wireless-N Broadband Router WRT300N
Wireless
Setup
Wireless
Security
Access Restrictions
Applications & Gaming
Administration
Status
Basic Wireless Settings
Wireless Security
Wireless MAC Filter
Advanced Wireless Settings
Wireless Security
Help...
Security Mode:
WPA2 Personal
Encryption:
AES
Passphrase:
junior17
Key Renewal:
3600
seconds
Top

Setting up wireless PCs. We set the network name **Cisco2107** and WPA2-Personal password – **junior17**

An example of the settings of one of the PCs:



6. Connect the cables and connect the departments.

We connect the PC with a twisted pair.

In all switches, we connect the cables to FastEthernet clockwise. In the router, we will connect to the gigabit connector, having previously turned it on.

We configure VLANs on all switches. To do this, open the switchboard in the first department. Go to the command line interface and enter the commands:

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

Consider all the commands.

```
 En – enable. Advanced Configuration access
Conf t – Configuration terminal. Opens the settings terminal
Vlan 10 – creates a virtual network with the index 10
Name Office1 – the VLAN name is set. The name is Office1.
 End – completion of the configuration.
```

Open the switchboard in the second department and write the following commands:

```
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
```

Open the switchboard in the third department and write the following commands:

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

We set VLAN 10 on the first switch for all ports to which there is a connection (Fa0/1-Fa0/5).

On the second switch, you need to set the port to which the switch from the first department of VLAN – 10 is connected, from the third VLAN – 30, and 2 PCs and the server of the second department of VLAN – 20. That is, Fa0/1 – VLAN 10, Fa0/2- Fa0/4 – VLAN 20, Fa0/5 – VLAN 30. Fa0/6, connecting the switch and the router are set to Trunk mode.

On the third switch, you need to set VLAN 30 (Fa0/1-Fa0/8) to all ports.

Then, we will configure the router to work with the VLAN.

Also, go to the CLI tab and prescribes commands there:

```
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
```

If you don’t have 1941 model of main router:

```
Router>en
Router#conf t
Router(config)#int fast 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
```

Now let 's analyze the commands:

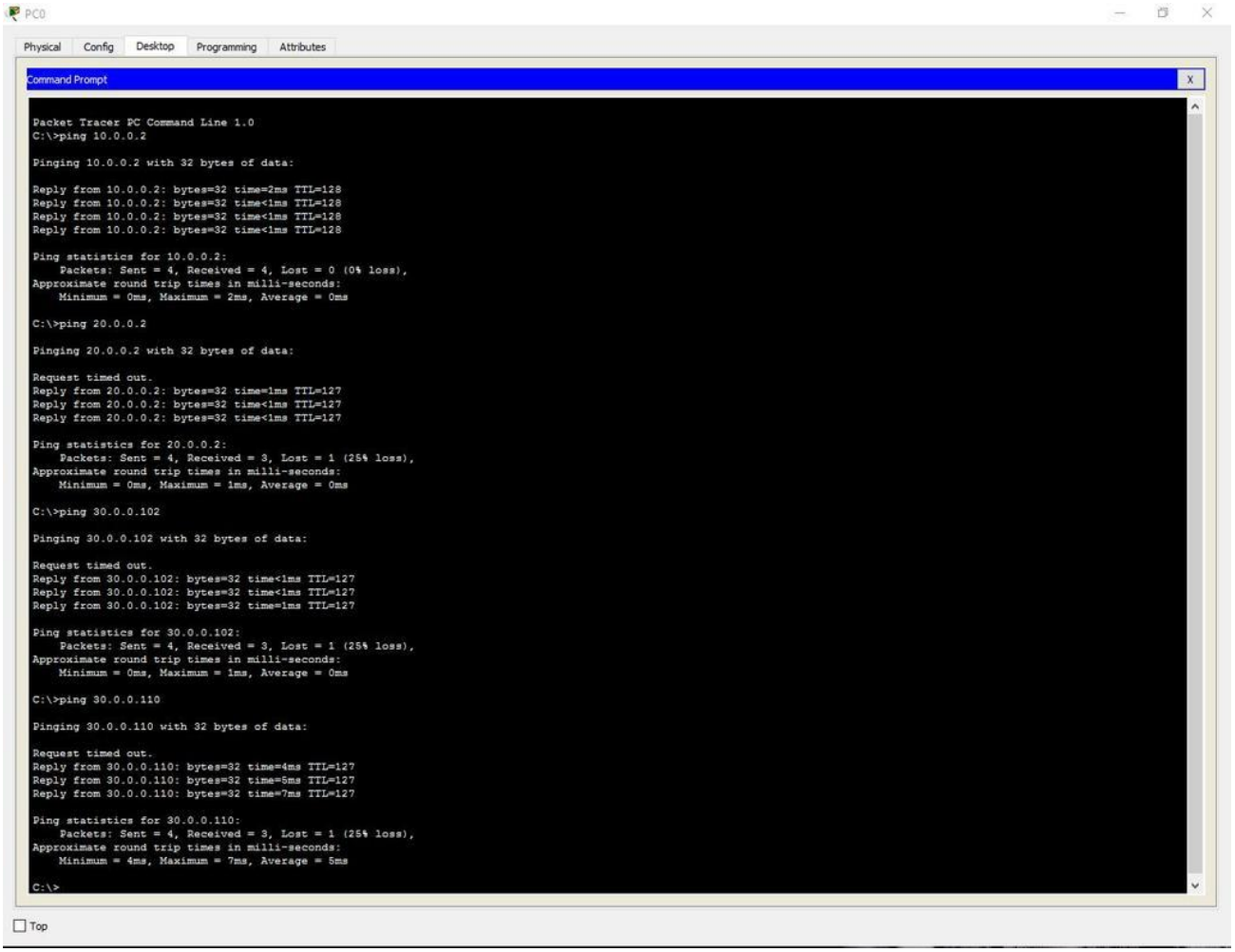
- int gig 0/0.10. The command connects a virtual interface to work with different VLANs. The digit after the dot is the VLAN number.
- Encapsulation dot1Q 10. The VLAN configuration command in sub. The number after dot1Q is the VLAN number.

- ip address 10.0.0.254 255.255.255.0. IP address of the output of information packets.

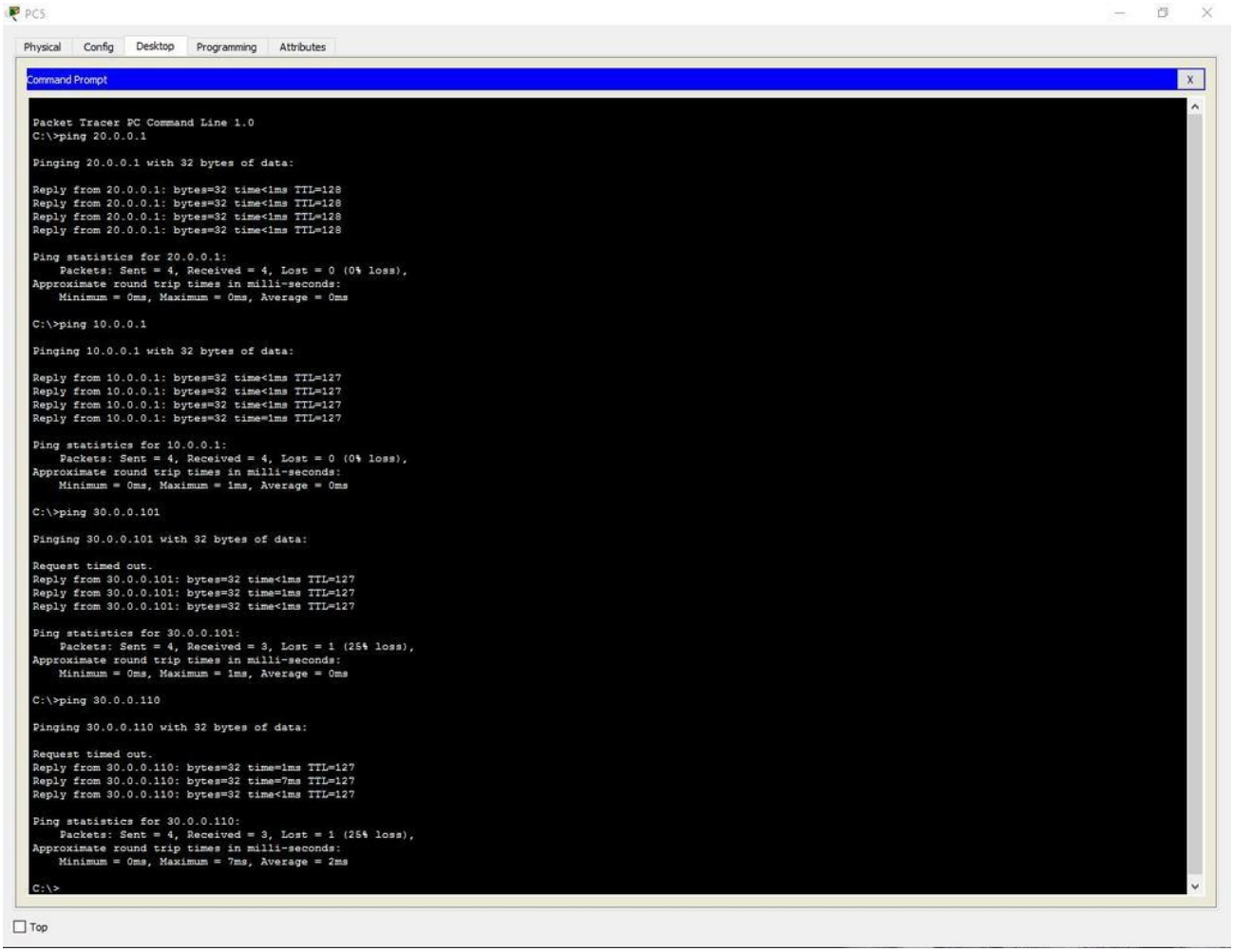
Now let's test the network with the ping command.

We will take any computer in each department and ping all departments (in the third department we will check both the wired network and the wireless one).

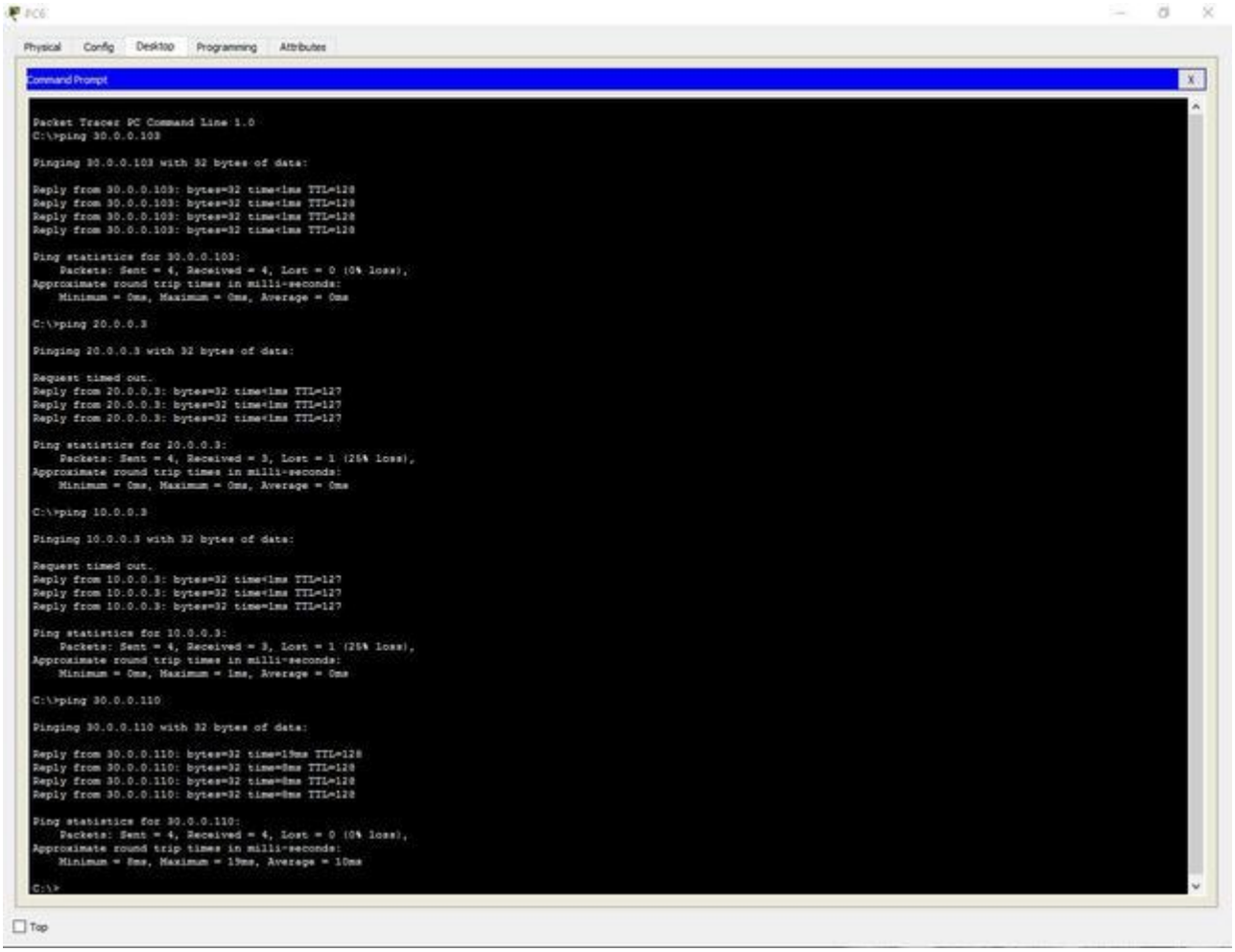
The first department:



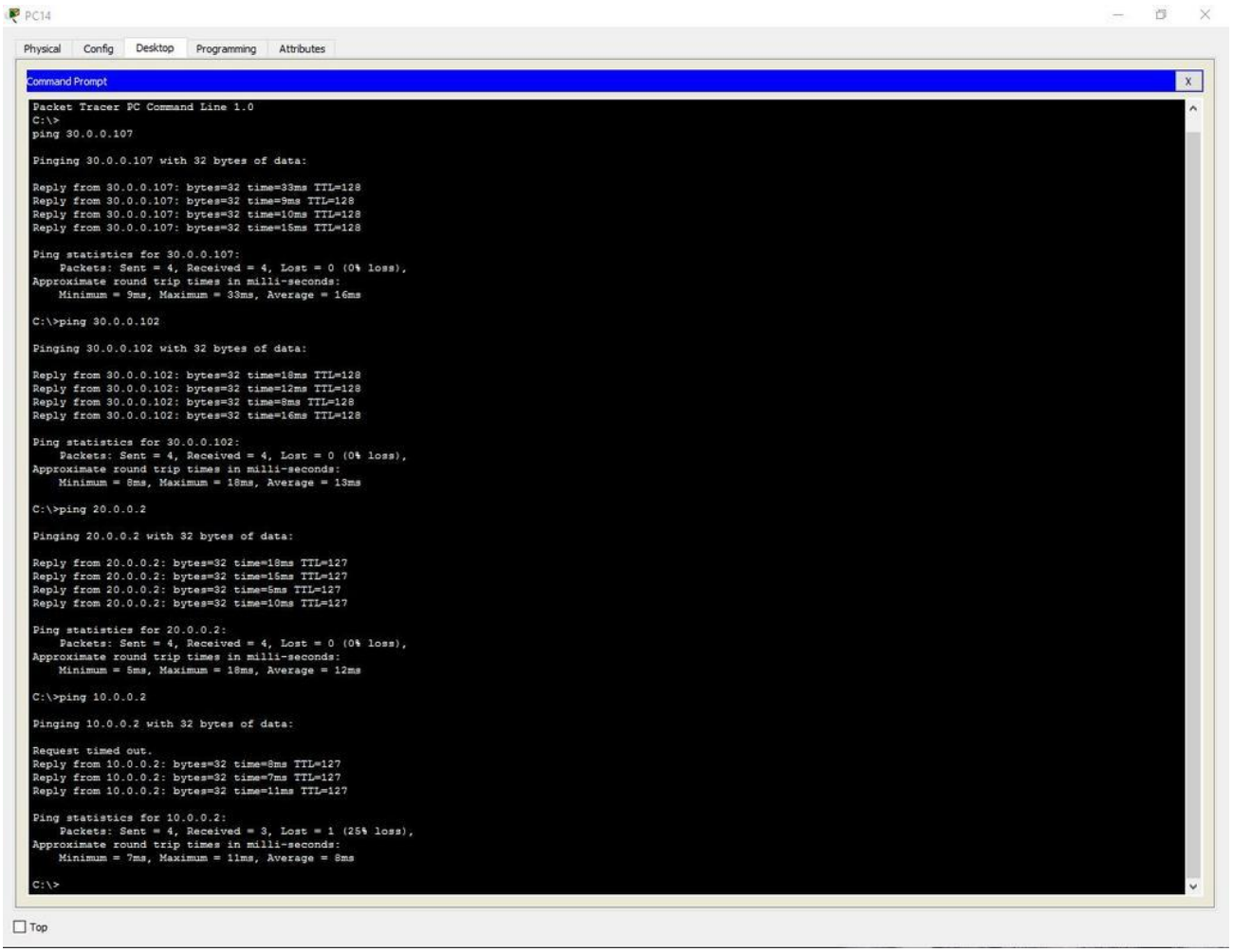
Second department:



Third department (cable):



Third Department (Wi-Fi):



Adding an administrative VLAN (40 — Management).

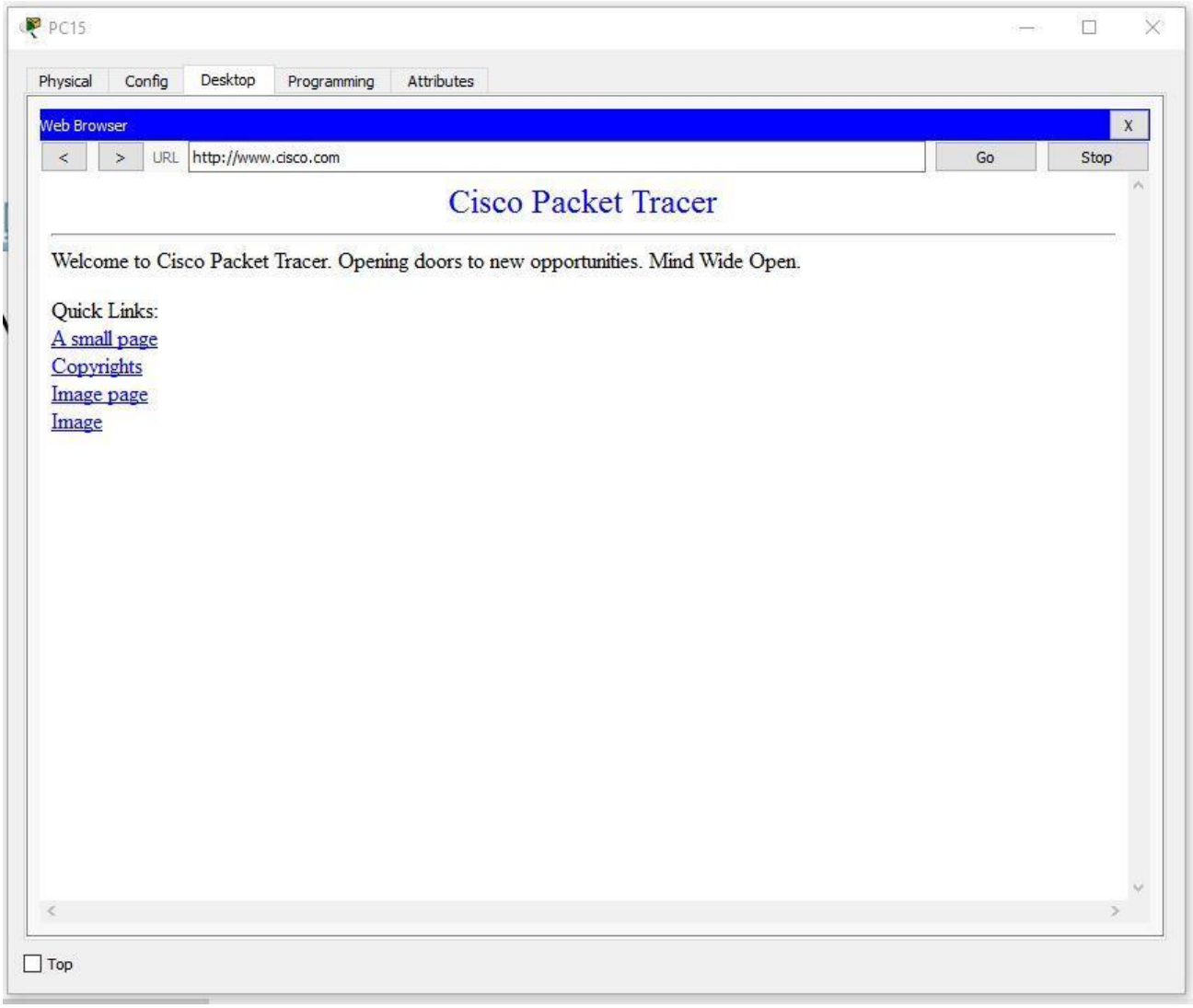
7. Server setup.

Enabling DNS.

Name — www.cisco.com.

Address – 20.0.0.3.

Let's check the possibility of accessing the site from any department. Enter the URL name in the browser and click Go.



8. Configure SSH.

To do this, go into the router and write commands:

```
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
```

Let's analyze each command:

- clock set 10:10:00 13 Oct 2017. Setting the exact time for key generation.
- ip domain name ssh.dom. Specify the domain name (required for key generation).
- crypto key generate rsa. Generate an RSA key (you will need to select the key size).
- service password-encryption. Activate password encryption in the configuration file.
- username Valery privilege 15 password 8 junior17. We start a user with the name Valery, the password junior17 and the privilege level 15.
- aaa new-model. Activate the AAA protocol (before activating AAA, at least one user must be installed in the system).
- line vty 0 4. We enter the configuration mode of terminal lines from 0 to 4.
- transport input ssh. We specify the default SSH network access environment.
- logging synchronous. We activate the automatic raising of the line after the system responds to the changes made.
- exec-timeout 60 0. We specify the timeout time before the SSH session is automatically closed in 60 minutes.
- copy running-config startup-config. We save the configuration file to non-volatile memory. (The line "Destination filename [startup-config]?" will be output here Enter "startup-config").

9. Configure the protection against on each switch.

To do this, open the switch and write commands:

```
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
```

Let's analyze each command:

- Interface range fastEthernet 0/X-Y. Selecting a range of interfaces (X is the first desired port, Y is the last).

Attention! Choose ports that are NOT active in connections!

- switchport mode access. Switching the port to access mode.
- switchport port-security. Enabling port protection.
- switchport port-security maximum K. We limit the number of MAC addresses on the interface (K is the number of ports).
- switchport port-security mac-address sticky. We choose the method of studying MAC addresses by the switch (there is a static (mac-address) and dynamic (sticky)).
- switchport port-security violation shutdown. We set the type of response to exceeding the number of allowed MAC addresses (there are protect - after overflow, all packets sent from other MAC addresses are discarded, restrict – the same thing, but with a notification in syslog or via SNMP, shutdown - the port is turned off before it is automatically or manually raised, notifications are also sent).

As a result , the work was done as follows: