Network Lab

Asia AL-KARKHI

Lab 1

Getting Started with Packet Tracer

This sheet will guide you through the installation of Packet Tracer, describe its graphical interface, and show you how to create your first simple topology in it. Because this is a simulator, not all real world (read real hardware) protocols are supported. So, we will begin by seeing which protocols it does support.

Protocols supported by Packet Tracer

A simulator, as the name suggests, simulates network devices and its environment, so protocols in Packet Tracer are coded to work and behave in the same way as they would on real hardware. The following table shows the protocols supported by Packet Tracer.

Technology	Protocols
LAN	Ethernet (including CSMA/CD*), 802.11 a/b/g/n wireless*, and PPPOE
Switching	VLANs, 802.1q, trunking, VTP, DTP, STP*, RSTP*, multilayer switching*, EtherChannel, LACP, and PAgP
TCP/IP	HTTP, HTTPS, DHCP, DHCPv6, Telnet, SSH, TFTP, DNS, TCP*, UDP, IPv4*, IPv6*, ICMP, ICMPv6, ARP, IPv6 ND, FTP, SMTP, POP3, and VOIP(H.323)
Routing	Static, default, RIPv1, RIPv2, EIGRP, single area OSPF, multiarea OSPF, BGP, inter-VLAN routing, and redistribution
WAN	HDLC, SLARP, PPP*, and Frame Relay*
Security	IPsec, GRE, ISAKMP, NTP, AAA, RADIUS, TACACS, SNMP, SSH, Syslog, CBAC, Zone-Based Policy Firewall, and IPS
QoS	Layer 2 QoS, Layer 3 DiffServ QoS, FIFO Hardware queues, Priority Queuing, Custom Queuing, Weighted Fair Queuing, MQC, and NBAR*
Miscellaneous	ACLs (standard, extended, and named), CDP, NAT (static, dynamic, inside/outside, and overload), and NATv6

* These protocols have substantial modelling limitations, so not all commands under these protocols work.

Installing Packet Tracer

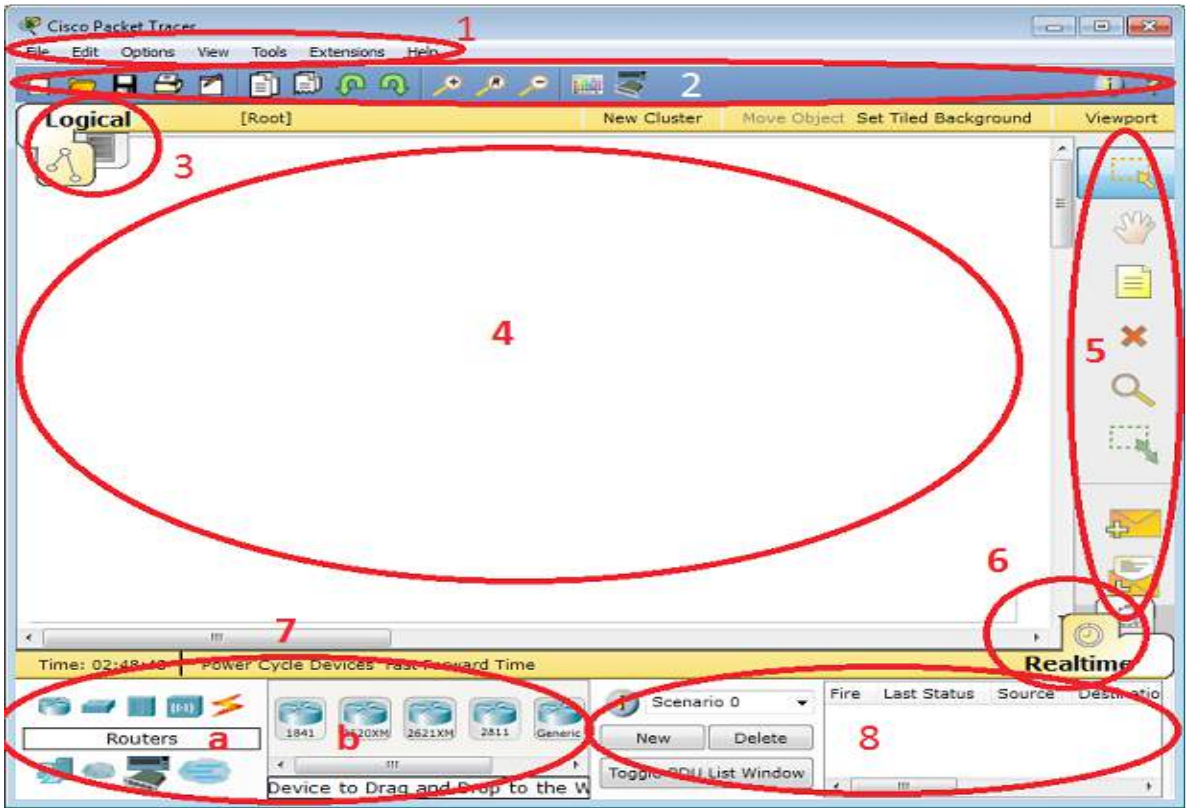
To download Packet Tracer, go to https://www.netacad.com and log in with your Cisco Networking Academy credentials; then, click on the Packet Tracer graphic and download the package appropriate for your operating system.

Windows

Installation in Windows is pretty simple and straightforward; the setup comes in a single file named Packettracer_Setup6.0.1.exe. Open this file to begin the setup wizard, accept the license agreement, choose a location, and start the installation.

Interface overview

The layout of Packet Tracer is divided into several components similar to a photo editor. Match the numbering in the following screenshot with the explanations given after it:



The components of the Packet Tracer interface are as follows:

Area 1: Menu bar – This is a common menu found in all software applications; it is used to open, save, print, change preferences, and so on.

Area 2: Main toolbar – This bar provides shortcut icons to menu options that are commonly accessed, such as open, save, zoom, undo, and redo, and on the right-hand side is an icon for entering network information for the current network.

Area 3: Logical/Physical workspace tabs – These tabs allow you to toggle between the **Logical** and **Physical** work areas.

Area 4: Workspace – This is the area where topologies are created and simulations are displayed.

Area 5: Common tools bar – This toolbar provides controls for manipulating topologies, such as select, move layout, place note, delete, inspect, resize shape, and add simple/complex PDU.

Area 6: Realtime/Simulation tabs – These tabs are used to toggle between the real and simulation modes. Buttons are also provided to control the time, and to capture the packets.

Area 7: Network component box – This component contains all of the network and end devices available with Packet Tracer, and is further divided into two areas:

- **Area 7a: Device-type selection box** – This area contains device categories
- **Area 7b: Device-specific selection box** – When a device category is selected, this selection box displays the different device models within that category

Area 8: User-created packet box – Users can create highly-customized packets to test their topology from this area, and the results are displayed as a list.

Make sure you are familiar with these names, because moving forward we will be referring to them frequently.

Creating a simple topology

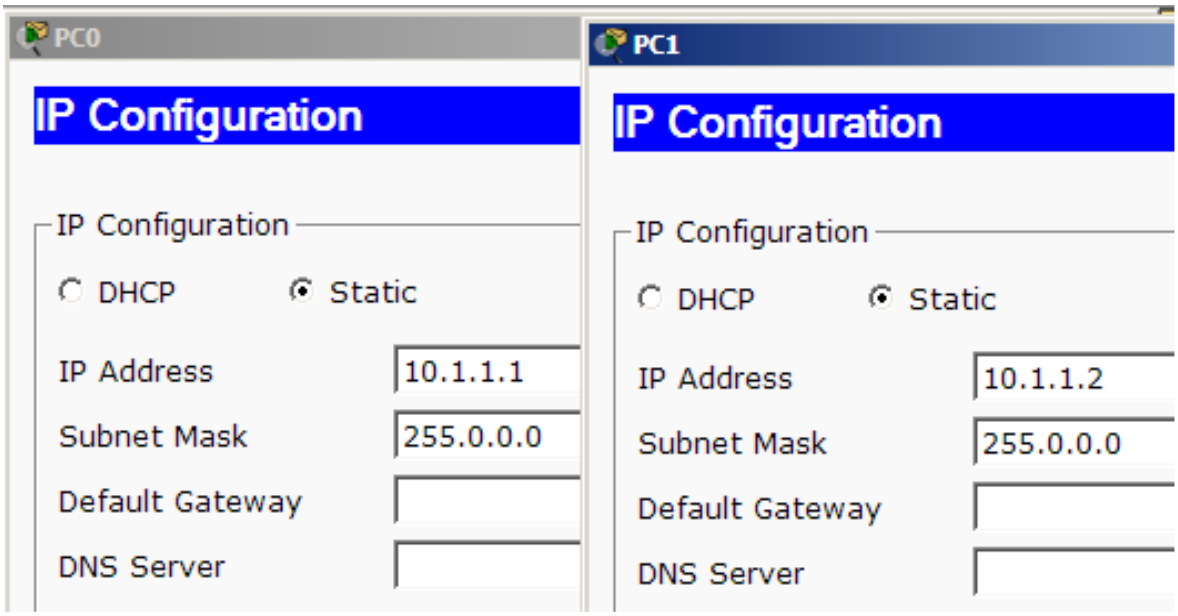
Now that you're familiar with the GUI of Packet Tracer, you can create your first network topology by carrying out the following steps:

1. From the network component box, click on **End Devices** and drag-and-drop a **Generic** PC icon and a **Generic** laptop icon into the Workspace.

2. Click on **Connections**, then click on **Copper Cross-Over**, then on **PC0**, and select **FastEthernet**. After this, click on **Laptop0** and select **FastEthernet**. The link status LED should show up in green, indicating that the link is up.

3. Click on the PC, go to the **Desktop** tab, click on **IP Configuration**, and enter an IP address and subnet mask. In this topology, the default gateway and DNS server information is not needed as there are only two end devices in the network.

4. Close the window, open the laptop, and assign an IP address to it in the same way. Make sure that both of the IP addresses are in the same subnet. We'll be learning more about end device configuration in this course, *Generic IP End Devices*.



5. Close the **IP Configuration** box, open the command prompt, and ping the IP address of the device at the end to check connectivity.

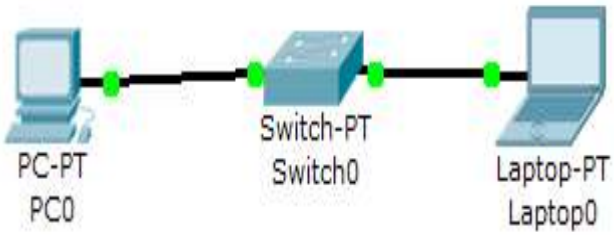
```
PC>ping 10.1.1.1

Pinging 10.1.1.1 with 32 bytes of data:

Reply from 10.1.1.1: bytes=32 time=62ms TTL=128
Reply from 10.1.1.1: bytes=32 time=31ms TTL=128
Reply from 10.1.1.1: bytes=32 time=32ms TTL=128
Reply from 10.1.1.1: bytes=32 time=31ms TTL=128

Ping statistics for 10.1.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 31ms, Maximum = 62ms, Average = 39ms
```

What is a network topology without a single network device in it? Add an Ethernet switch to this topology so that more than two end devices can be connected, by performing the following steps:

1. Click on **Switches** from the device-type selection box and insert any switch (except **Switch-PT-Empty**) into the workspace.

2. Remove the link between the PC and the laptop using the delete tool from the common tools bar.

3. Choose the **Copper Straight-Through** cable and connect the PC and laptop with the switch. At this point, the link indicators on the switch are orange in color because the switchports are undergoing the listening and learning states of the **Spanning Tree Protocol** (**STP**).



4. Once the link turns green, as shown in the previous screenshot, ping again to check the connectivity. The next chapter, *Chapter 2*, *Network Devices*, will deal with the configuration of network devices.

5. To save this topology, navigate to **File** | **Save As** and choose a location. The topology will be saved with a .pkt extension, with the devices in the same state.

Summary

You have successfully installed Packet Tracer and used it to create a simple topology. Keep trying different topologies with only PCs/laptops and switches to familiarize yourself

with the GUI. You have also seen a list of protocols supported by Packet Tracer; use this list as a reference. Whenever you want to try a new technology in the future, make sure that the protocols to be configured are fully supported by Packet Tracer before moving ahead.

In the next lab., you'll learn about the different types of network devices and how to customize them according to your needs. You'll also see how to configure them through the CLI as well as through the graphical interface.

with the GUI. You have also seen a list of protocols supported by Packet Tracer; use this list as a reference. Whenever you want to try a new technology in the future, make sure that the protocols to be configured are fully supported by Packet Tracer before moving ahead.

In the next lab., you'll learn about the different types of network devices and how to customize them according to your needs. You'll also see how to configure them through the CLI as well as through the graphical interface.

Lab. 2

Network Devices

Network devices form the core of networking. In this sheet, you'll learn about all of the network devices available in Packet Tracer and the modules used by it. After reading the *Configuring network device* section, you'll be on your way to configure Cisco routers and switches without using any commands.

Cisco devices and Packet Tracer devices

Selecting **Switches** or **Routers** from the device-type selection box lists both Cisco devices and some devices labelled **Generic**.

Routers

A router provides connectivity between two logical networks. Every router in Packet Tracer can be switched on or off by using the provided power button.

The power switch is required to make a device simulate its real counterpart. Modules can be added or removed only after powering off the device. If the running configuration is not saved, power cycling a device will make it lose its configuration.

The following routers are available in Packet Tracer:

Cisco 1841: This is an **Integrated Service Router** (**ISR**) having two Fast Ethernet ports, two slots for **HighSpeed WAN Interface Cards** (**HWICs**), and one slot for **Advanced Integration Module** (**AIM**)
Cisco 1941: This is similar to the previous model but runs on Cisco IOS Version 15. It has two ports that operate at Gigabit Ethernet speeds.
Cisco 2620XM: This is a multiservice router with one Fast Ethernet port, two slots for WAN Interface cards, and one slot for AIM.
Cisco 2621XM: This is similar to the previous model, except that this router has two Fast Ethernet ports.
Cisco 2811: This ISR comes with two Fast Ethernet ports, four WIC slots, and a dual slot for AIM.
Cisco 2901: This router has two Gigabit Ethernet ports, four WIC slots, and two **Digital Signal Processor** (**DSP**) slots. This router uses Cisco IOS Version 15.
Cisco 2911: This router has three Gigabit Ethernet ports and all the other features of the previous router. It runs on IOS Version 15.
Generic Router-PT: This is a custom router running on Cisco IOS. It contains 10 slots and has separate modules with a naming convention beginning with **PT**.

Lab. 2

Switches

A switch, also called a multiport bridge, connects more than two end devices together. Each switch port is a collision domain. The following switches are available in Packet Tracer:

Cisco 2950-24: This managed switch comes with 24 Fast Ethernet ports.
Cisco 2950T-24: This switch is a member of the Catalyst 2590 Intelligent Switch family and has two Gigabit Ethernet ports in addition to the 24 Fast Ethernet ports.
Cisco 2960-24TT: This is another 24 port switch; the previous switch has **Gigabit Interface Converter** (**GBIC**) for Gigabit Ethernet ports, whereas this switch has **Small Form-factor Pluggable** (**SFP**) modules for the same. Note that this is a difference only on real switches, it has no impact on Packet Tracer.

Cisco 3560-24PS: This switch is different from the others because it is a layer 3 switch that can be used to perform routing in addition to switching. The **PS** suffix implies support for **Power over Ethernet** (**PoE**), which can be used to power up IP phones without using power adapters.

The Cisco Catalyst 3560-24PS is a fixed-configuration, enterprise-class multilayer switch designed for mid-sized networks.

• **Bridge PT**: This is a device used to segment a network and it has only two ports (which is why it is a bridge; if it had more, it'd be called a switch).

• **Generic Switch PT**: This is a Packet-Tracer-designed switch running on Cisco IOS. This is the only customizable switch with 10 slots and several modules.

Other devices

Packet Tracer has more than just Cisco routers and switches, which we'll see in this section. These devices do not have any configuration options and work out of the box.

Hub PT: This network hub was the oldest way to connect multiple end devices together. It still exists in Packet Tracer so that you can simulate and learn about network storms and broadcasts. This Packet Tracer device has 10 slots.

Repeater PT: This device is used to boost the signal on a wire when the distance between two points is high.

Coaxial Splitter PT: This is used to split a single coaxial connector into two. It has three coaxial ports and cannot be customized in any way.

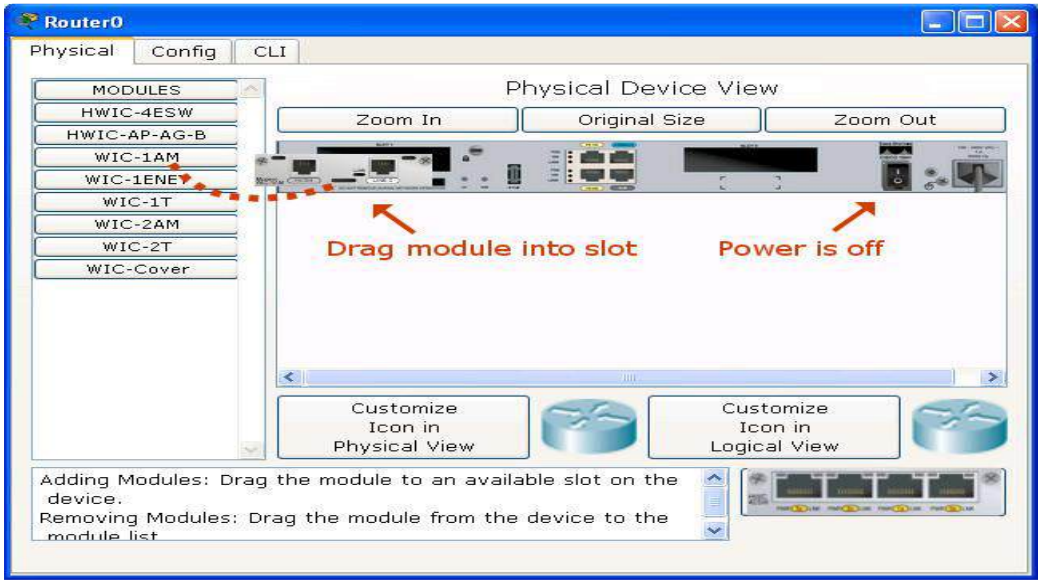
Lab. 2

Customizing devices with modules

A device module is a piece of hardware containing several device interfaces. For example, a **HWIC-4ESW** module contains four Ethernet (10 MBps) ports. Similar to a real router/switch, the device has to be powered off in order to add or remove modules.

The power switch is on the right-hand side of each device, with a green LED indicating that the power is on. Click on this switch to turn it off. To add a module, drag one from the modules list and drop it onto an empty slot. If a module doesn't fit into that slot, it automatically returns to the module list.

To remove a module, power off the device and drag it from the slot back to the module list.



hub, switch, and router are essential network devices, each with its distinct functions. Let's explore their differences using Packet Tracer:

Hub:

- **Broadcast Domain:** A hub operates at the physical layer of the OSI model. It broadcasts every incoming packet to all connected devices.
- **No Filtering:** It doesn't filter or examine the packet's destination address.
- **Collision Domain:** All devices connected to a hub share the same collision domain, meaning only one device can transmit at a time.

Lab. 2

- **Performance:** Hubs can be inefficient, especially in larger networks, due to excessive broadcast traffic.

Switch:

- **Broadcast Domain:** A switch operates at the data link layer. It examines the MAC address of the packet and forwards it only to the intended recipient.
- **Filtering:** Switches filter traffic based on MAC addresses, reducing broadcast traffic.
- **Collision Domain:** Each port on a switch creates a separate collision domain, improving performance.
- **Performance:** Switches offer better performance and scalability compared to hubs.

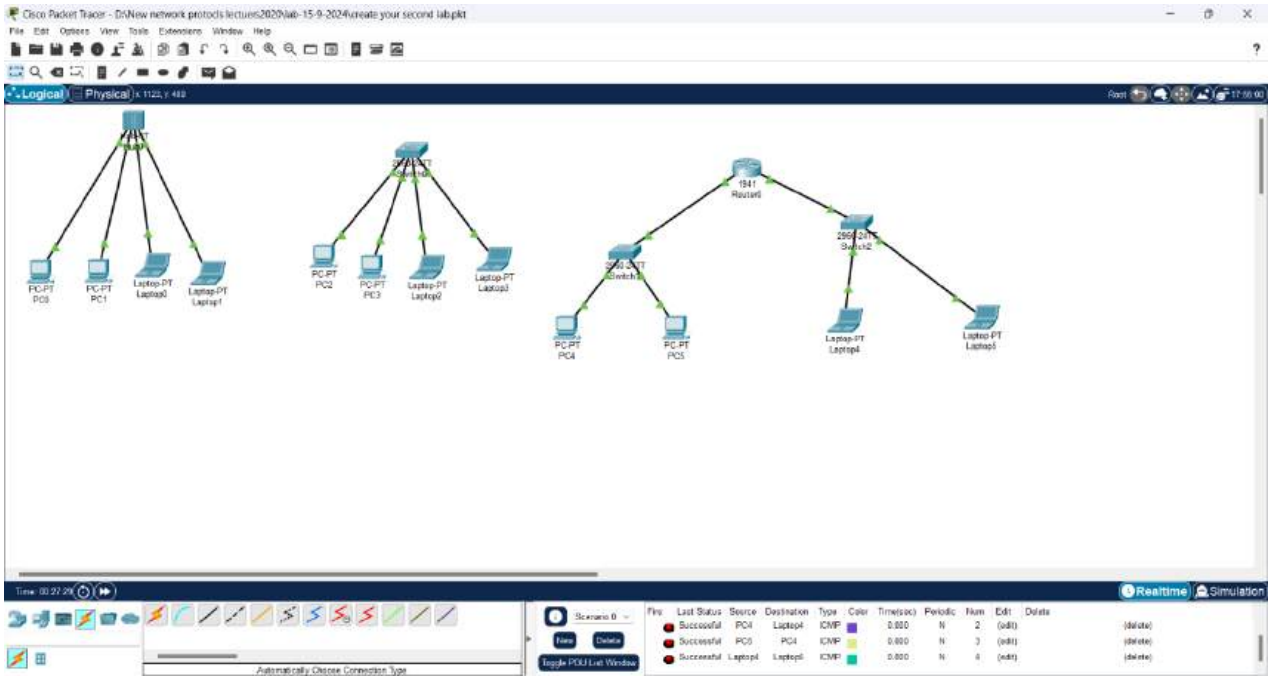
Router:

- **Network Domain:** A router operates at the network layer of the OSI model. It examines the IP address of the packet and forwards it to the appropriate network.
- **Routing:** Routers use routing protocols to determine the best path for packets to reach their destination.
- **Internetworking:** Routers are used to connect different networks (e.g., LANs, WANs).
- **Performance:** Routers are typically more complex and expensive than hubs or switches but are essential for larger and more complex networks.

In Packet Tracer:

Differences between hub, switch and routers.

Lab. 2

- 

  Hub: You'll observe that all devices connected to a hub receive every packet, leading to potential performance issues.

- **Switch:** When a device sends a packet, the switch will only forward it to the intended recipient, reducing network congestion.
- **Router:** You can configure routers to connect different networks and observe how packets are routed between them based on their IP addresses.

To summarize:

- **Hubs:** Simple, inexpensive, but inefficient.
- **Switches:** More efficient than hubs, suitable for smaller networks.
- **Routers:** Essential for larger networks, capable of connecting different networks and routing packets

Basic setup you can try:

1. **Create a network:** Start by creating a new network in Packet Tracer.
2. **Add devices:** Add a router, a switch, and multiple PCs to your network.
3. **Connect devices:** Use cables to connect the PCs to the switch and the switch to the router.

Lab. 2

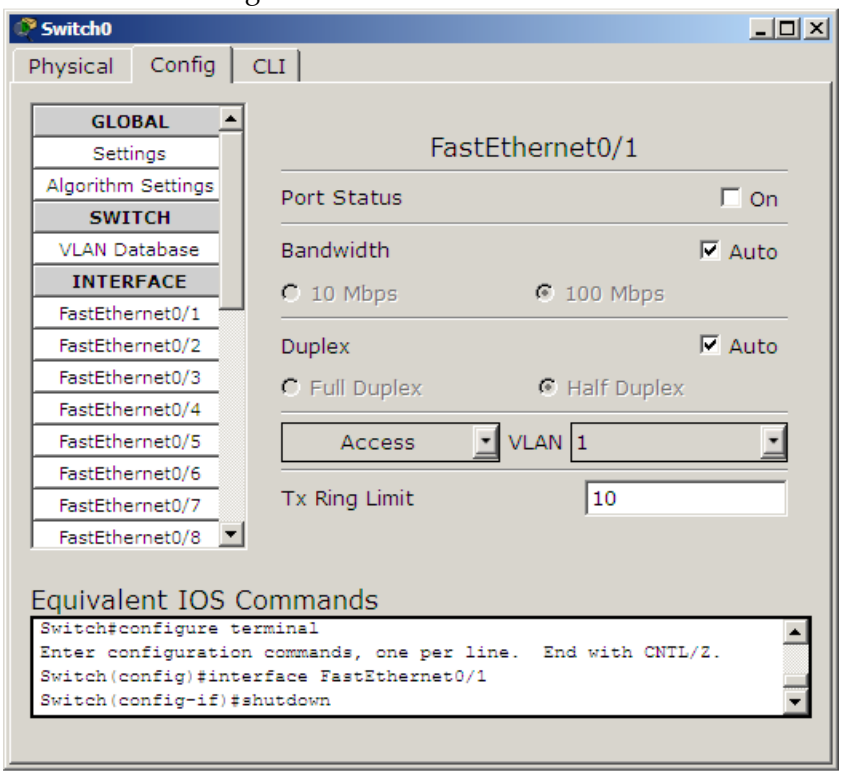
4. **Configure devices:** Assign IP addresses to the PCs and configure the router's interfaces.
5. **Test connectivity:** Try to ping between the PCs to verify connectivity.

To demonstrate the differences between hubs, switches, and routers, you can:

- **Replace the switch with a hub:** Observe how broadcast traffic increases and performance degrades.
- **Add more PCs:** See how the switch handles increased traffic more efficiently than a hub.
- **Configure the router with different routing protocols:** Experiment with how routing decisions affect network traffic.

Configuring network devices

In this section, you'll learn how to configure Cisco routers and switches. Packet Tracer provides a **Config** tab that contains GUI options for the most common configurations. What's more, as you tinker with the GUI, its equivalent Cisco IOS command is also displayed. Take a look at the following screenshot:

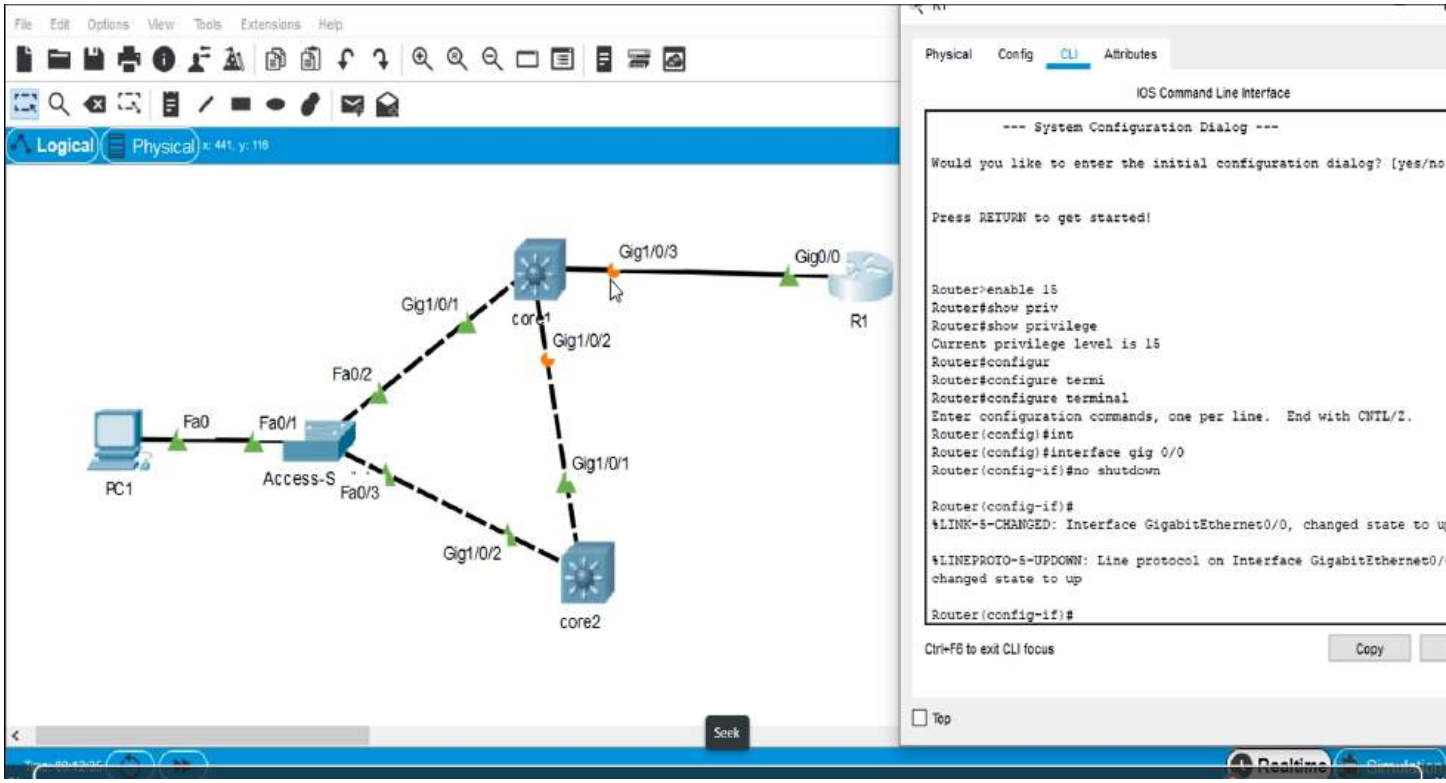


From the **Config** tab of the switch, we will set the **Interface** option to **FastEthernet0/1** and uncheck the **On** checkbox for **Port Status**. So the **Equivalent IOS Commands** section displays the following command to achieve this process:

Lab. 2

Switch>enable
Switch#configure terminal
Switch(config)#interface FastEthernet0/1
Switch(config-if)#shutdown

In the following topology we configure the router



University of Technology

Computer Science Department

Lab sheet: Network protocols

Class: Year 2

Lecturer: Asia Ali

Connecting two networks using a router.

Objective:

- The experiment is to understand how to connect two networks with each other.
- Testing the networks.

Experiment steps;

Network (1)

a. **Choose 2 or 3 generic pc(s).**
b. **Choose a switch (0) 2960-24TT.**
c. **Copper straight-through cable.**
d. **Sort out the interface (FastEthernet) as you have learned in lab 1 and lab 2.**

Network (2)

A. Choose another 2 or 3 generic pc(s)
B. Choose a switch (1) 2960-24TT.
C. Copper straight-through cable.
D. Sort out the interfaces (FastEthernet) as you have learned in lab 1 and lab 2.

Configuration the router:

A. **Choose a router 1941.**
B. **We need to connect the switches through the router.**
C. **Choose straight-through cable to connect the switch to the router. You can use either FastEthernet0/4 interface if you have used 3 pc(s) or FastEthernet0/3 if you have used 2 pc(s). In addition, you can try for the interface, gigabitethernet0/0.**
D. **Connect the router to switch (1) using copper straight-through cable. For the interface, choose gigabitethernet0/1 if you have used**

gigabitethernet0/0 with switch (0). As shown in the screen shot figure 1.

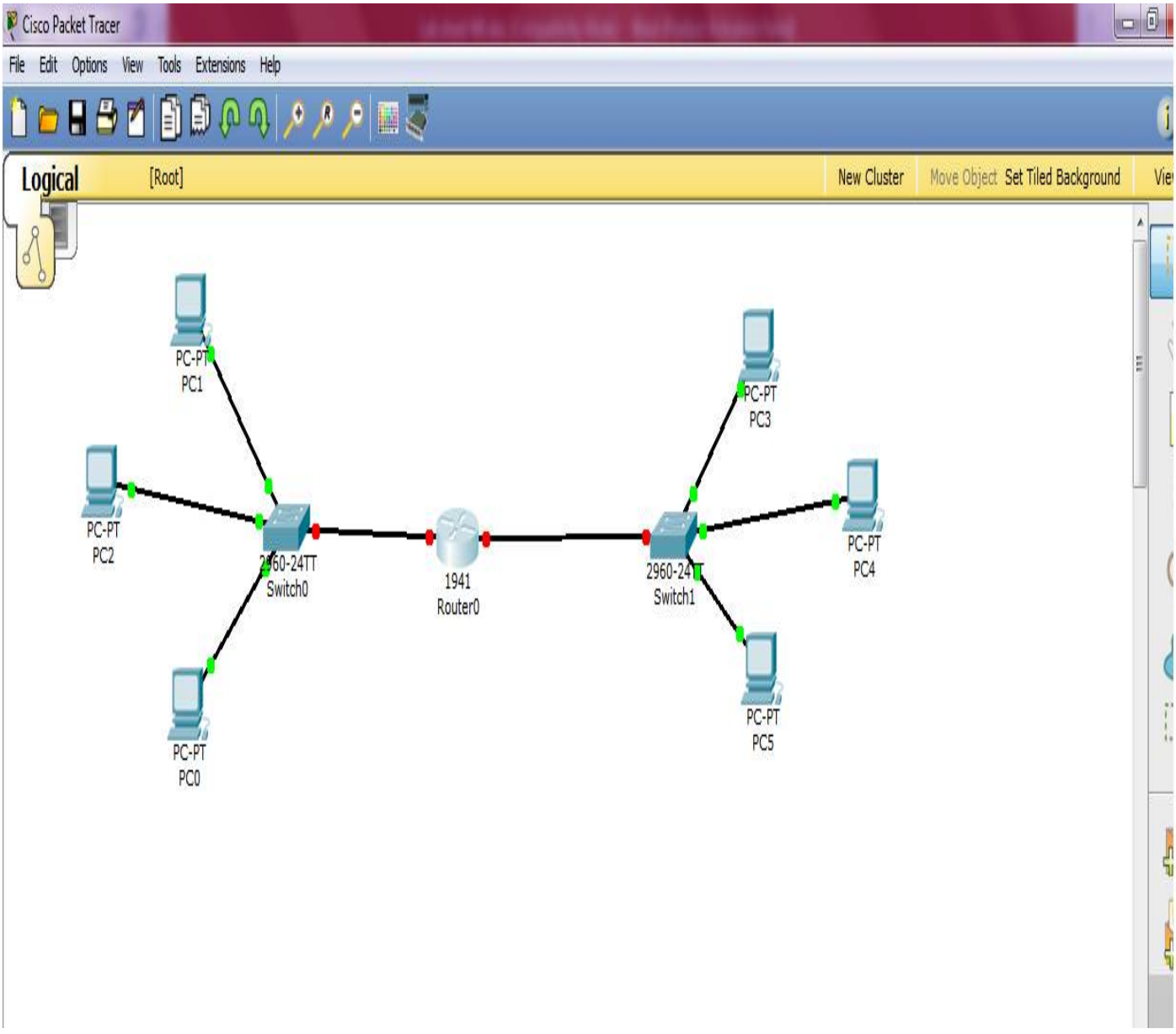


Figure 1- Two networks and a router.

Use IP addressing for network (1) to be in class C and for network (2) to be in class B.
192.168.10.1
192.168.10.2
192.168.10.3
ROUTER :GETWAY;192.168.10.254

CLASSE B
172.16.10.1
172.16.10.2
172.16.10.3
ROUTER GETWAY: 172.16.10.254

1- ping from PC0 to PC1
2- Click after PC> prompt and type the following ping command, ping 192.168.10.2 and press the Enter key. What type of output have you received?

1- Pings and the ICMP protocol. Ping program generates an IP packet with an encapsulated ICMP Echo Request message. It is a tool used to test the destination device, which receive the ping, Echo Request, it issues an Echo Reply.

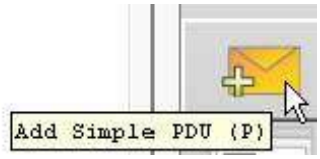
2- Command to be issued from PC0 to pc2 ping 192.168.10.3 , what has happened ,explain?

3- Packet Tracer allows you either to issue the command from the command prompt or to use the Add Simple PDU tool in the simulation mode

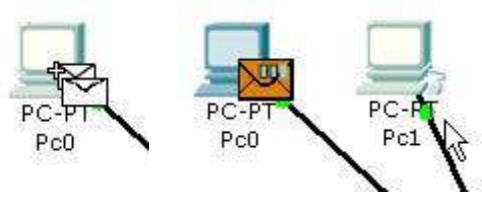
.

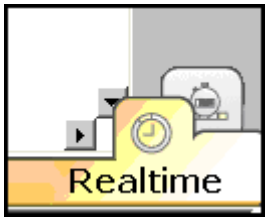
4- To enter Simulation Mode click the Simulation Mode tab in the lower right hand corner 0f the interface.

5- Choose the Add Simple PDU tool from the tool box



Click once on PC0, the device issuing the ping (ICMP Echo Request) and then click once on PC1 (the destination of the ICMP Echo Request).





6- In order to view only the “pings”, in the Event List, click on ALL/NONE to clear all protocols, and then click on ICMP to select only that protocol

7- Click on the Capture / Forward button in Play Controls (the yellow bar below the windows) to view a step-by-step process of the ping command.

8- Continue clicking the Capture / Forward button until all frames have been sent.

VLAN (Virtual Local Area Network)

A VLAN is a logical network segment within a physical network. It allows you to group devices together based on their function or location, regardless of their physical proximity. This provides several benefits:

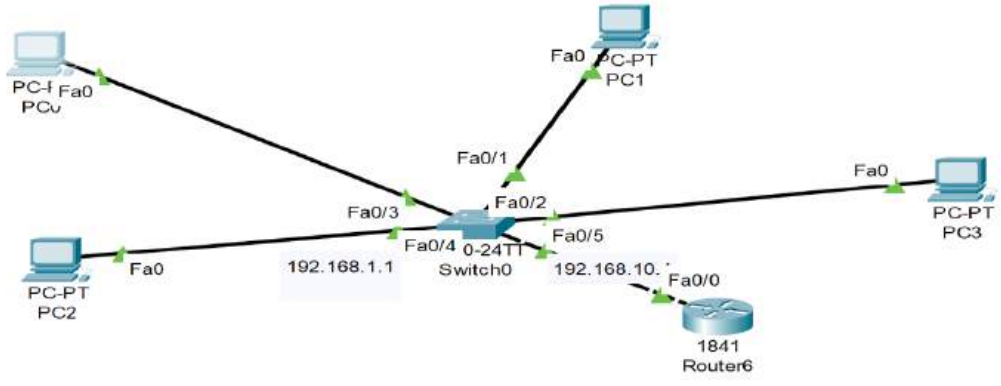
- **Isolation:** Prevents unauthorized access between different groups of devices.
- **Security:** Enhances network security by limiting the spread of malware or unauthorized access.
- **Management:** Simplifies network management by organizing devices into logical groups.
- **Scalability:** Allows for efficient network growth and expansion.

How VLANs work:

VLANs are created and managed by network switches. Each device connected to a switch is assigned to a VLAN. The switch uses tagging mechanisms (like IEEE 802.1q) to identify the VLAN of each packet and forwards it accordingly.

Types of VLANs:

- **Default VLAN:** The VLAN to which devices are assigned by default when not explicitly configured.
- **Data VLANs:** Used for general data traffic.
- **Management VLANs:** Used for managing network devices.
- **Voice VLANs:** Optimized for voice traffic, often with Quality of Service (QoS) settings.



After IP addresses have been assigned to all PCs, create the necessary VLANs on the switch and assign the ports to them.

Sw1> config

Sw1(config)#vlan 10

Sw1(config-vlan)#name NAT1

Sw1(config-vlan)#vlan 20

Sw1(config-vlan)#name NAT2

Sw1(config-vlan)#int fa0/1

SW1(config-inf)#switchport mode access vlan 10

SW1(config-inf)#switchport access vlan 10

Sw1(config-vlan)#int fa0/2

SW1(config-inf)#switchport mode access vlan 10

SW1(config-inf)#switchport access vlan 10

Sw1(config-vlan)#int fa0/3

SW1(config-inf)#switchport mode access vlan 20

SW1(config-inf)#switchport access vlan 20

Sw1(config-vlan)#int fa0/4

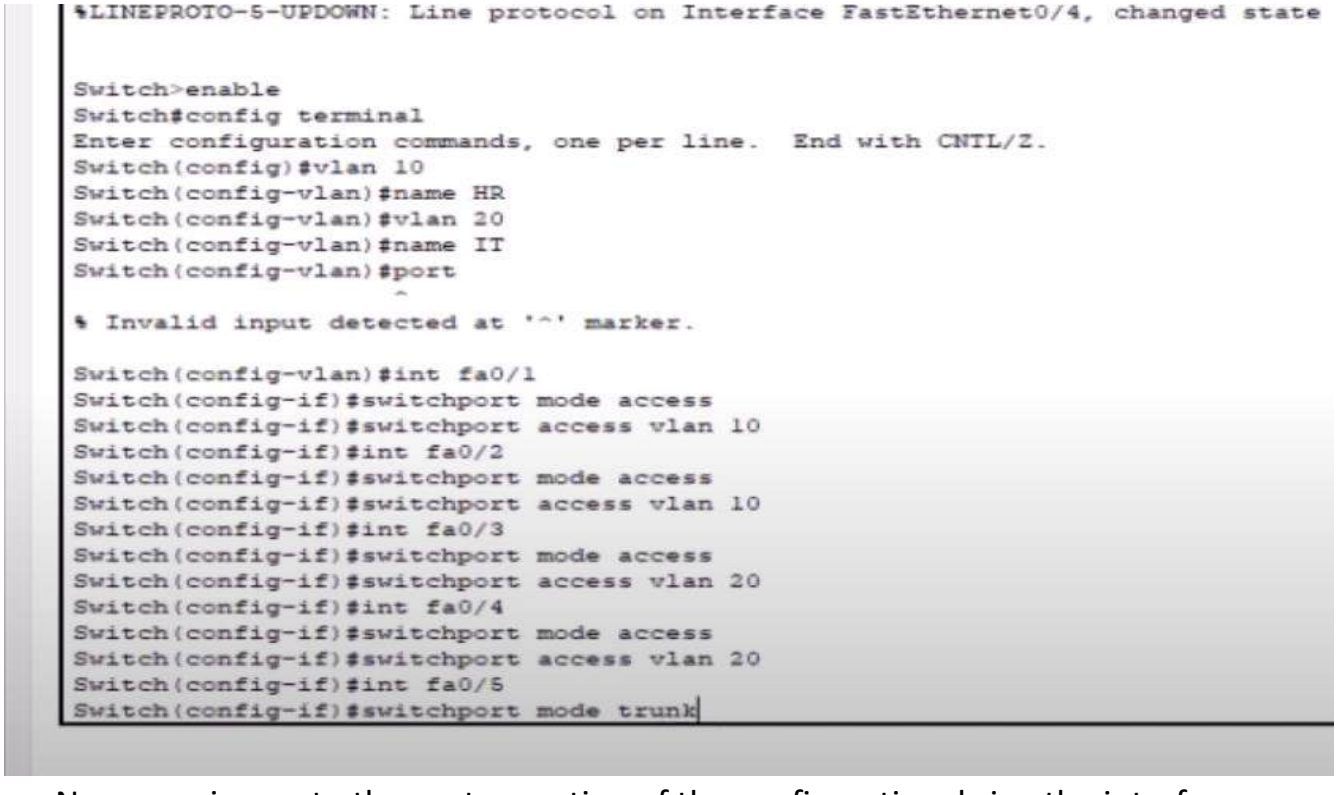
SW1(config-inf)#switchport mode access vlan 20

SW1(config-inf)#switchport access vlan 20

1. Configure the switch port that connects to the router as a trunk link. More on this in the *Switch-to-switch trunk links* section.

Sw1(config)#int f0/5

Sw1(config-if)#switchport mode trunk



Now, moving on to the router portion of the configuration, bring the interface up.

R1(config)#int f0/0

R1(config-if)#no shutdown

1. We will now create the sub interfaces. Each will have its own IP address in a different network.

R1(config-subif)#int f0/0.10

R1(config-subif)#encapsulation dot1Q 10

R1(config-subif)#ip address 192.168.1.10 255.255.255.0

R1(config-subif)#int f0/0.20

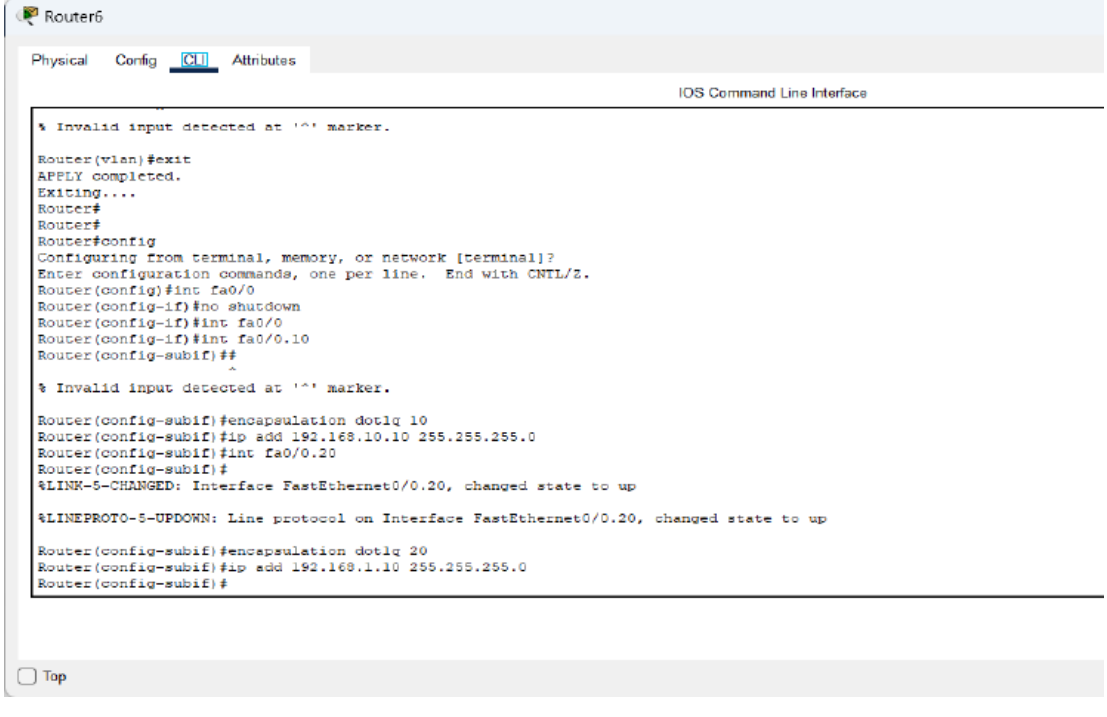
R1(config-subif)#encapsulation dot1Q 20

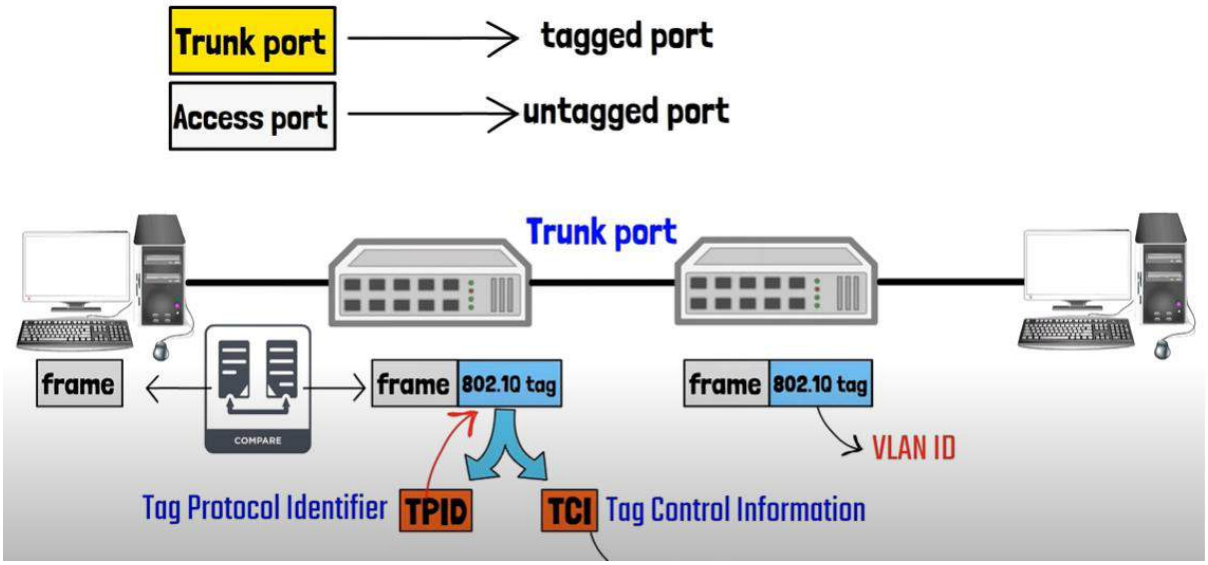
R1(config-subif)#ip address 192.168.10.10 255.255.255.0

1. Notice the encapsulation command here. It specifies the VLAN ID the interface will handle.

2. That's it, now test the connectivity between hosts on different VLANs using simple PDUs or a ping. The first packet will always time

3. out as it takes some time for the **ARP** (**Address Resolution Protocol**) to complete.



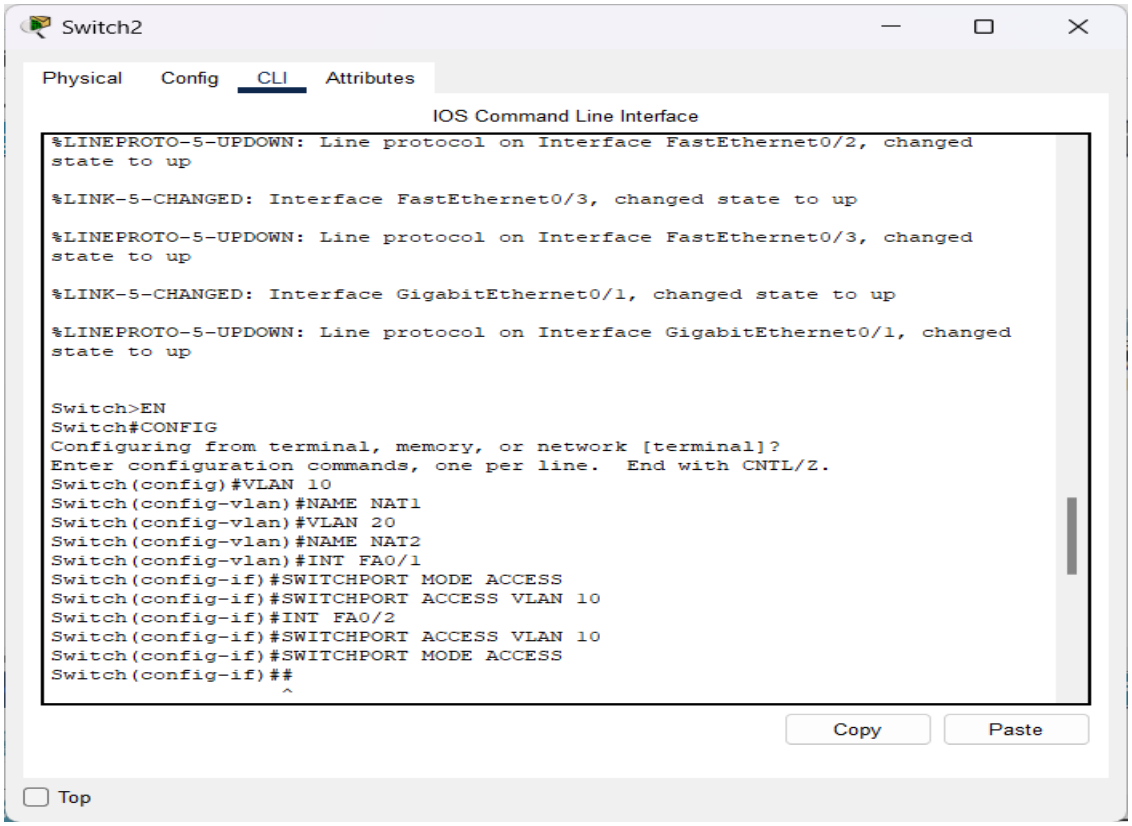


IEEE 802.1Q is the standard that defines VLAN tagging, which is crucial for trunking. A trunk link is a network connection that carries traffic for multiple VLANs over a single physical link. This allows you to efficiently segregate traffic and optimize network resources.

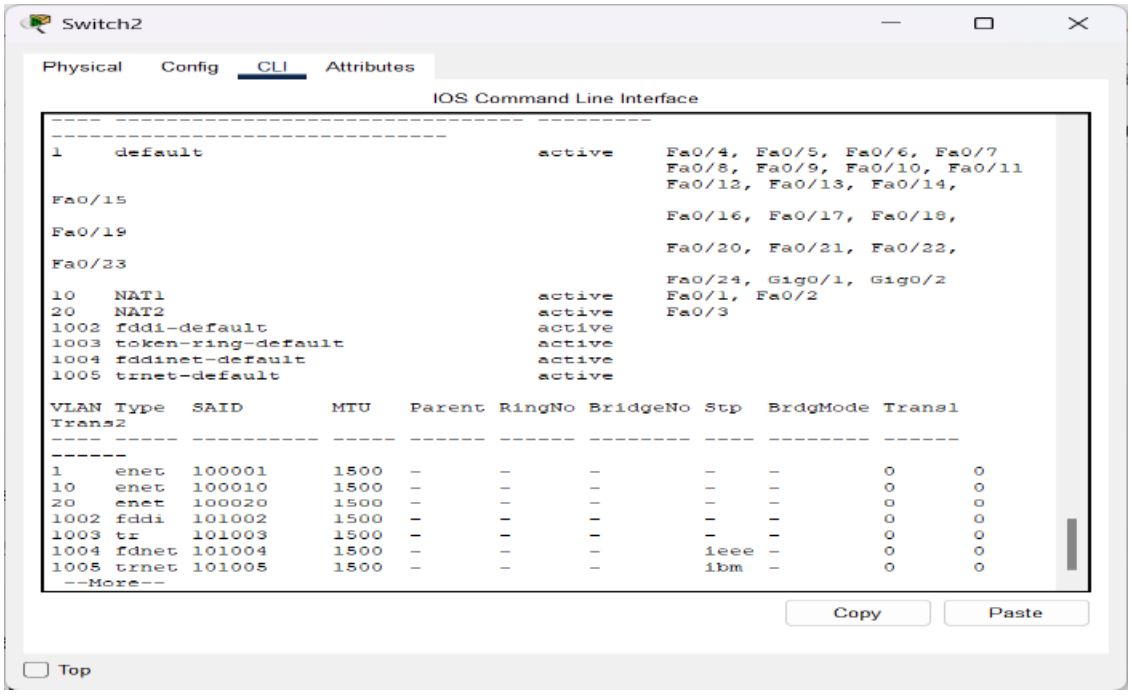
Key points about 802.1Q trunking:

- **VLAN Tagging:** Each frame on a trunk link is tagged with a VLAN ID, indicating the VLAN to which the frame belongs.
- **Trunk Port Configuration:** Network devices (switches) must be configured as trunk ports to support VLAN tagging.
- **Inter-VLAN Communication:** Trunk links enable communication between devices in different VLANs, facilitating network segmentation and security.
- **Scalability:** Trunking allows for efficient scaling of networks by consolidating multiple VLANs onto a single physical link.

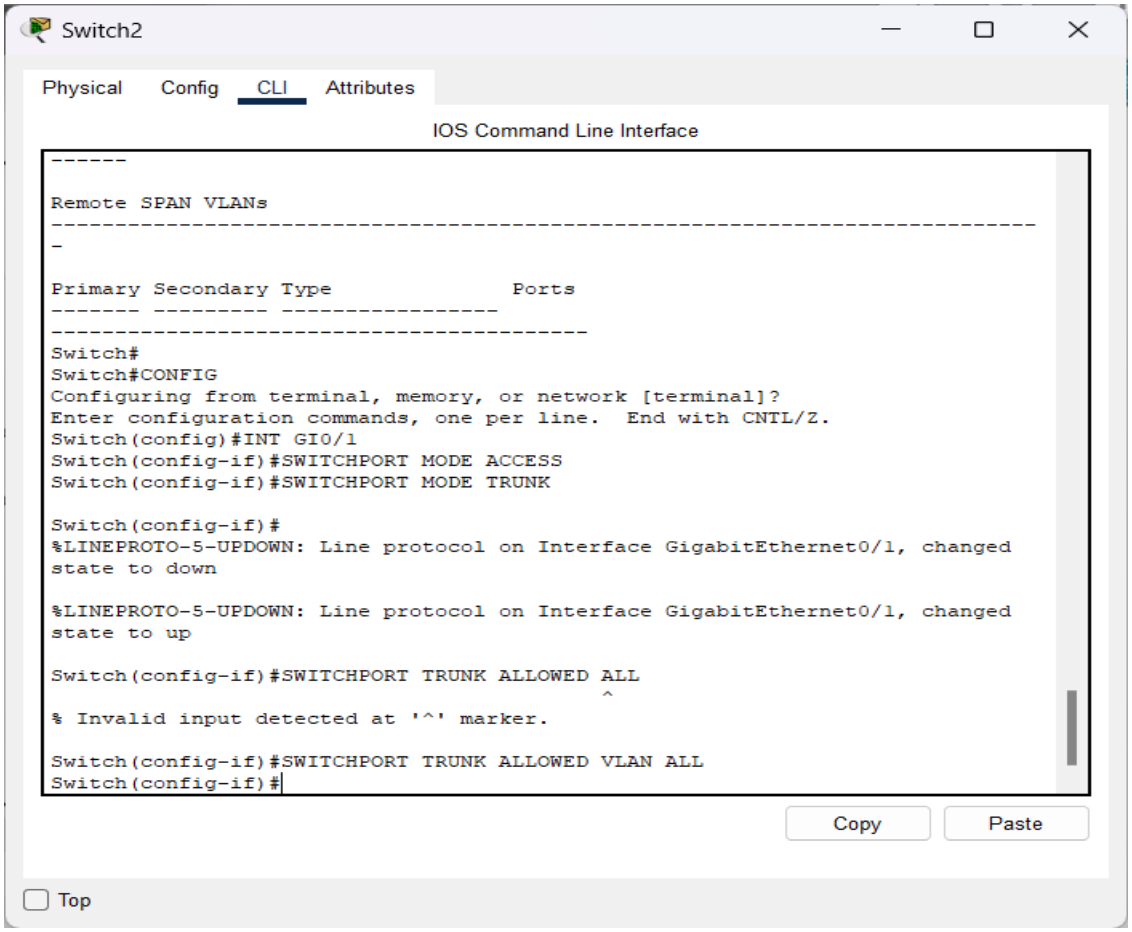
SWITCH CONFIG



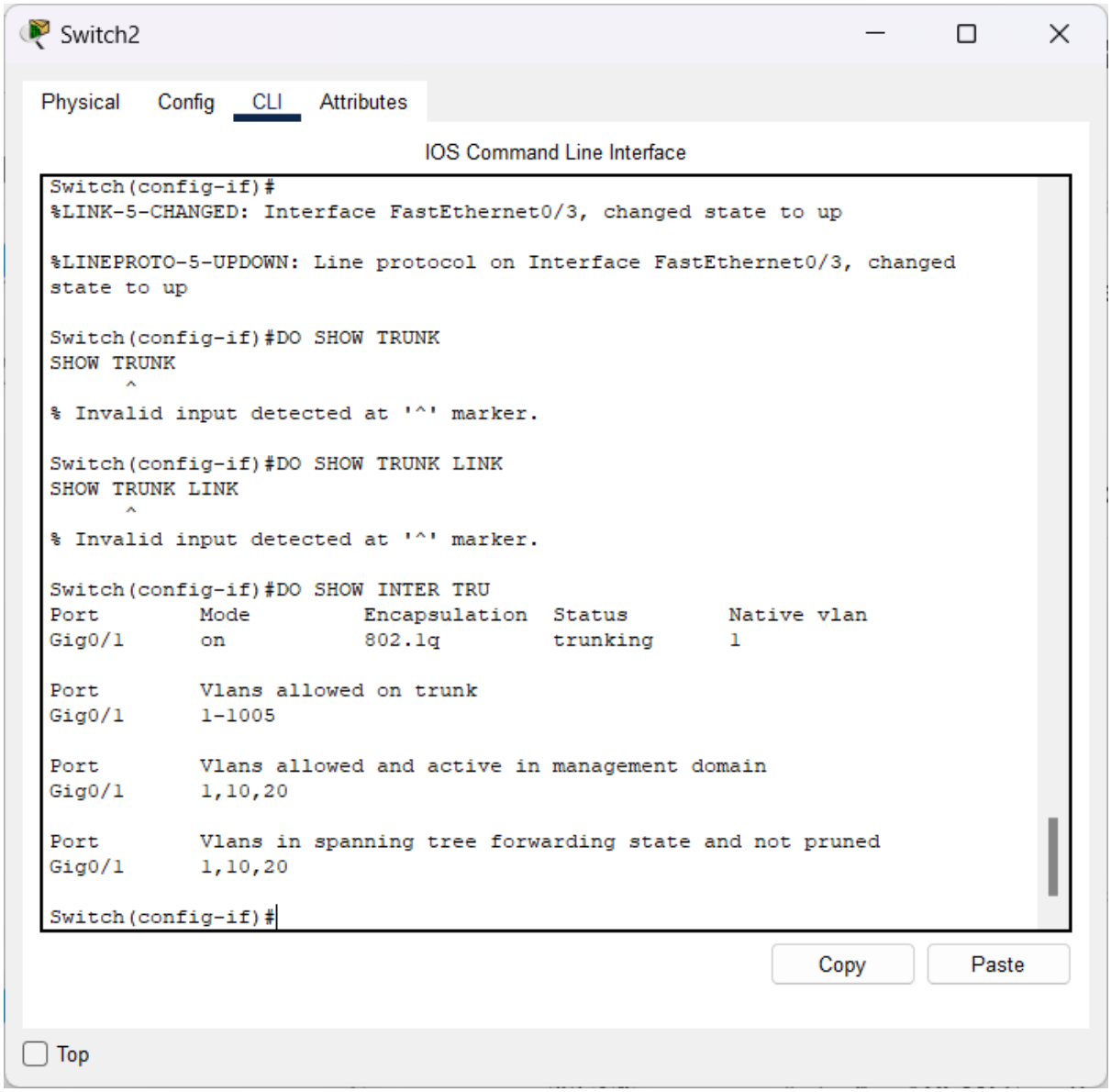
CREATE THE SCOND VLAN ON THE FIRST SWITCH



ALLOW THE FIRST SWITCH CONNECT TO THE SECOND BY TRUNK THE LINK

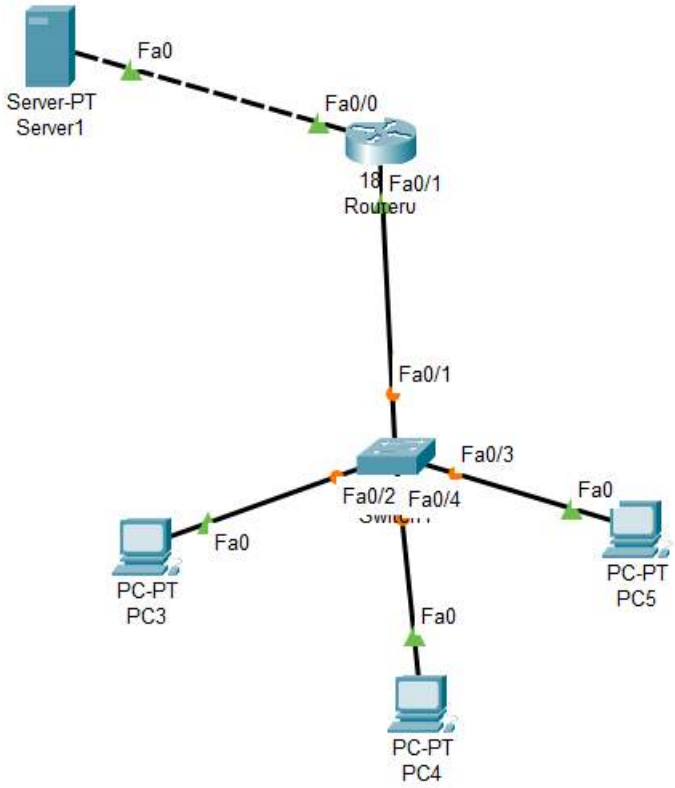


also you can specify only one vlan to see any another vlan in other switch.


Switch2
Physical
Config
CLI
Attributes
IOS Command Line Interface
Switch(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up
Switch(config-if)#DO SHOW TRUNK
SHOW TRUNK
^
% Invalid input detected at '^' marker.
Switch(config-if)#DO SHOW TRUNK LINK
SHOW TRUNK LINK
^
% Invalid input detected at '^' marker.
Switch(config-if)#DO SHOW INTER TRU
Port Mode Encapsulation Status Native vlan
Gig0/1 on 802.1q trunking 1
Port Vlans allowed on trunk
Gig0/1 1-1005
Port Vlans allowed and active in management domain
Gig0/1 1,10,20
Port Vlans in spanning tree forwarding state and not pruned
Gig0/1 1,10,20
Switch(config-if)#
Copy
Paste
Top

File Transfer Protocol (FTP) in Cisco Packet Tracer

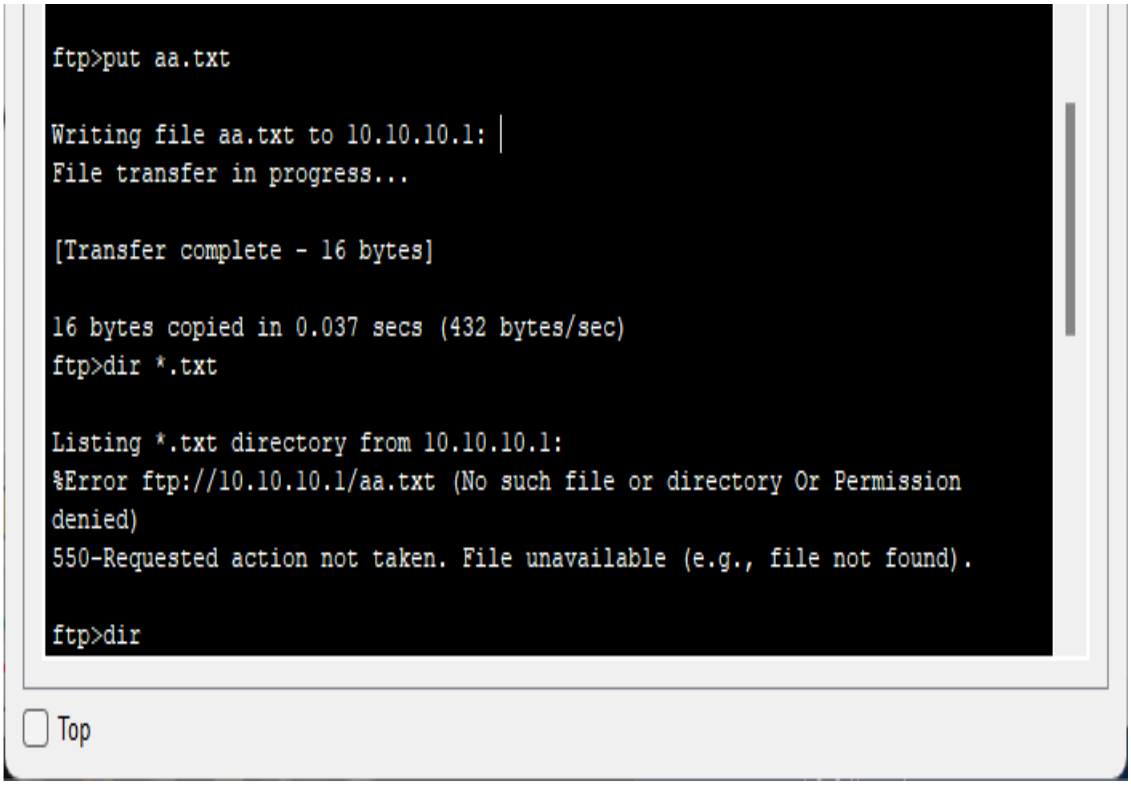
Setting up an FTP server (Learn how to download files from an FTP server)

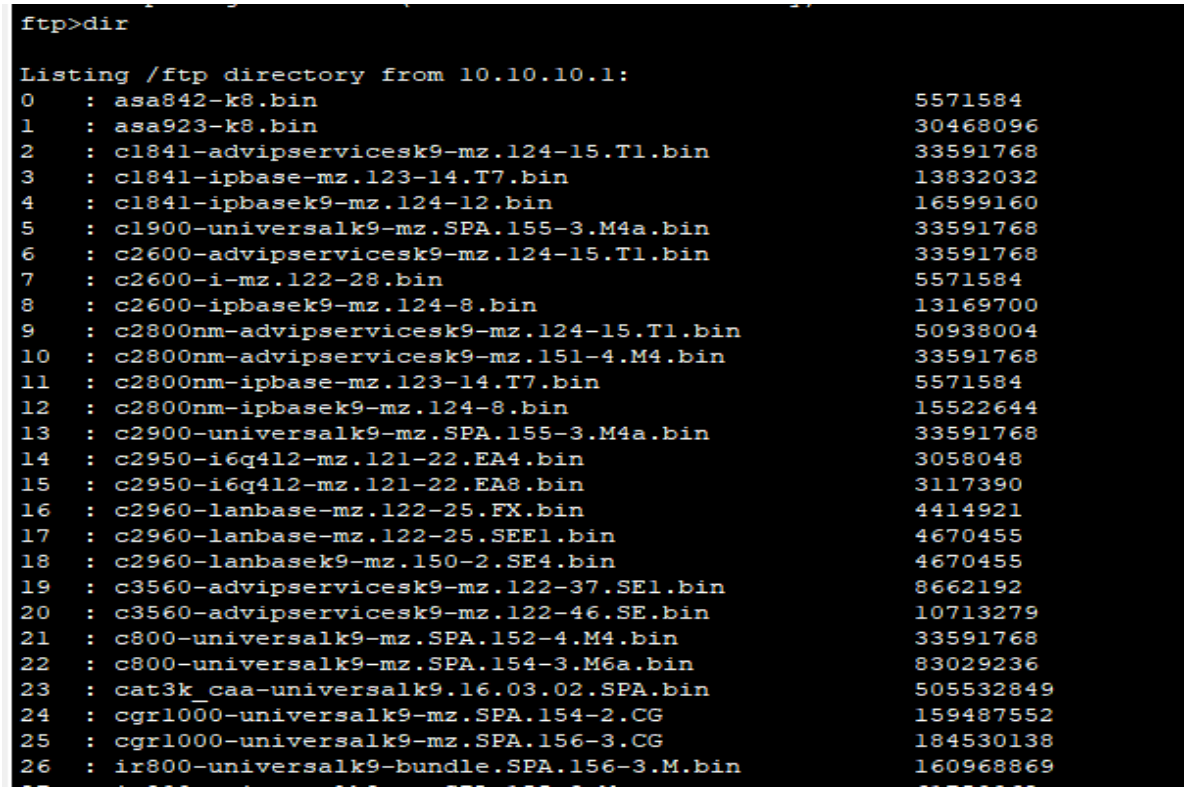


IP address setup for devices

Pc	IP	GETWAY	Switch		
PC1	192.168.1.1	192.168.1.10	2950T-24		
PC2	192.168.1.2	192.168.1.10			
PC3	192.168.1.	192.168.1.10			
ROUTER	192.168.1.10				
SERVER	10.10.10.1	10.10.10.10			

```
C:\>ping 10.10.10.1

Pinging 10.10.10.1 with 32 bytes of data:

Reply from 10.10.10.1: bytes=32 time<1ms TTL=128
Reply from 10.10.10.1: bytes=32 time<1ms TTL=128
Reply from 10.10.10.1: bytes=32 time<1ms TTL=128
Reply from 10.10.10.1: bytes=32 time<1ms TTL=128

Ping statistics for 10.10.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ftp
Cisco Packet Tracer PC Ftp

Usage: ftp target

C:\>ftp 10.10.10.1
Trying to connect...10.10.10.1
Connected to 10.10.10.1
220- Welcome to PT Ftp server
Username:cisco1

%Error ftp://10.10.10.1/ (No such Account)
332- Need account for login



C:\>CISCO1
Invalid Command.

C:\>ftp 10.10.10.1
Trying to connect...10.10.10.1
Connected to 10.10.10.1
220- Welcome to PT Ftp server
Username:CISCO1
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
```

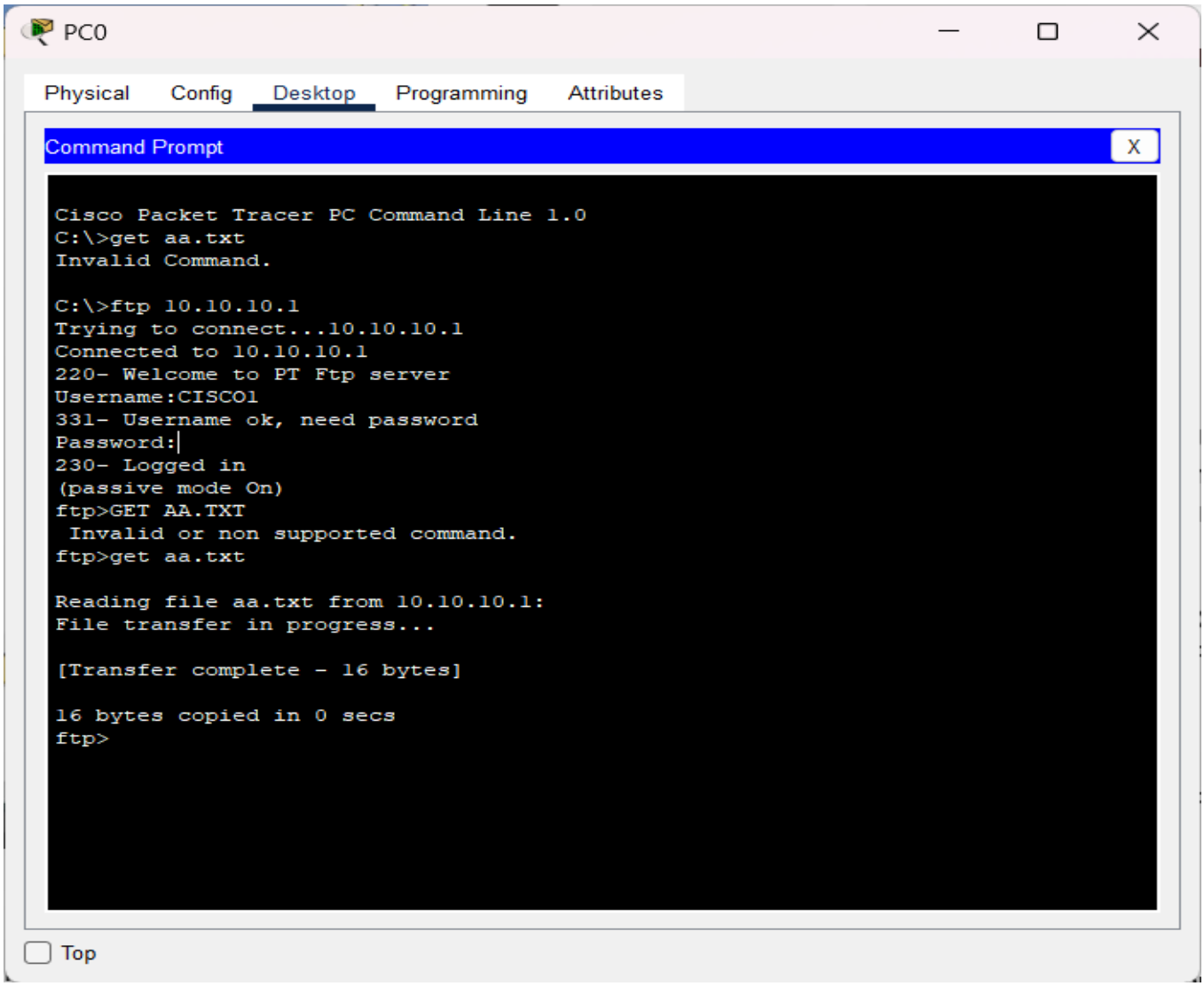




Move to another pc and open command prompt call ftp using

The below command: ftp 10.10.10.1

To connect with the server then ask the server to provide you with the text file that we have moved it from one of pc to the server.



In pc0 type get file name for example(get filename.txt)