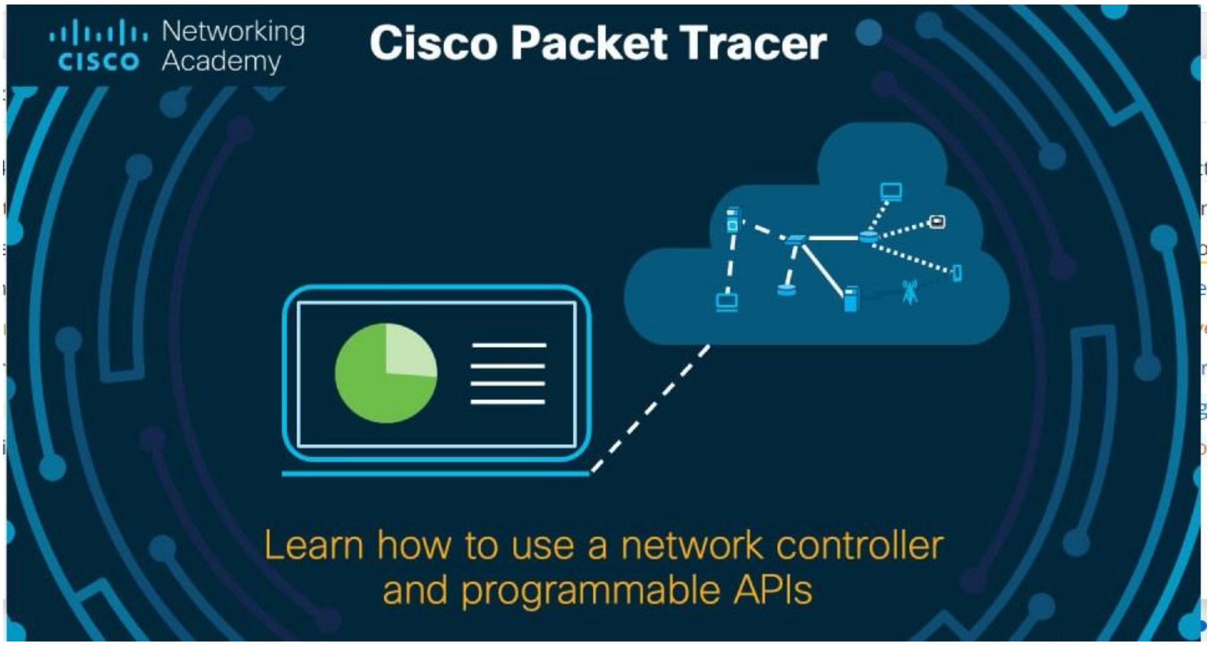
SESSION 1

1.1 INTRODUCTION TO PACKET TRACER

Cisco Packet Tracer is a free application that enables you to practice network configuration and troubleshooting on your desktop or laptop computer. It enables you to mimic networks without having physical access to the underlying hardware. Along with networking, you may improve your Internet of Things (IoT) and cybersecurity skills through education and practice. You have the option of creating a network from scratch, using a pre-built sample network, or completing lab projects. While Packet Tracer is not a substitute for practising on physical routers, switches, firewalls, and servers, it does offer a number of advantages.

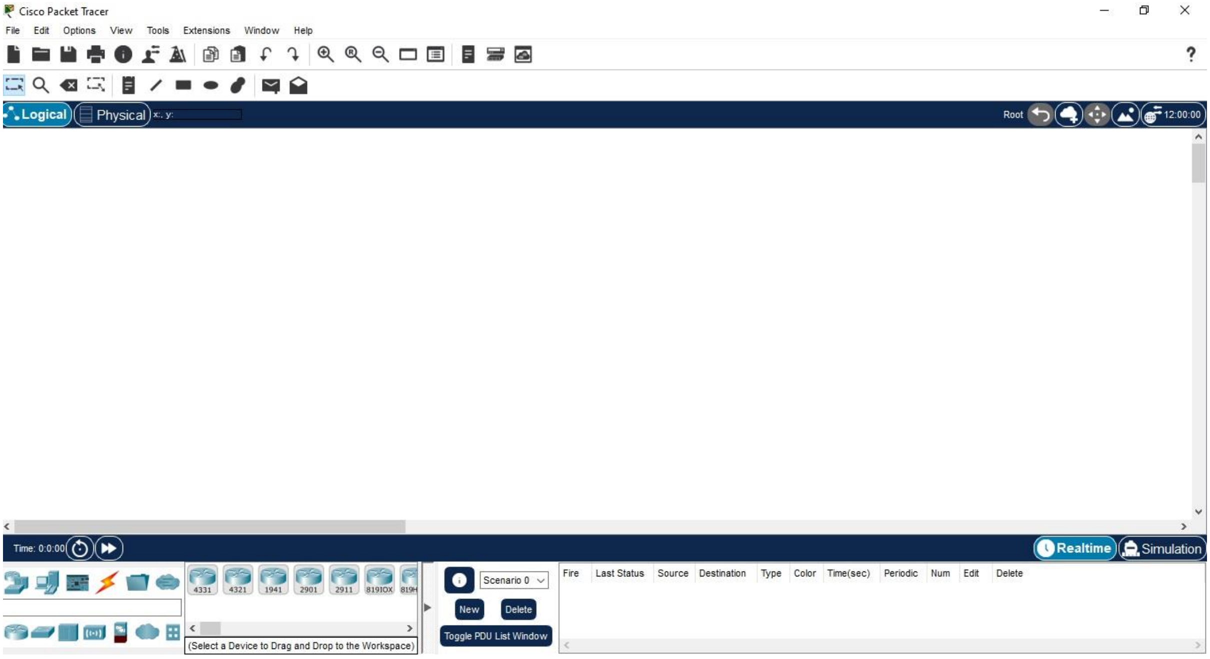


1.a What are the Benefits of Using Packet Tracer?

Imagine being able to peer inside a small business network or the internet. Have you ever wished to create an Internet of Things system that would notify you through the phone if there was an issue in your home environment? Welcome to Cisco Packet Tracer, the simulation environment that may assist you in doing all of these tasks and more. It is intended to familiarize you with the Cisco Packet Tracer network simulation and visualization tool.

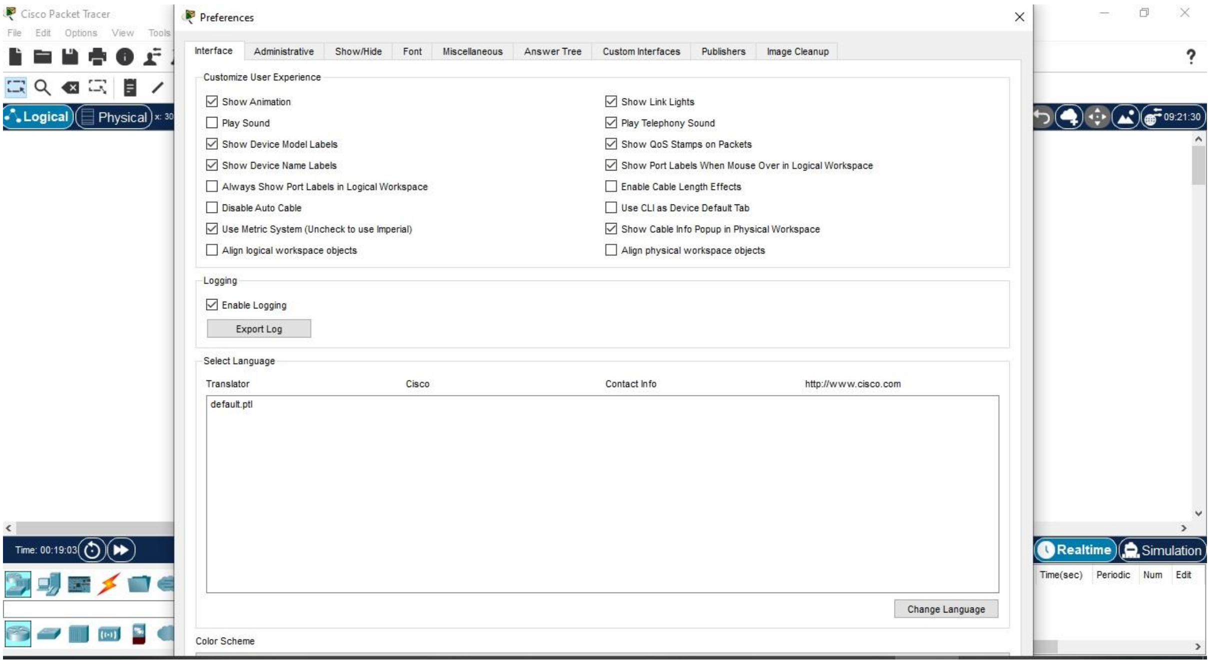
In Packet Tracer, you will design your own network (PT). Additionally, you will learn about the many sorts of PT files.

1.b Packet Tracer UI:


Cisco Packet Tracer
File Edit Options View Tools Extensions Window Help
Logical
Physical
Root
12:00:00
Time: 0:0:00
Realtime
Simulation
4331 4321 1941 2901 2911 819IOX 819H
(Select a Device to Drag and Drop to the Workspace)
Scenario 0
New
Delete
Toggle PDU List Window
Fire Last Status Source Destination Type Color Time(sec) Periodic Num Edit Delete

Packet Tracer is a tool that allows you to simulate real networks. It provides three main menus that you can use for the following:

- Add devices and connect them via cables or wireless.
- Select, delete, inspect, label, and group components within your network.
- Manage your network.


Cisco Packet Tracer
File Edit Options View Tools
Logical
Physical
09:21:30
Time: 00:19:03
Realtime
Simulation
Time(sec) Periodic Num Edit
Preferences
Interface Administrative Show/Hide Font Miscellaneous Answer Tree Custom Interfaces Publishers Image Cleanup
Export Log
Change Language

Customize User Experience

- ☑ Show Animation
- □ Play Sound
- ☑ Show Device Model Labels
- ☑ Show Device Name Labels
- □ Always Show Port Labels in Logical Workspace
- □ Disable Auto Cable
- ☑ Use Metric System (Uncheck to use Imperial)
- □ Align logical workspace objects
- ☑ Show Link Lights
- ☑ Play Telephony Sound
- ☑ Show QoS Stamps on Packets
- ☑ Show Port Labels When Mouse Over in Logical Workspace
- □ Enable Cable Length Effects
- □ Use CLI as Device Default Tab
- ☑ Show Cable Info Popup in Physical Workspace
- □ Align physical workspace objects

Logging

- ☑ Enable Logging

Select Language

Translator	Cisco	Contact Info	http://www.cisco.com
default.ptl			

Color Scheme

The network management menu lets you do the following:

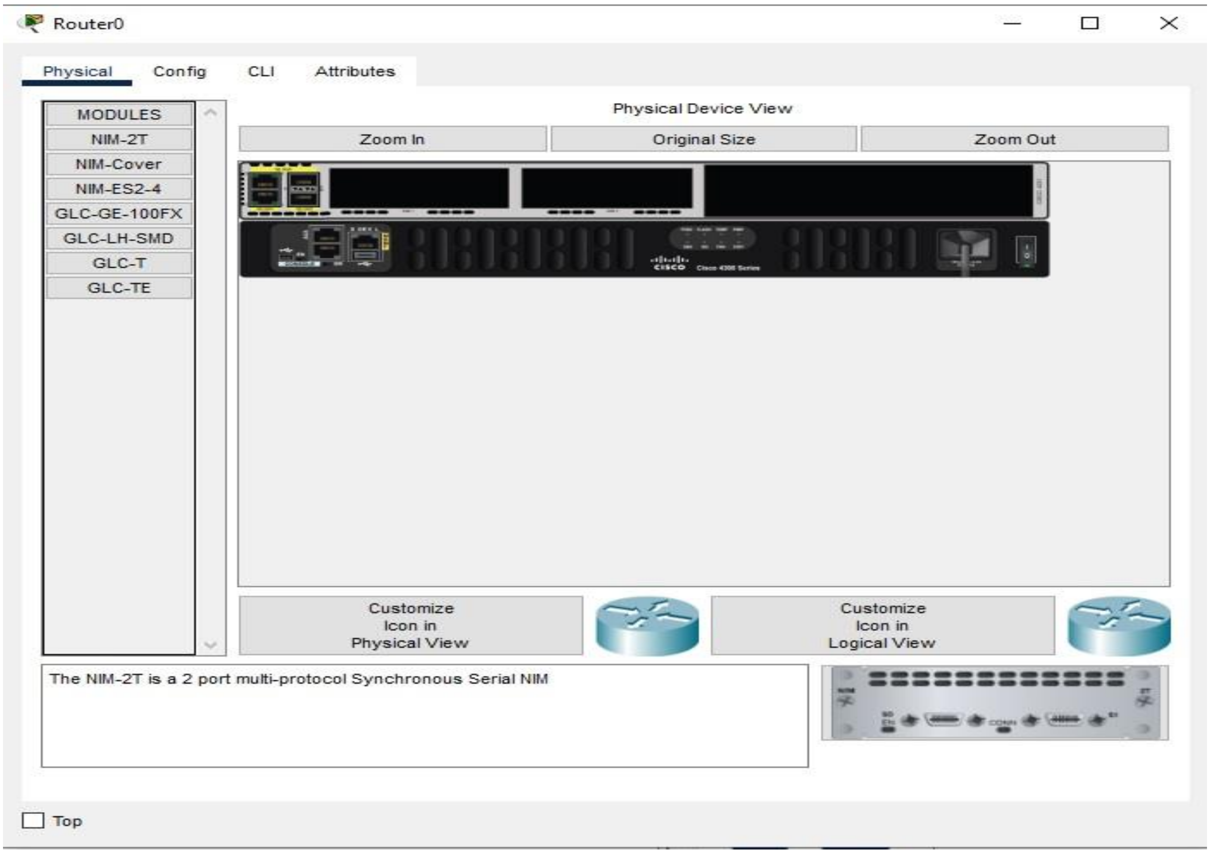
- Open an existing/sample network.
- Save your current network.
- Modify your user profile or your preferences.

Packet Tracer also provides a variety of tabs for device configuration including the following:

- Physical
- Config
- CLI
- Desktop
- Services

The tabs that are shown depend on the device you are currently configuring.

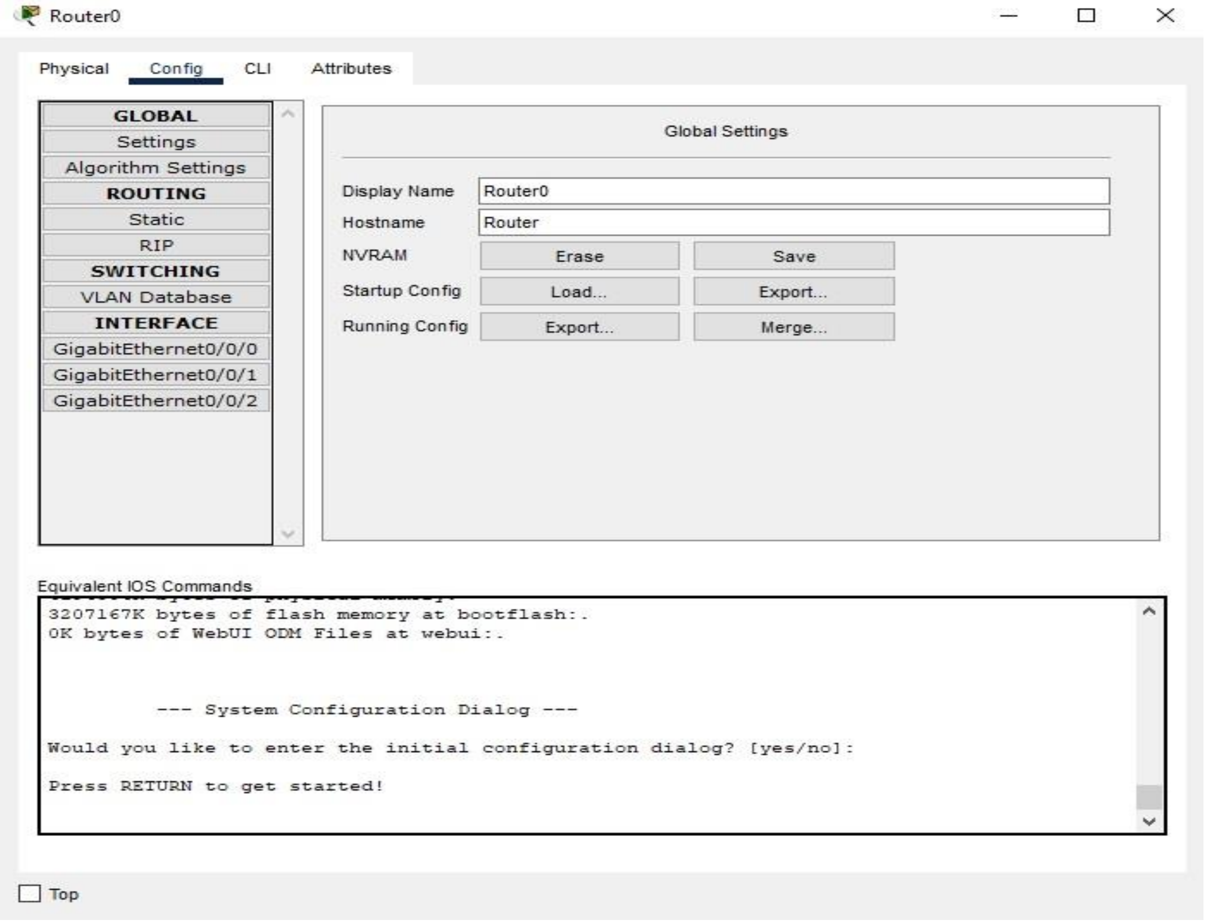
Physical Tab



The NIM-2T is a 2 port multi-protocol Synchronous Serial NIM

The Physical tab provides an interface for interacting with the device including powering it on or off or installing different modules, such as a wireless network interface card (NIC).

Config Tab



Display Name: Router0

Hostname: Router

NVRAM

Startup Config

Running Config

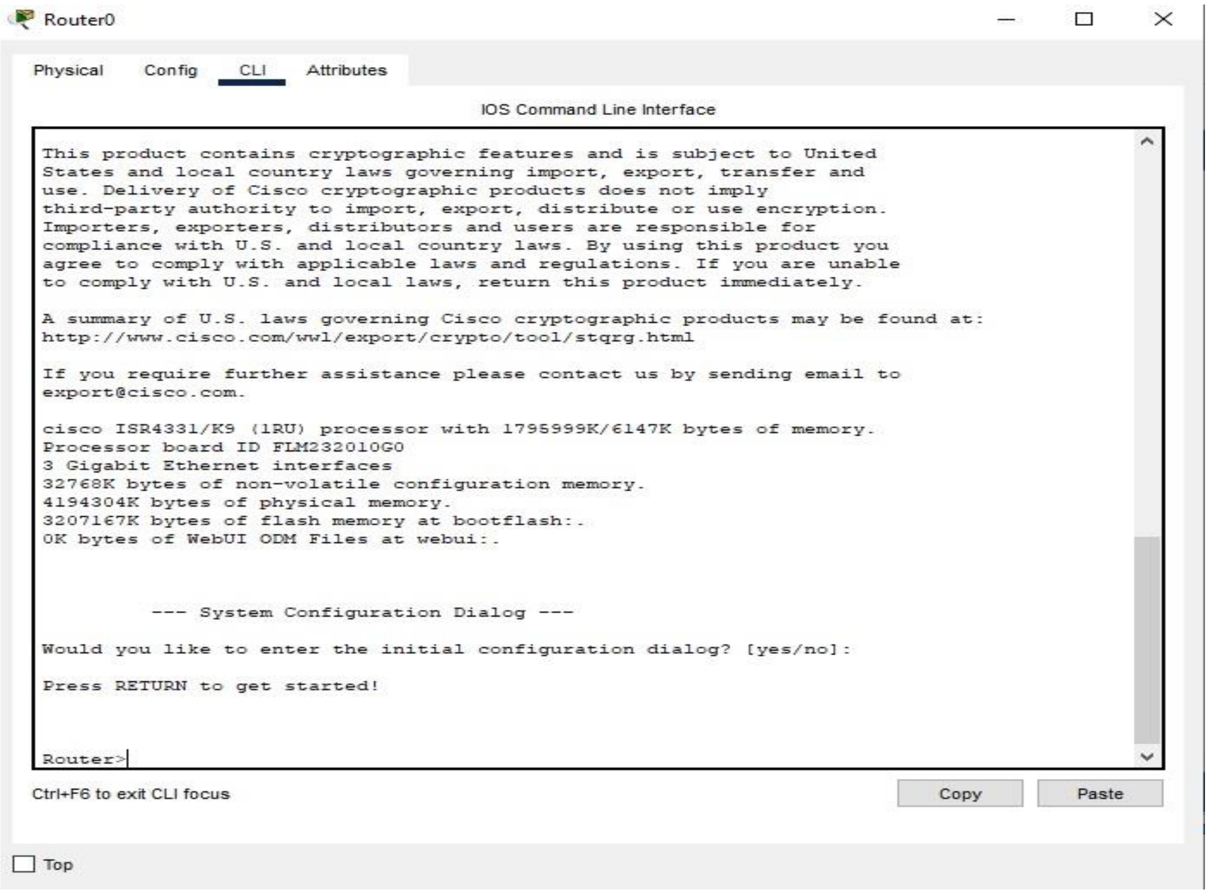
```
3207167K bytes of flash memory at bootflash:.
0K bytes of WebUI ODM Files at webui:.


         --- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]:

Press RETURN to get started!
```

For intermediate devices such as routers and switches, there are two ways to access device configurations. Configurations can be accessed via a Config tab, which is a Graphical User Interface (GUI). Configurations can also be accessed using a command line interface (CLI).

The Config tab does not simulate the functionality of a device. This tab is unique to Packet Tracer. If you don’t know how to use the command line interface, this tab provides a way to use a Packet Tracer-only GUI to configure basic settings. As settings are changed in the GUI, the equivalent CLI commands appear in the Equivalent IOS Commands window. This helps you to learn the CLI commands and the Cisco Internetwork Operating System (IOS) while you are using the Config tab.

For example, in the figure, the user has configured MyRouter as the name of the device. The Equivalent IOS Commands window shows the IOS command that achieves the same results in the CLI. In addition, device configuration files can be saved, loaded, erased, and exported here.

CLI Tab

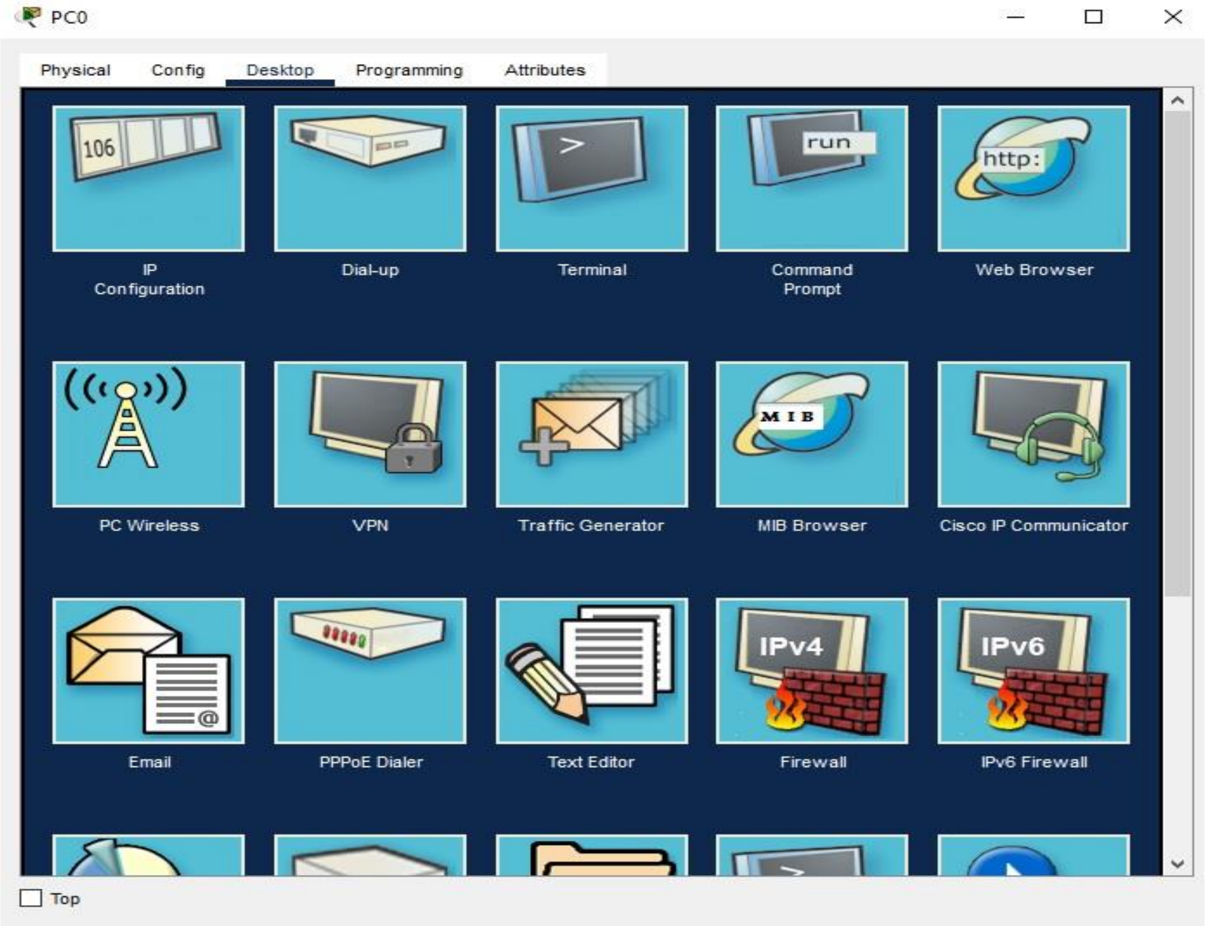


```
This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

cisco ISR4331/K9 (1RU) processor with 1795999K/6147K bytes of memory.
Processor board ID FLM232010G0
3 Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
4194304K bytes of physical memory.
3207167K bytes of flash memory at bootflash:.
0K bytes of WebUI ODM Files at webui:.



         --- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]:

Press RETURN to get started!


Router>
```

The CLI tab provides access to the command line interface of a Cisco device. Using the CLI tab requires knowledge of device configuration with IOS. Here, you can practice configuring Cisco devices at the command line. CLI configuration is a necessary skill for more advanced networking implementations.

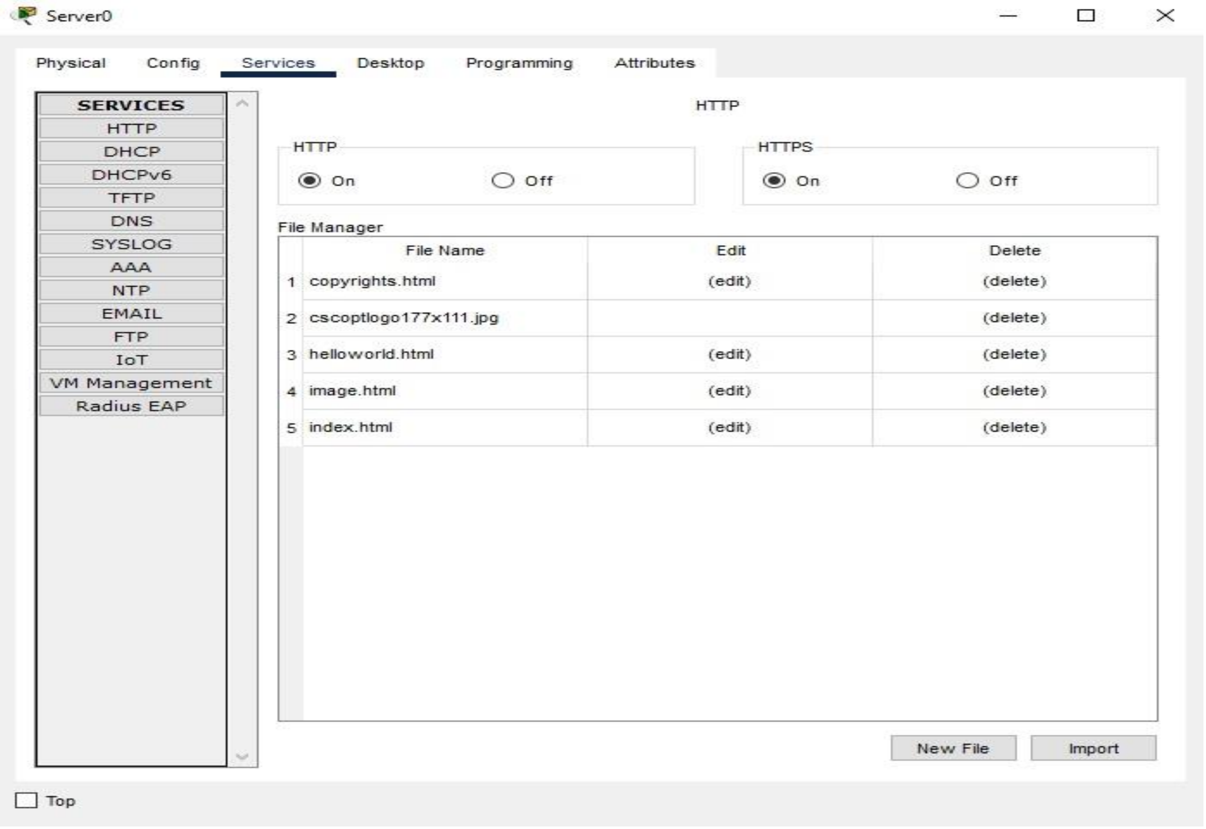
Note: Any commands that were entered from the Config tab are also shown in the CLI tab.

Desktop Tab



For some end devices, such as PCs and laptops, Packet Tracer provides a desktop interface that gives you access to IP configuration, wireless configuration, a command prompt, a web browser, and other applications.

Services Tab



Server0

Physical | Config | Services | Desktop | Programming | Attributes

SERVICES: HTTP, DHCP, DHCPv6, TFTP, DNS, SYSLOG, AAA, NTP, EMAIL, FTP, IoT, VM Management, Radius EAP

HTTP

HTTP: ● On ○ Off

HTTPS: ● On ○ Off

File Manager

	File Name	Edit	Delete
1	copyrights.html	(edit)	(delete)
2	cscoptlogo177x111.jpg		(delete)
3	helloworld.html	(edit)	(delete)
4	image.html	(edit)	(delete)
5	index.html	(edit)	(delete)

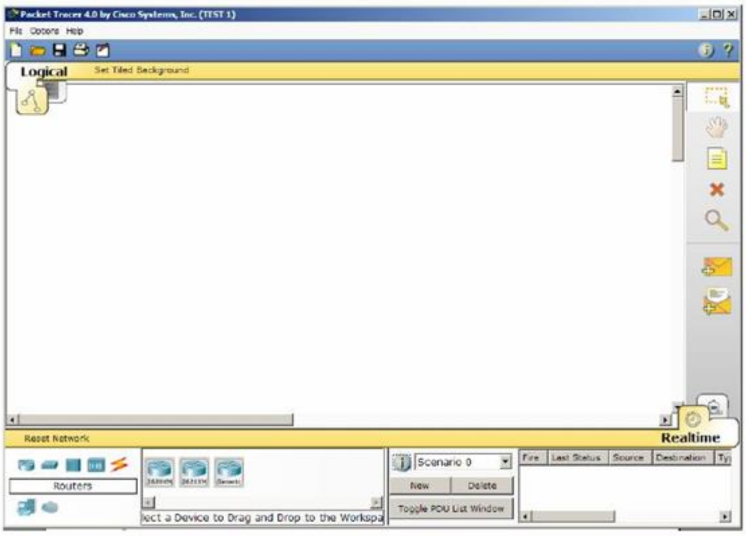
New File | Import

□ Top

A server has all of the functions of a host with the addition of one more tab, the Services tab. This tab allows a server to be configured with common server processes such as HTTP, DHCP, DNS, or other services, as shown in the figure.

1.3 Demonstration of Packet Tracer Interface using a Hub Topology

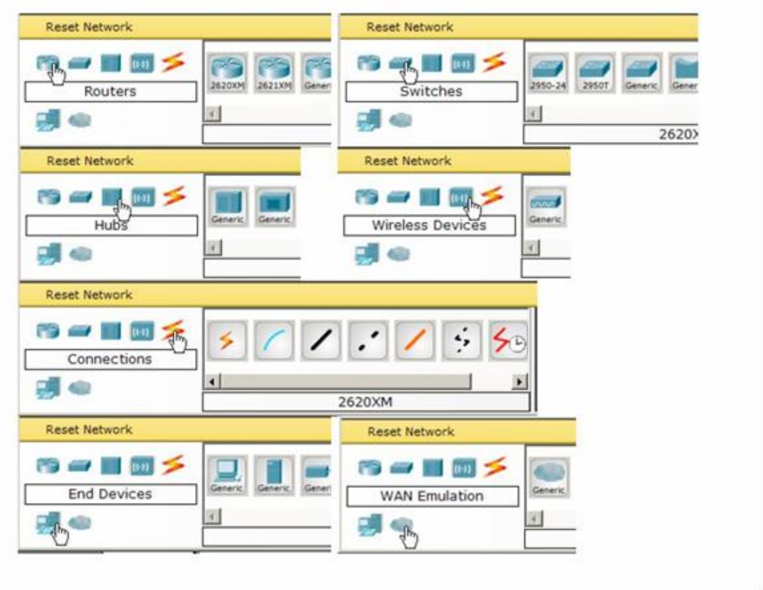
Step 1: Start Packet Tracer and Enter Simulation Mode



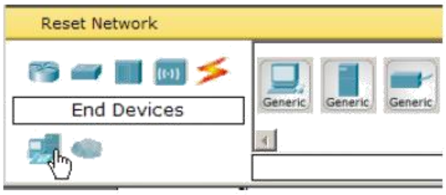
Step 2: Choosing Devices and Connections

We will begin building our network topology by selecting devices and the media in which to connect them. Several types of devices and network connections can be used. For this lab we will keep it simple by using End Devices, Switches, Hubs, and Connections.

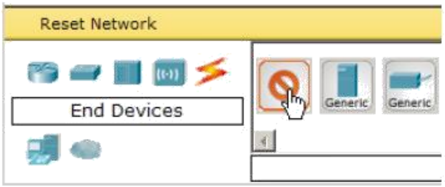
A single click on each group of devices and connections to display the various choices.



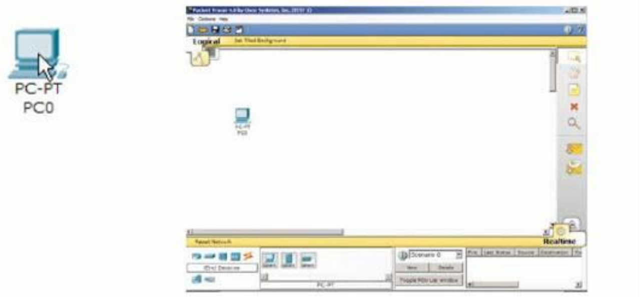
Step 3: Building the Topology – Adding Hosts Single click on the End Devices.



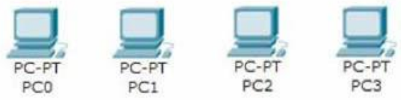
Single click on the **Generic** host.



Move the cursor into the topology area. You will notice it turns into a plus "+" sign. Single-click in the topology area and it copies the device.

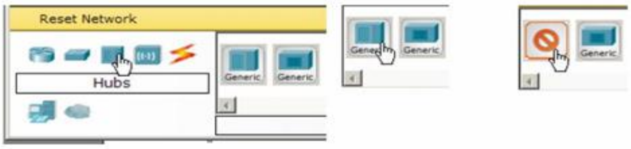


Add three more hosts.

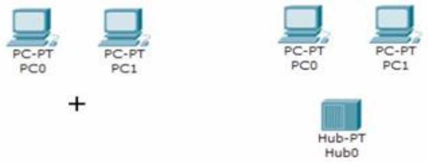


Step 4: Building the Topology – Connecting the Hosts to Hubs and Switches

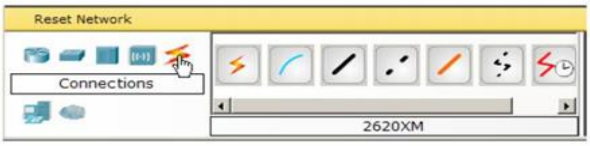
Adding a Hub - Select a hub, by clicking once on Hubs and once on a Generic hub.



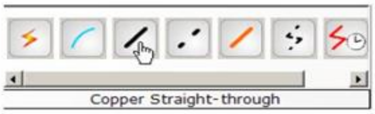
Add the hub by moving the plus sign "+" below PC0 and PC1 and click once.



Connect PC0 to Hub0 by first choosing **Connections.**

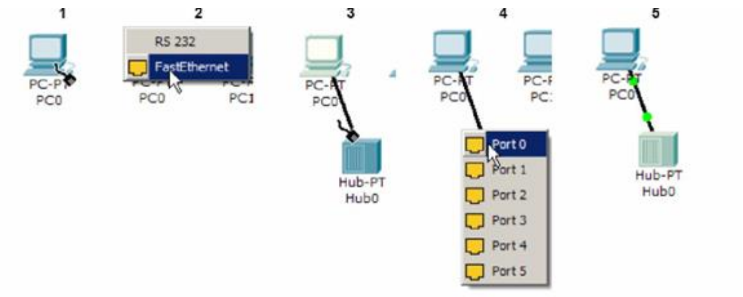


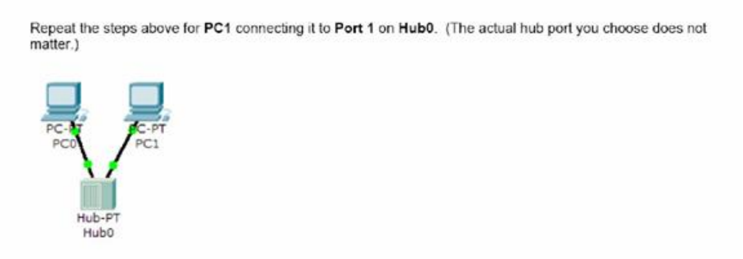
Click once on the **Copper Straight-through** cable.



Perform the following steps to connect PC0 to Hub0:

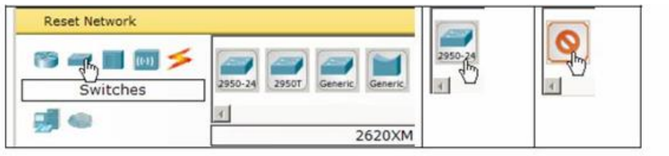
1. Click once on PC0
2. Choose FastEthernet
3. Drag the cursor to Hub0
4. Click once on Hub0 and choose Port 0
5. Notice the green link lights on both the PC0 Ethernet NIC and the Hub0 Port 0 showing that the link is active.



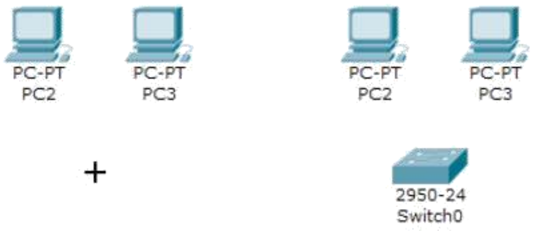


Repeat the steps above for **PC1** connecting it to **Port 1** on **Hub0**. (The actual hub port you choose does not matter.)

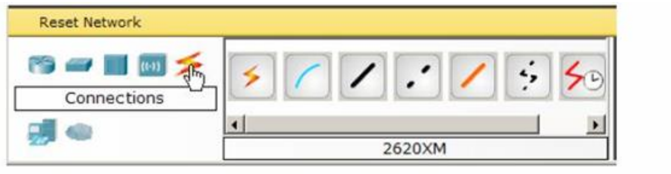
Adding a Switch - Select a switch, by clicking once on Switches and once on a 2950-24 switch.



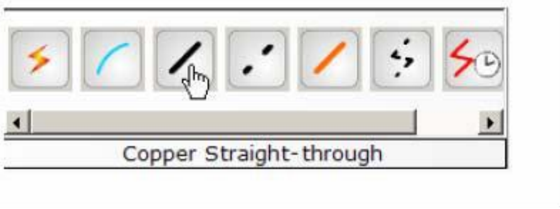
Add the switch by moving the plus sign “+” below PC2 and PC3 and click once.



Connect PC2 to Hub0 by first choosing Connections.

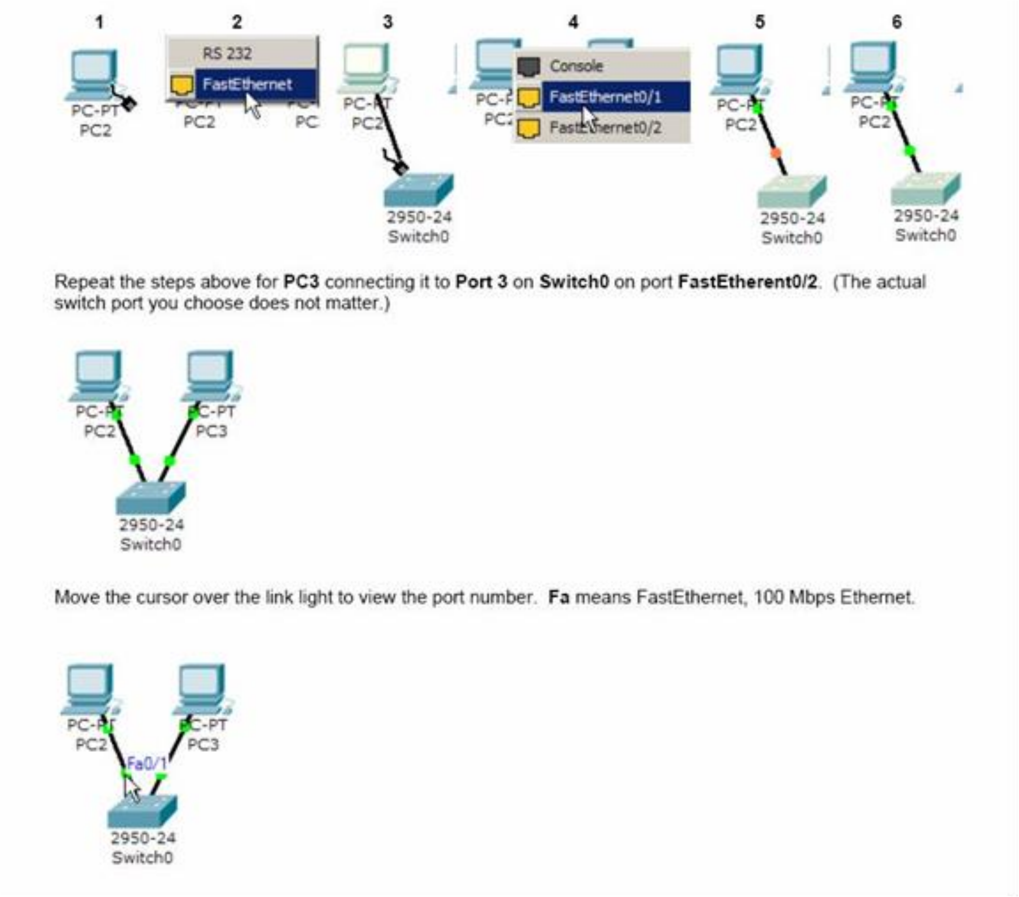


Click once on the Copper Straight-through cable.



Perform the following steps to connect PC2 to Switch0:

1. Click once on PC2
2. Choose FastEthernet
3. Drag the cursor to Switch0
4. Click once on Switch0 and choose FastEthernet0/1
5. Notice the green link lights on PC2 Ethernet NIC and amber light Switch0 FastEthernet0/1 port. The switch port is temporarily not forwarding frames, while it goes through the stages for the Spanning Tree Protocol (STP) process.
6. After a about 30 seconds the amber light will change to green indicating that the port has entered the forwarding stage. Frames can now forwarded out the switch port.



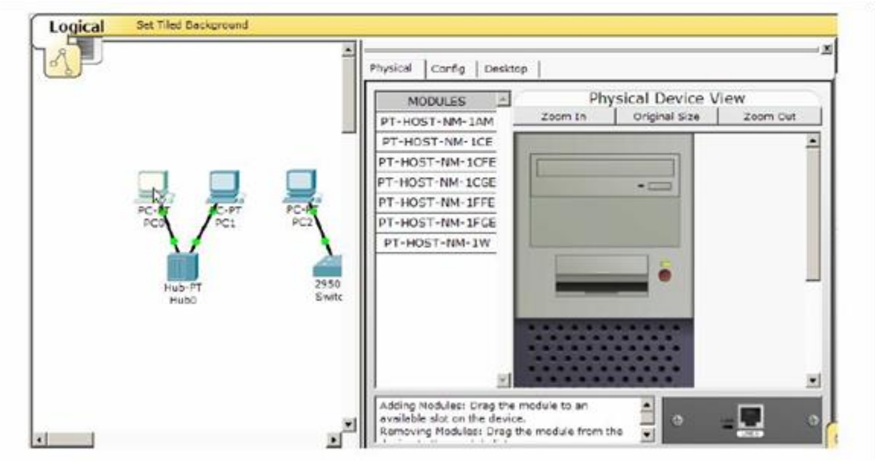
Repeat the steps above for **PC3** connecting it to **Port 3** on **Switch0** on port **FastEtherent0/2**. (The actual switch port you choose does not matter.)

Move the cursor over the link light to view the port number. **Fa** means FastEthernet, 100 Mbps Ethernet.

Step 5: Configuring IP Addresses and Subnet Masks on the Hosts

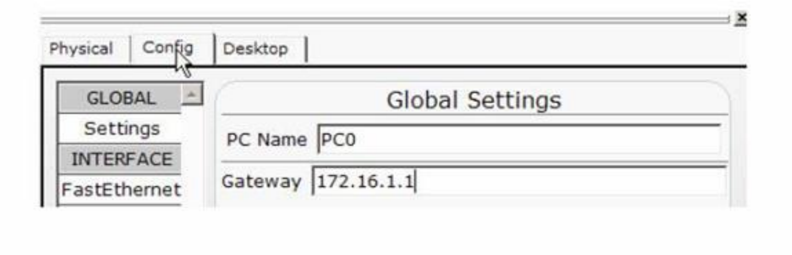
Before we can communicate between the hosts we need to configure IP Addresses and Subnet Masks on the devices.

Click once on PC0.



Adding Modules: Drag the module to an available slot on the device.
Removing Modules: Drag the module from the

Choose the Config tab. It is here that you can change the name of PC0. It is also here where you would enter a Gateway IP Address, also known as the default gateway. We will discuss this later, but this would be the IP address of the local router. If you want, you can enter the IP Address 172.16.1.1, although it will not be used in this lab.

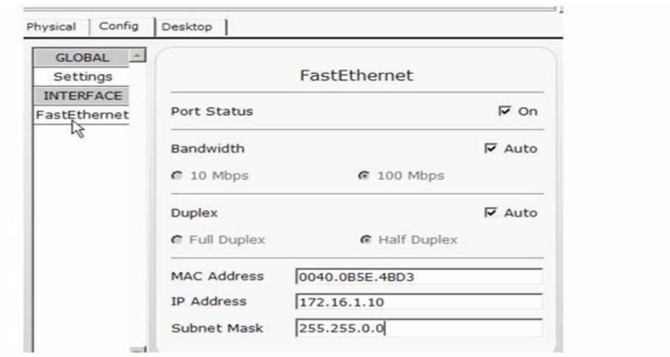


Global Settings

PC Name PC0

Gateway 172.16.1.1

Click on FastEthernet. Although we have not yet discussed IP Addresses, add the IP Address to 172.16.1.10. Click once in the Subnet Mask field to enter the default Subnet Mask. You can leave this at 255.255.0.0. We will discuss this later.



FastEthernet

Port Status ☑ On

Bandwidth ☑ Auto

○ 10 Mbps ● 100 Mbps

Duplex ☑ Auto

○ Full Duplex ● Half Duplex

MAC Address 0040.0B5E.4BD3

IP Address 172.16.1.10

Subnet Mask 255.255.0.0

Also, notice this is where you can change the Bandwidth (speed) and Duplex of the Ethernet NIC (Network Interface Card). The default is Auto (autonegotiation), which means the NIC will negotiate with the hub or switch. The bandwidth and/or duplex can be manually set by removing the check from the Auto box and choosing the specific option.

Bandwidth - Auto

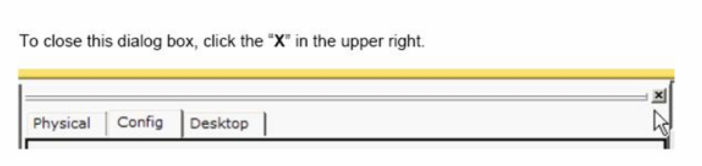
If the host is connected to a hub or switch port which can do 100 Mbps, then the Ethernet NIC on the host will choose 100 Mbps (Fast Ethernet). Otherwise, if the hub or switch port can only do 10 Mbps, then the Ethernet NIC on the host will choose 10 Mbps (Ethernet).

Duplex - Auto

Hub: If the host is connected to a hub, then the Ethernet NIC on the host will choose Half Duplex.

Switch: If the host is connected to a switch, and the switch port is configured as Full Duplex (or Autonegotiation), then the Ethernet NIC on the host will choose Full Duplex. If the switch port is configured as Half Duplex, then the Ethernet NIC on the host will choose Half Duplex. (Full Duplex is a much more efficient option.)

The information is automatically saved when entered.



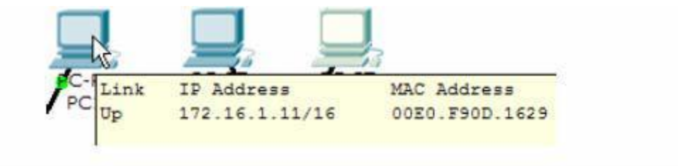
To close this dialog box, click the "X" in the upper right.

Repeat these steps for the other hosts. Use the information below for IP Addresses and Subnet Masks.

Host	IP Address	Subnet Mask
PC0	172.16.1.10	255.255.0.0
PC1	172.16.1.11	255.255.0.0
PC2	172.16.1.12	255.255.0.0
PC3	172.16.1.13	255.255.0.0

Verify the information

To verify the information that you entered, move the Select tool (arrow) over each host.



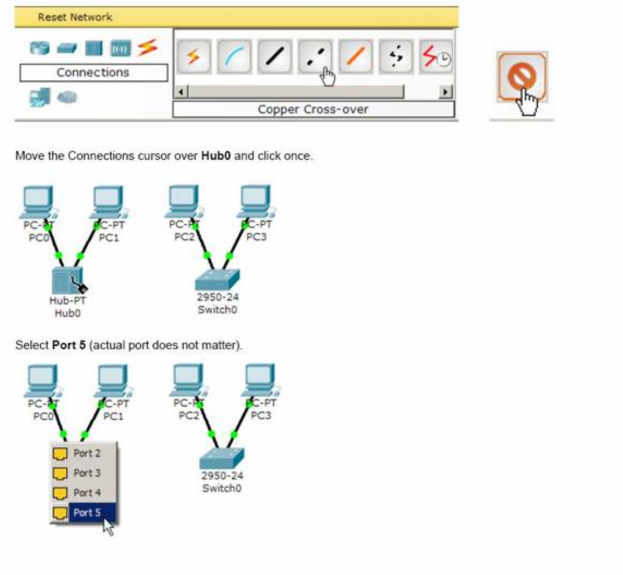
Link	IP Address	MAC Address
Up	172.16.1.11/16	00E0.F90D.1629

Deleting a Device or Link

To delete a device or link, choose the Delete tool and click on the item you wish to delete.

Step 6: Connecting Hub0 to Switch0

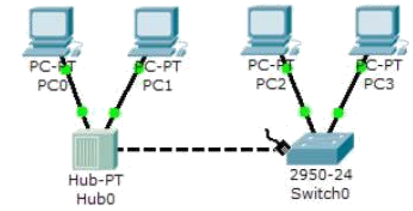
To connect like-devices, like a Hub and a Switch, we will use a Cross-over cable. Click once the Cross-over Cable from the Connections options.



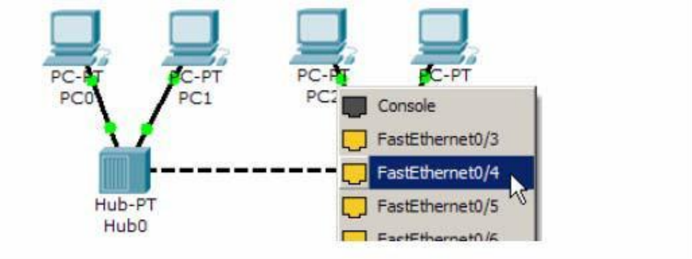
Move the Connections cursor over **Hub0** and click once.

Select **Port 5** (actual port does not matter).

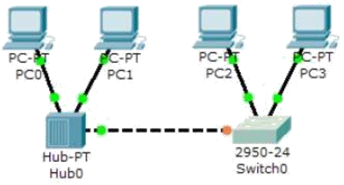
Move the Connections cursor to Switch0.

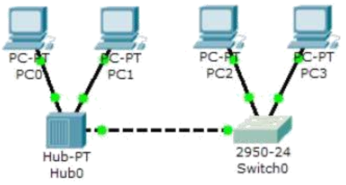


Click once on Switch0 and choose FastEthernet0/4 (actual port does not matter).



The link light for switch port FastEthernet0/4 will begin as amber and eventually change to green as the Spanning Tree Protocol transitions the port to forwarding.





1.2 NETWORKING COMMANDS

VNStat

It is one of the most complete network commands. It works on all Linux and BSD systems, and allows us to monitor network traffic from the console.

- Installation is simple and fairly quick, allowing monitoring of all network interfaces.
- With VNStat we can collect all traffic needed from any configured interface.
- One of the big differences between VNStat and other tools is that VNStat collects kernel data instead of the interface itself, which means a lighter execution for the system.
- It will not require administrator permissions to run.
- It has the ability to store gathered information so your information never goes missing, even if the system crashes or reboots itself.
- You can set Vnstat to listen to traffic, daily or by billing period, as well as many other options.
- It stands out for its flexibility when configuring the reading of traffic.
- Finally, it is possible to set Vnstat output to generate console graphics and even customize them with colours.

Ping (Unix/Windows)

Ping dates from the 70s and is known for being one of the most basic network commands. However, it is not as simple as we believe and has many more uses than those we already know. It is based on the ICMP protocol and is used to determine:

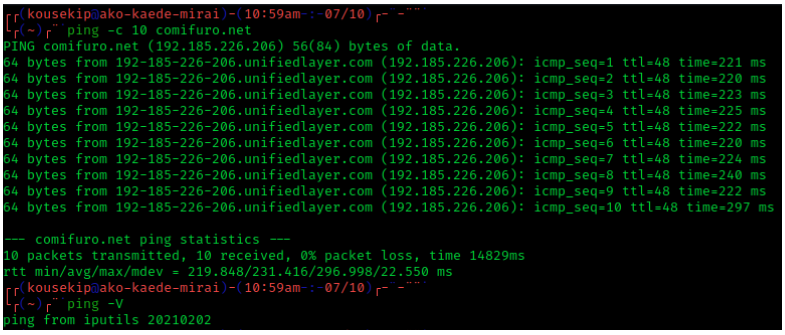
- If there is connectivity between your machine and another machine on the network.
- It’s used to measure the “speed” or latency time.

It is a command that exists on all operating systems that support TCP/IP, and it is a basic command that you should know.

Ping is known for having dozens of parameters and the one that we find more useful is the one responsible for monitoring “the number of packages to send.” There are networks that undo the first package, so it is essential to send at least three so we can check that at least one has arrived without being discarded. For this, we use the -c parameter.

The same technique can be used to determine the loss percentage of packages in our network, sending ten packages and seeing if any gets lost. The number of packages that usually get lost in the network will surprise you. (This tool is included in Pandora FMS)

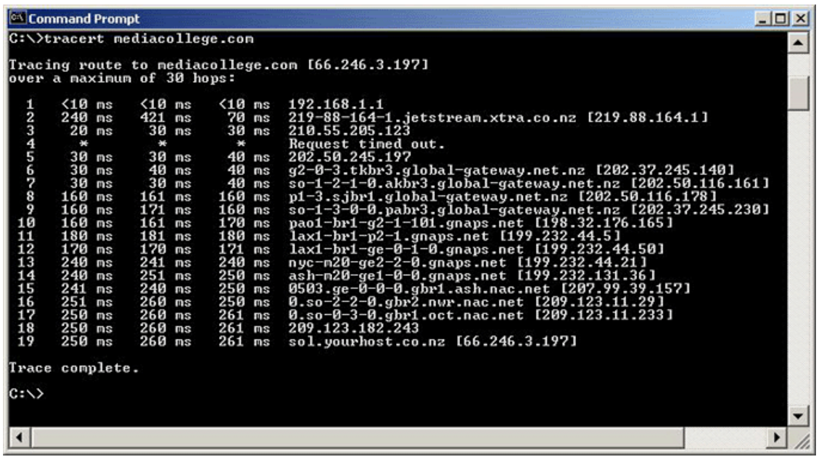
Execution: Ping name/System IP



```
┌┌(kousekip@ako-kaede-mirai)-(10:59am-:-07/10)┌-
└┌(~)┌ ping -c 10 comifuro.net
PING comifuro.net (192.185.226.206) 56(84) bytes of data.
64 bytes from 192-185-226-206.unifiedlayer.com (192.185.226.206): icmp_seq=1 ttl=48 time=221 ms
64 bytes from 192-185-226-206.unifiedlayer.com (192.185.226.206): icmp_seq=2 ttl=48 time=220 ms
64 bytes from 192-185-226-206.unifiedlayer.com (192.185.226.206): icmp_seq=3 ttl=48 time=223 ms
64 bytes from 192-185-226-206.unifiedlayer.com (192.185.226.206): icmp_seq=4 ttl=48 time=225 ms
64 bytes from 192-185-226-206.unifiedlayer.com (192.185.226.206): icmp_seq=5 ttl=48 time=222 ms
64 bytes from 192-185-226-206.unifiedlayer.com (192.185.226.206): icmp_seq=6 ttl=48 time=220 ms
64 bytes from 192-185-226-206.unifiedlayer.com (192.185.226.206): icmp_seq=7 ttl=48 time=224 ms
64 bytes from 192-185-226-206.unifiedlayer.com (192.185.226.206): icmp_seq=8 ttl=48 time=240 ms
64 bytes from 192-185-226-206.unifiedlayer.com (192.185.226.206): icmp_seq=9 ttl=48 time=222 ms
64 bytes from 192-185-226-206.unifiedlayer.com (192.185.226.206): icmp_seq=10 ttl=48 time=297 ms

--- comifuro.net ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 14829ms
rtt min/avg/max/mdev = 219.848/231.416/296.998/22.550 ms
┌┌(kousekip@ako-kaede-mirai)-(10:59am-:-07/10)┌-
└┌(~)┌ ping -V
ping from iputils 20210202
```

Traceroute (Unix/Windows)

The main objective of this tool is to know the traveling path of a package through our network. This network command will tell us where the package is going through (machines, switches, routers) and check that our network is working properly. If you encounter any problems, it will allow us to have a rough idea about where the fault lies.



```
C:\>tracert mediacollege.com

Tracing route to mediacollege.com [66.246.3.197]
over a maximum of 30 hops:

  1    <10 ms   <10 ms   <10 ms  192.168.1.1
  2    240 ms   421 ms    70 ms  219-88-164-1.jetstream.xtra.co.nz [219.88.164.1]
  3     20 ms    30 ms    30 ms  210.55.205.123
  4      *        *        *     Request timed out.
  5     30 ms    30 ms    40 ms  202.50.245.197
  6     30 ms    40 ms    40 ms  g2-0-3.tkbr3.global-gateway.net.nz [202.37.245.140]
  7     30 ms    30 ms    40 ms  so-1-2-1-0.akbr3.global-gateway.net.nz [202.50.116.161]
  8    160 ms   161 ms   160 ms  p1-3.sjbr1.global-gateway.net.nz [202.50.116.178]
  9    160 ms   171 ms   160 ms  so-1-3-0-0.pabr3.global-gateway.net.nz [202.37.245.230]
 10    160 ms   161 ms   170 ms  pao1-br1-g2-1-101.gnaps.net [198.32.176.165]
 11    180 ms   181 ms   180 ms  lax1-br1-p2-1.gnaps.net [199.232.44.5]
 12    170 ms   170 ms   171 ms  lax1-br1-ge-0-1-0.gnaps.net [199.232.44.50]
 13    240 ms   241 ms   240 ms  nyc-m20-ge2-2-0.gnaps.net [199.232.44.21]
 14    240 ms   251 ms   250 ms  ash-m20-ge1-0-0.gnaps.net [199.232.131.36]
 15    241 ms   240 ms   250 ms  0503.ge-0-0-0.gbr1.ash.nac.net [207.99.39.157]
 16    251 ms   260 ms   250 ms  0.so-2-2-0.gbr2.nwr.nac.net [209.123.11.29]
 17    250 ms   260 ms   261 ms  0.so-0-3-0.gbr1.oct.nac.net [209.123.11.233]
 18    250 ms   260 ms   261 ms  209.123.182.243
 19    250 ms   260 ms   261 ms  sol.yourhost.co.nz [66.246.3.197]

Trace complete.

C:\>
```

Execution:

traceroute –n (on Unix / Linux)

tracert –d (on Windows)

Arp (Unix/Windows)

This network command is used to change and view the ARP table, which contains the mappings between the IP address and the MAC address. It only sees the connections in our local area network segment (LAN), so it could be called “low level”. However, it’s used to discover what machines are directly connected to our host or what machines we are connected to. It is a diagnostic tool, and sometimes it can be interesting to monitor it in order to discard ARP Poisoning attacks, which are one of the most common forms of phishing attacks in local networks.

Execution: arp –a

Curl and wget (Unix/ Windows)

These are essential commands to do HTTP, HTTPS or FTP requests to remote servers. It allows you to download files or whole web pages, even recursively (it literally allows us to make a “copy” of a website, including images). It supports cookies and allows you to send POST requests, in addition to “simulate a” user agent, use a http proxy or even a SOCKS4/5 proxy.

One of the most common utilities in integration with Pandora FMS, is to verify the contents of a specific web page. Because wget / curl allows us to download the entire contents of a web, it is easy to compare the MD5 of that content with a value previously verified. If it changes, it means that the Web has been altered.

Netstat (Unix/Windows)

Network command identifies all TCP connections and UDP open on a machine. Besides this, it allows us to know the following information:

- Routing tables to meet our network interfaces and its outputs.
- Ethernet statistics that show sent and received packages and possible errors.
- To know the id of the process that is being used by the connection.
- Netstat is another basic command as Ping that meets many elementary functions.

Whois (Unix/ Windows)

This network command is used to query data domains: to find out who owns the domain, when that domain expires, to view the configured logs, contact details, etc. Its use is highly recommended to contact the administrators of the domains or when incidents of migration of services such as mail and web happen.

To use ‘whois’ on Windows you need to download the software from this url: https://technet.microsoft.com/en-us/sysinternals/whois.aspx

SSH (Unix/Linux/Windows)

Command to run terminals on remote machines safely. SSH allows any user to run a console just by registering and entering his credentials. So you can run the commands you want as if you were in local.

More details you need to know about SSH:

Putty is recommended when using SSH in Windows. You can find it here: http://www.putty.org/

- To enable a remote computer to connect to our server via SSH, an SSH server must be installed and set up as FreeSSHd.
- SSH also allows to obtain an interactive remote Shell, execute remote commands and copy files in both directions.
- SSH is the natural replacement of classic tools like Telnet or FTP, and has become a basic tool in the administration of systems over the years. It is extremely powerful despite its complex combinations of symmetric encryption and authentication schemes, and verification, and it is the target of continuous attacks.

TCPDump (Unix/Linux/Windows)

It is one of the “basic” tools of network commands, and when used right, goes on to become a great ally for network administrators, system administrators or programmers.

TCPDump is an advanced command used to inspect traffic from different interfaces of a machine so you can get the exchanged packages. You can dump output to file so then you can analyse it with more powerful sniffers and graphical interfaces such as Wireshark. For Windows, you must use WinDump.

Ngrep (Unix/Linux/Windows)

- The grep command power is taken to the network.

- It is a TCPDump with a substring text filter in real time.
- It has a very powerful filtering system for regular expressions and it is typically used to process files generated by tcpdump, wireshark, etc.
- It is a communication package filter over HTTP, SMTP, FTP, DNS and other protocols.

NMAP (Unix/Windows)

NMAP is considered the father of the general network scanners. Although today there are more reliable tools for some tasks (like Fping), NMAP is a very versatile tool for scanning networks. It is used to determine which hosts are alive in a network and to do different ways of scanning.

Netcat (Windows/Unix)

NetCat, or NC, is the network command most versatile that exists nowadays and one of the lightest. However, its use requires some imagination. Only if you've played with scripting, you will understand the subtlety of its name: NetCat. It is a tool designed to be used as a destination of a redirect (one pipe or |). It is used to send or receive information about a connection. For example, a WEB request to service would be something as simple as:

```
echo -e “GET http://pandorafms.com HTTP/1.0\n\n” | nc pandorafms.com 80
```

Lsof (Unix/Windows)

The ‘lsof’ command is not only used as a network tool, but also is used to identify which files have an open process. In Unix environments, a file can be a network connection, so that is used to know which ports have an open particular running process, something extremely useful in specific cases.

IPtraf (Linux)

Special command to obtain traffic statistics. It has a ncurses interface (text) to analyze real-time traffic passing through an interface. It allows you to work at low-level and to see what pairs of connections are established on each machine, and to see in detail the traffic connection of every pair, all in real-time.

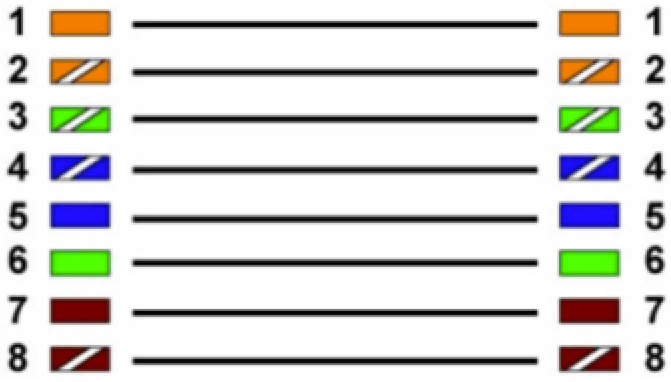
Exercise 2: Cabling – Straight Through and Cross-over Cabling

Ethernet cable:

An Ethernet cable is a network cable used for high-speed wired network connections between two devices. This network cable is made of four-pair cable, which is consists of twisted pair conductors. It is used for data transmission at both ends of the cable, which is called RJ45 connector.

The Ethernet cables are categorized as Cat 5, Cat 5e, Cat 6, and UTP cable. Cat 5 cable can support a 10/100 Mbps Ethernet network while Cat 5e and Cat 6 cable to support Ethernet network running at 10/100/1000 Mbps.

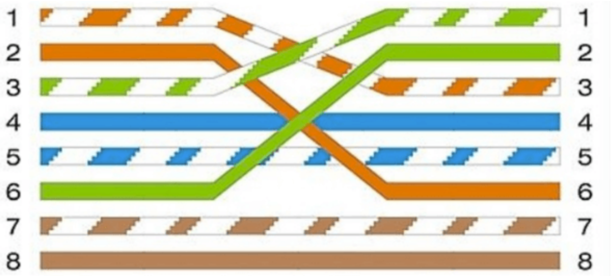
Straight Through Cable:



Straight Through Cable

Straight-through cable is a type of CAT5 with RJ-45 connectors at each end, and each has the same pin out. It is in accordance with either the T568A or T568B standards. It uses the same color code throughout the LAN for consistency. This type of twisted-pair cable is used in LAN to connect a computer or a network hub such as a router. It is one of the most common types of network cable.

Crossover Cable:



Crossover Cable