**LAB MANUAL**

**COURSE Title: Computer Networks**

**Course Code: CS-577**

**Credit Hours: 4(3-3)**



Prepared By:

**Dr. Kashif Sattar (Coordinator)**

**Mr. Adeel Shahid (TA)**

University Institute of Information Technology

PMAS-Arid Agriculture University, Rawalpindi

**Table of Contents**

|  |  |  |
| --- | --- | --- |
| **Lab #** | **Topics Covered** | **Page #** |
| Lab # 01 | Ping and Traceroute Commands |  |
| Ping and Traceroute Commands for customized information |
| Lab # 02 | Basic Network Commands on windows (ipconfig etc) |  |
| Basic Network Commands on Linux (ifconfig etc) |
| Lab # 03 | LAN Cable Construction (Cat-6, Cross vs Straight Cable) |  |
| LAN Cable Testing (Cross vs Straight Cable) |
| Lab # 04 | Building a Physical LAN using switch |  |
| Resource (File/Printer) sharing in LAN |
| Lab # 05 | Introduction & Installation of Wireshark Network Monitor |  |
| GUI understanding, Packet Capturing and Analyzing |
| Lab # 06 | Analysing Frame Header on Wireshark (Layer-2) |  |
|  |
| Lab # 07 | CISCO Packet Tracer, Introduction and Installation |  |
| Building LAN on Packet Tracer and message passing |
| Lab # 08 | Configuration and Installation of Physical Switch and GUI Understanding |  |
| VLAN Configuration |
| Lab # 09 | Configuration and Installation of Physical Router and GUI Understanding |  |
| Analysing Datagram Header on Wireshark (Layer-3) |
| Lab # 10 | Design Problem Using Router |  |
| PC Network TCP/IP Configuration. |
| Lab # 11 | Basic OSPF Configuration |  |
| Basic EIGRP Configuration |  |
| Lab # 12 | Analysing Segment Header on Wireshark (Layer-4) |  |
| Well Known Port identification through packet capturing in wireshark |
| Lab # 13 | Analyzing Layer 5 for Encrypted and Unencrypted Traffic |  |
|  |

 **LAB # 01**

**Lab Title:**

Ping and Traceroute Commands for generic and customized information

**Lab Objective:**

Objective of this lab is to make students understand the use of ping and traceroute commands of network for generic and customized information.

**Activity Outcomes:**

The student will understand the advantages of ping and traceroute commands.

**Introduction:**

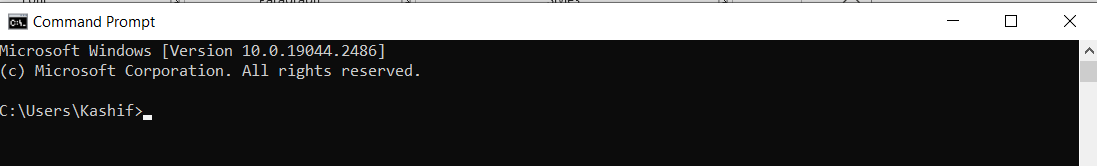
Ping uses the Internet Control Message Protocol(ICMP) echo-request and echo-reply feature to test physical connectivity. Because ping reports on four attempts (by default in windows), it gives an indication the reliability of the connection. Look over the result and verify that the ping was successful. Was the ping successful? If not, report to the instructor.

**Activity-1(Solved):**

**Network Ping Command (Windows)**

1. **Command Prompt:**

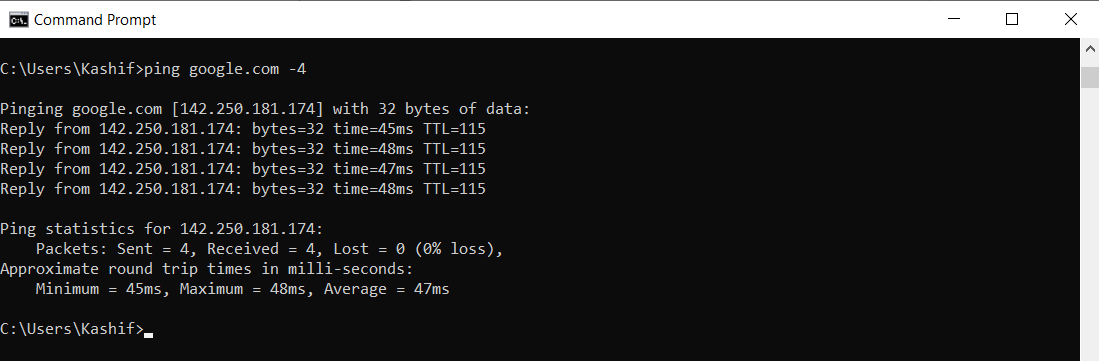
It takes input command from user in a text-based user interface. > sign is used as a separator and before that you have path of working directory. E.g:



1. **ping [specific address e.g. google.com]**

**Command:**

**C:\Users\Kashif>ping google.com**

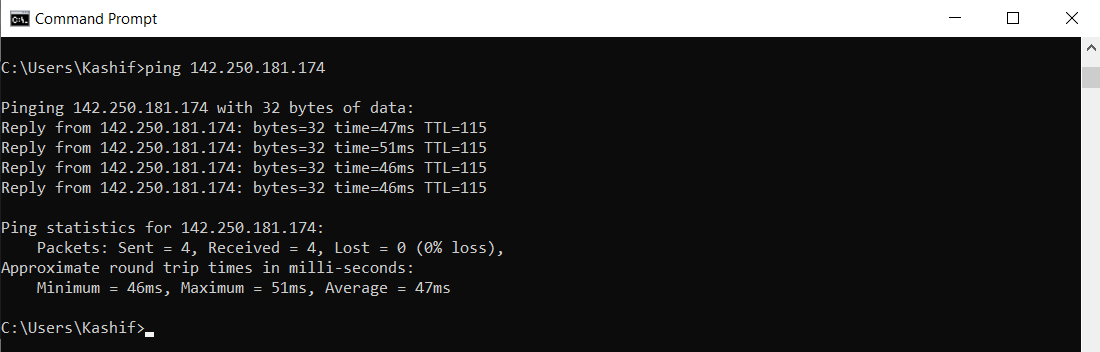
****

Note: Sometimes ping command shows IPv6 address by default, so to show IPv4 address you need to type -4 at the end of ping command as shown above.

1. **ping [IP Address]** //We can ping with IP address directly

**Command:**

**C:\Users\Kashif>ping 142.250.181.174**

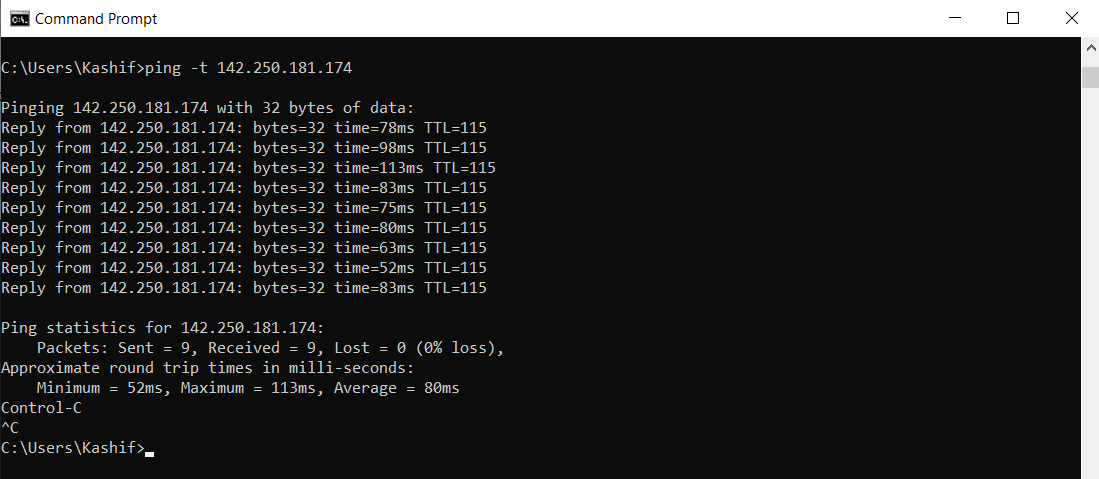


1. **ping -t [specific address]** // for continuous ping until stopped with ctrl^c

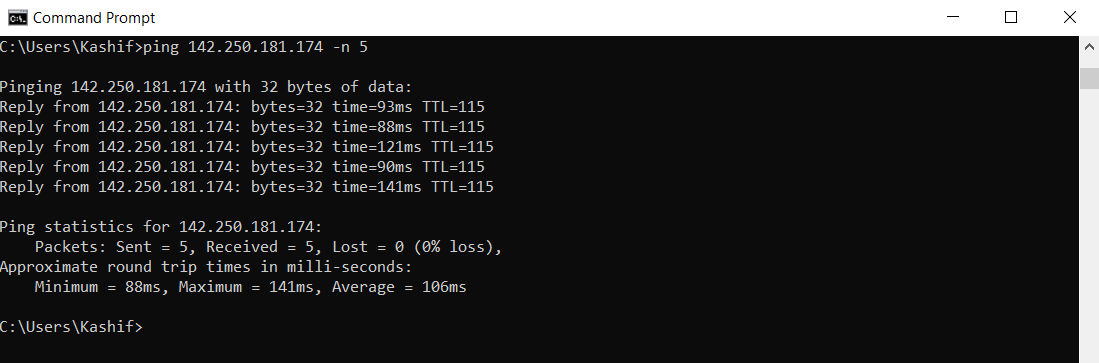
// for 5 pings, ping -n 5 google.com

**Command:**

**C:\Users\Kashif>ping -t google.com**



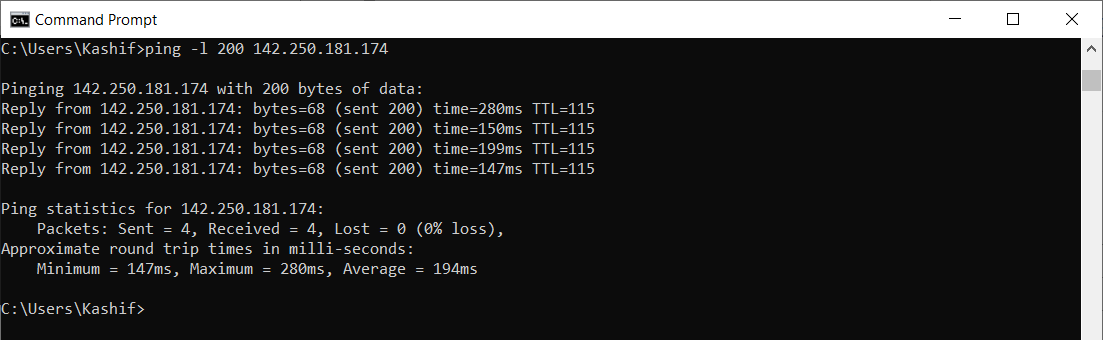
//-n 5 for 5 pings



1. **ping -l [Pkt Size in Bytes] [specific address]** // for change pkt size from default 32 to 200 upto 65500

**Command:**

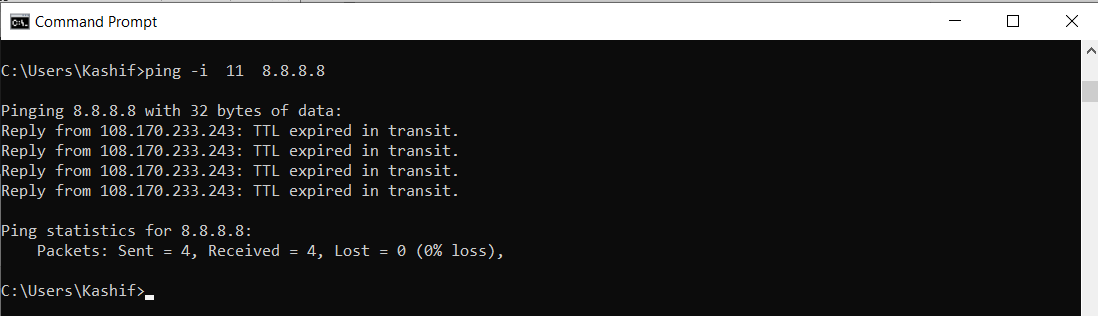
**C:\Users\Kashif> ping -l 200 google.com**



1. **ping -i [TTL in number] [specific address]** //-i 2 for setting TTL=2, 8.8.8.8 public DNS server

**Command:**

**C:\Users\Kashif> ping -i 2 8.8.8.8**

****

1. **ping 127.0.0.1** //for loopback testing

**Command:**

**C:\Users\Kashif> ping 127.0.0.1**

**Explanation:**

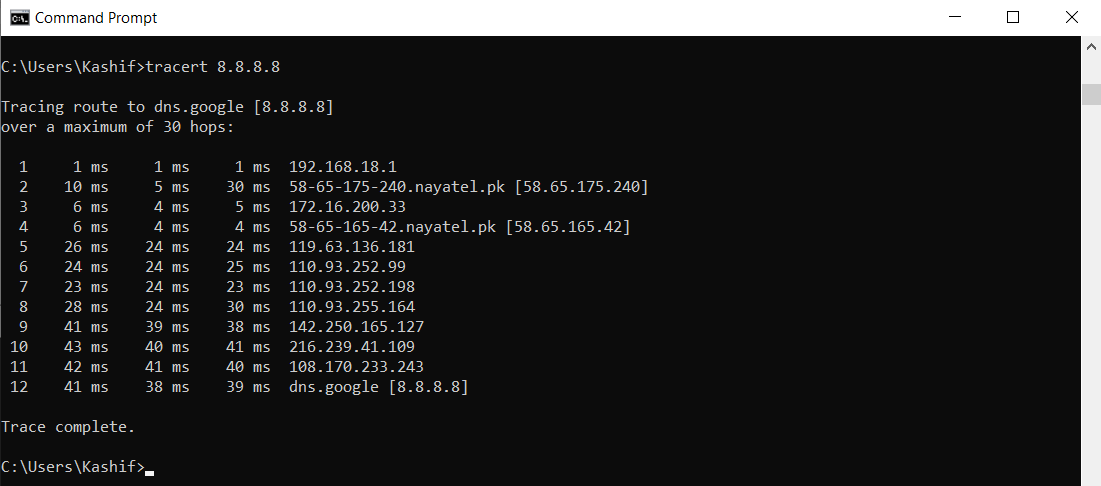
The address 127.0.0.1 is reserved for loopback testing. If the ping is successful, then TCP/IP is properly installed and functioning on this computer. Packets sent to this address never reach the network but are looped through the network interface card only. This can be used for diagnostic purposes to verify that the internal path through the TCP/IP protocols is working.

**Network Trace Route Command**

1. **tracert [specific address or IP]**

**Command:**

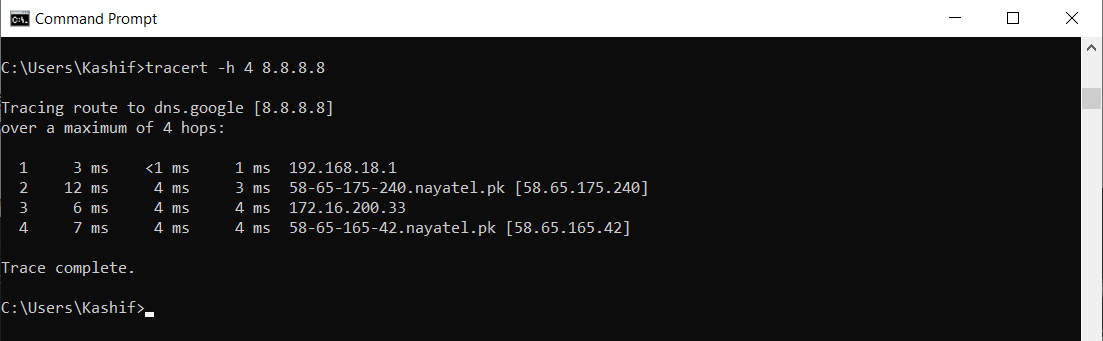
**C:\Users\Kashif> tracert 8.8.8.8**



1. **tracert -h [max\_hops] [specific address or IP] //Max. number of hops to search for target.**

**Command:**

**C:\Users\Kashif> tracert -h 4 8.8.8.8**



**Activity-2(Students will do their self):**

**Find the equivalent of all above commands in linux and execute. Also paste the screen shots of the outputs.**



**LAB # 02**

**Lab Title:**

Basic Network Commands on windows and Linux

**Lab Objective:**

Objective of this lab is to make students understand the use of network important commands for generic and customized information about the network configuration.

**Activity Outcomes:**

The student will understand the advantages of network commands and configuration.

**Introduction:**

The network infrastructure is a very complex structure of cables, routers, access points, data packets, and a many other small components that together make the entire network work seamlessly. Any issue in any of these smaller components may lead to an overall collapse of the network infrastructure. This may lead to disruption of WiFi, cellular and wired (ethernet) infrastructure. This is the reason why it's very important to have an access to how the network is performing and know troubleshooting techniques, namely networking commands, which are used at the command prompt to get network information.

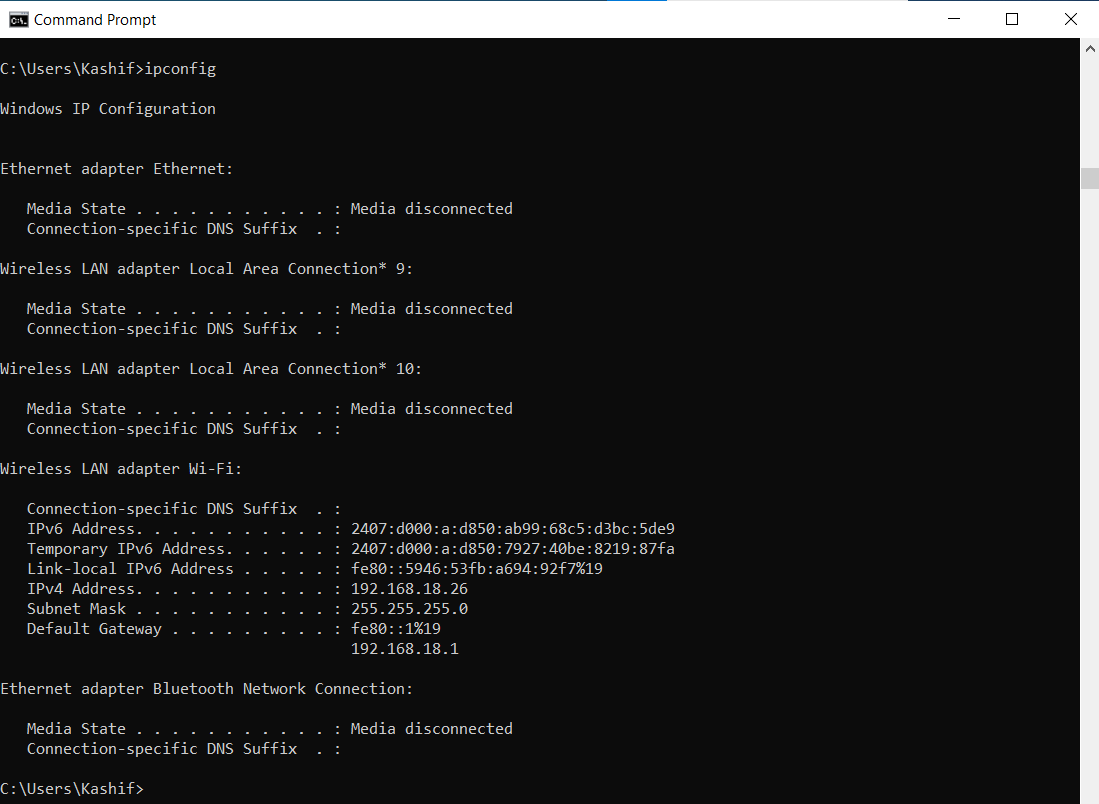
Networking commands are used at the command prompt to get network information like the IP address of the system (remember that an IP address is the address of your device in a network), MAC address, network route traversed by a packet, and the IP address of the server in which a website or URL is hosted.

The IP address and the default gateway should be in the same network or subnet; otherwise this host wouldn’t be able to communicate outside the network

**Activity-1:**

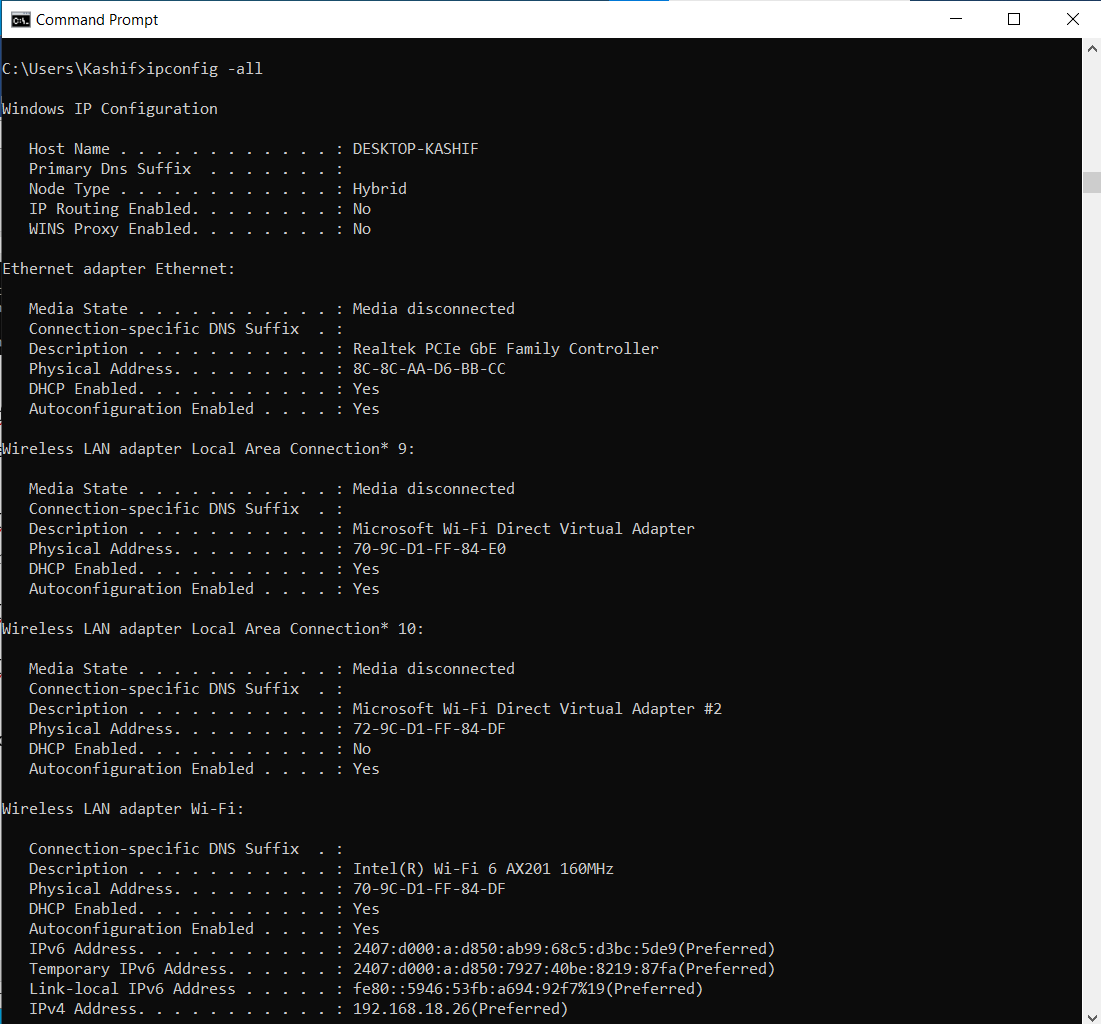
1. **Network ipconfig command (**Internet Protocol Configuration**):**

The IPCONFIG network command provides a comprehensive view of information regarding the [IP address](https://www.simplilearn.com/tutorials/cyber-security-tutorial/what-is-an-ip-address) configuration of the device we are currently working on.



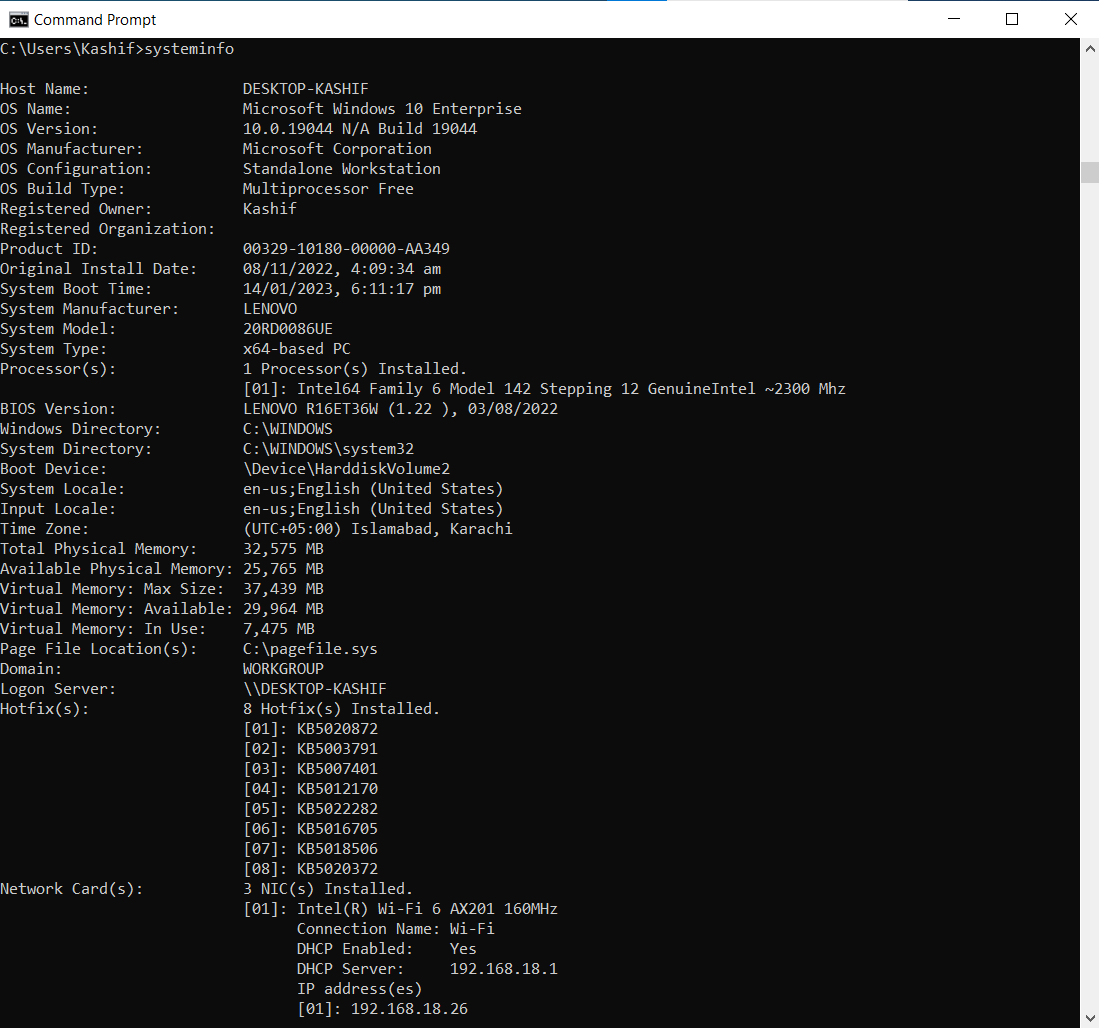
The IPConfig command also provides us with some variation in the primary command that targets specific system settings or data, which are:

* IPConfig/all - Provides primary output with additional information about network adapters.
* IPConfig/renew - Used to renew the system’s IP address.
* IPConfig/release - Removes the system’s current IP address.

****

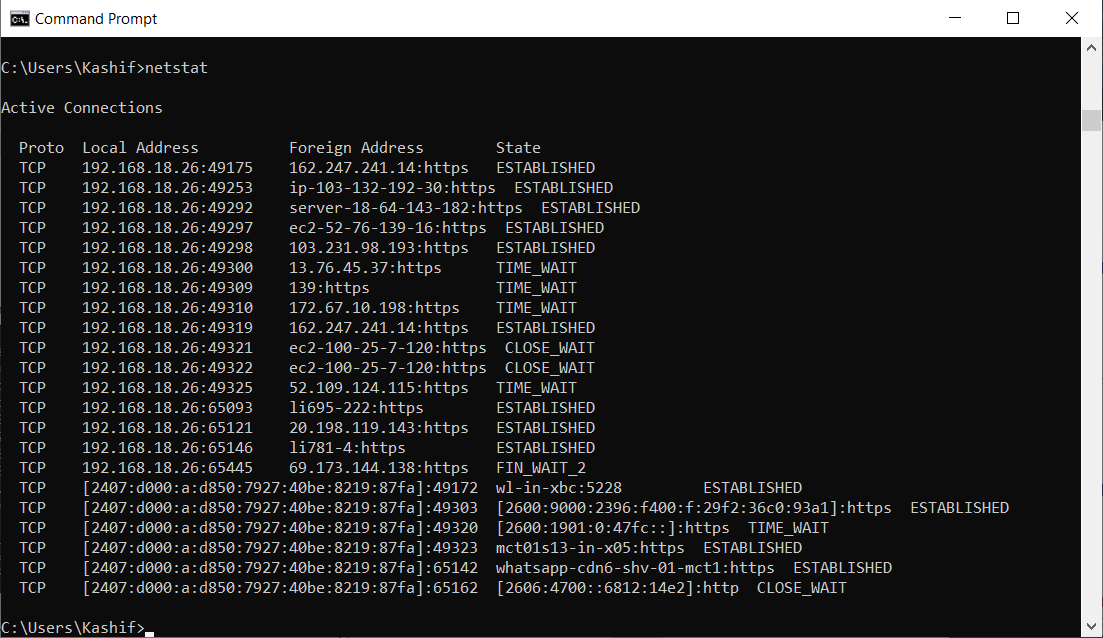
1. **System Info command:**

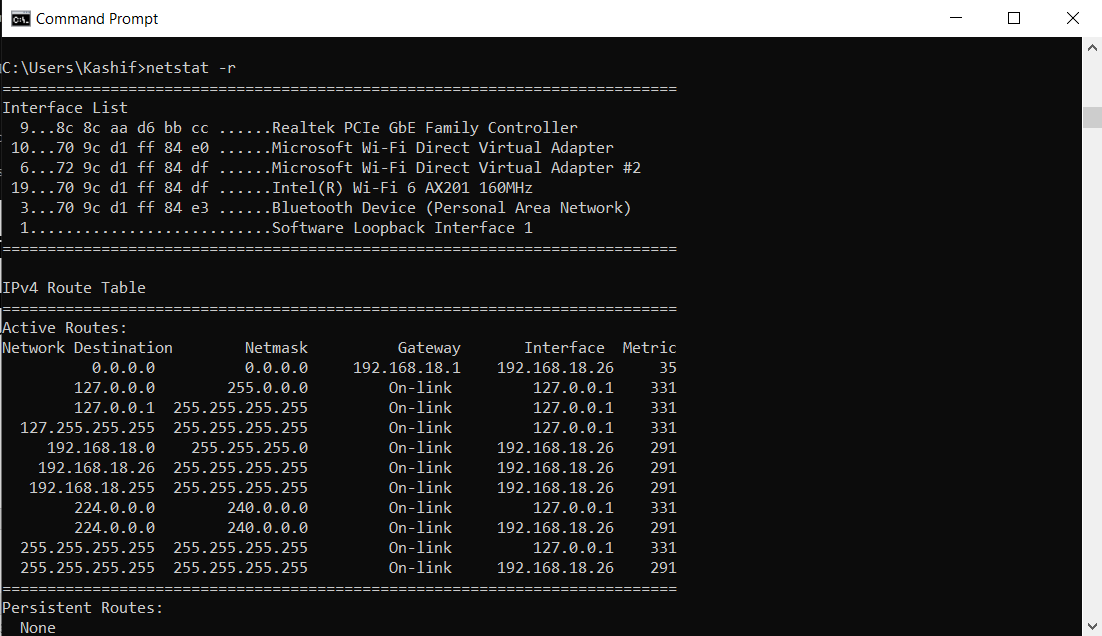
Displays detailed configuration information about a computer and its operating system, including operating system configuration, security information, product ID, and hardware properties (such as RAM, disk space, and network cards).



1. **Netstat Command**

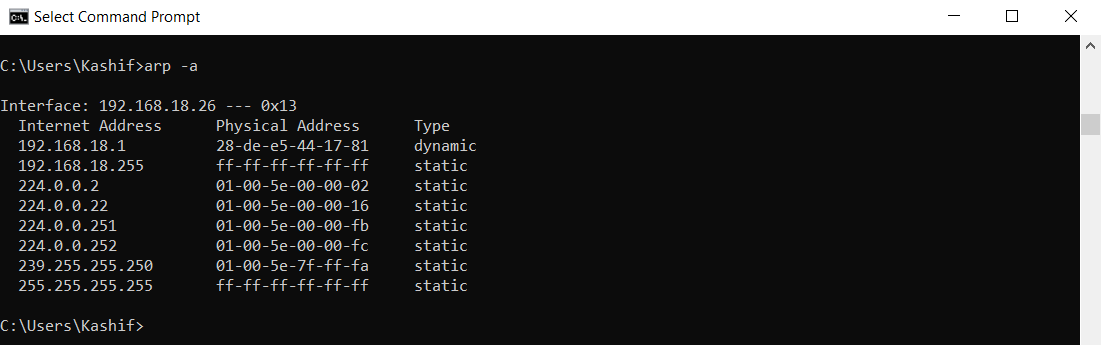
The Netstat command as the name suggests displays an overview of all the network connections in the device. The table shows detail about the connection protocol, address, and the current state of the network.





1. **ARP (Address Resolution Protocol) command:**

The ARP command is used to access the mapping structure of IP addresses to the MAC address. This provides us with a better understanding of the transmission of packets in the network channel.



1. NSLOOKUP Command

The NSLOOKUP command is used to troubleshoot network connectivity issues in the system. Using the nslookup command, we can access the information related to our system’s DNS server, i.e., domain name and IP address.

**LINUX COMMANDS**

To use Linux Terminal online use following link: <https://www.tutorialspoint.com/linux_terminal_online.php>

OR

<https://bellard.org/jslinux/vm.html?cpu=riscv64&url=fedora33-riscv.cfg&mem=256>

**Activity-2(Students will do their self):**

**Find the equivalent of all above commands in linux and execute. Also paste the screen shots of the outputs.**

 **LAB # 03**

**Lab Title:**

LAN Cable Construction (Cat-6, Cross vs Straight Cable)

**Lab Objective:**

Aim: Study of different types of Network cables and practically implement the cross-wired cable and straight through cable using clamping tool.

**Activity Outcomes:**

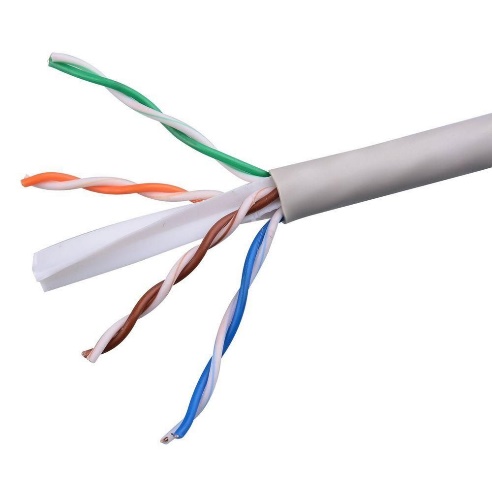
Students will learn about different type of cables and LAN cable construction

**Introduction:**

**Category 6 cable:**

Category 6 cable is a standardized twisted pair cable for Ethernet and other network physical layers that is backward compatible with the Category 5/5e and Category 3 cable standards. Cat 6 must meet more stringent specifications for crosstalk and system noise than Cat 5 and Cat 5e. Category 6 cables support Gigabit Ethernet data rates of 1 gigabit per second. These cables can accommodate 10 Gigabit Ethernet connections over a limited distance—commonly about 180 feet for a single cable. Cat 6 cable contains four pairs of copper wire and uses all the pairs for signaling to obtain its high level of performance. It is compatible with fast Ethernet 10BASE-T, 100BASE-TX and Gigabit networks, and is backward compatible with previous iterations, such as Cat5/5E and Cat3.

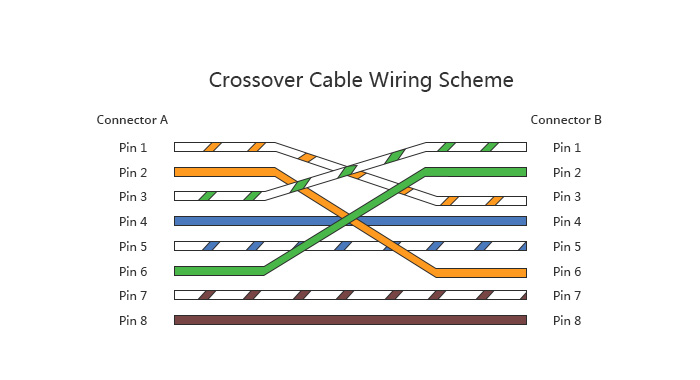
In most cases, Cat6 cable is used for connecting a computer to another device like a hub, router or switch in order to allow the sharing of files across a network or for accessing the Internet. It can also be used for connecting computers to other devices together such as printers or scanners, or for incoming and outgoing LAN connections on patch panels.



**Crossover Cable:**

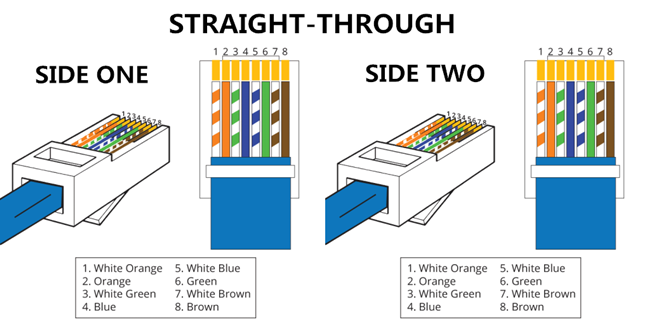
An Ethernet crossover cable is a network cable used to connect two Ethernet network devices directly, such as two computers without a switch or router in between. They are used to send and receive data by enabling complex data transfers between computers, routers, and networks. Ethernet crossover cables are similar to straight-through cable except that they have pairs of wires that crisscross. Their internal wiring reverses the incoming and outgoing signals. It uses a design that allows the data output pins on one end of the cable to be connected directly to the data input pins on the other end of the cable.

Crossover cables look much like a regular **Ethernet cable**, but they are unique. Unlike an Ethernet cable, crossover cables have specific wiring designed with a reversed path for signal transmission. Opting for Ethernet wiring in temporary networking situations stops the system from working properly. Crossover cables work best for direct networking. If you are conjoining a network switch and a peripheral, you shouldn't use crossover cables. An Ethernet cable is the best for this scenario because of its versed wiring methods. A crossover cable uses an entirely different wiring process, where signals are obtained but sent reversely to both endpoints.



**Straight Through Cable**

A straight-through cable is an ethernet cable that connects the wires within it one to one on both sides. This means that wire one will connect to pin spot one in both connectors, wire two will connect to pin spot two in both connectors, and so on.



#### **Key Difference between Straight Through Cables and Crossover Cables**

* Crossover cable, Pin 1 is crossed with Pin 3, and Pin 2 is crossed with Pin 6, while in Straight-through cable Pin connection is one-to-one.
* Straight-through cables are mainly used for connecting non-similar devices, while crossover cables are mostly used for connecting similar devices.
* Straight-through cable connects a computer with a DSL modem, while Crossover cable connects Router to Router and Computer

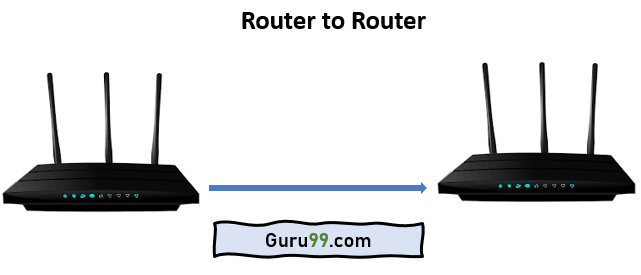
## When to use Straight Through Cable?

## https://www.guru99.com/images/2/101920_1030_StraightThr3.png

* It helps you to connect a computer to a switch/hub’s normal port.
* You can use it to connect a computer to a cable/DSL modem’s LAN port.
* It allows you to connect a router’s WAN port to a cable/DSL modem’s LAN port.
* Connect 2 switches or hubs with one of the hub or switch using an upline port and the other one using a normal port.

## When to use Crossover Cable?

## https://www.guru99.com/images/2/101920_1030_StraightThr4.png



* It can use a computer to a computer with no switch or hub.
* Network devise to the network device. For example, the route to the router.
* Crossover cable enables one to establish a direct connection between two computing devices using Ethernet ports.
* It Connects two computers directly.
* You can connect two hubs/switches by using the normal port in both switches and hubs.

**LAB # 04**

**Lab Title:**

Building a Physical LAN using switch & GUI Understanding

**Lab Objective:**

Configure a switch with a name and an IP Address.

Configure password to ensure that access to the CLI is secure.

Configure VLAN.

Save the active configuration.

View the switch browser interface.

**Activity Outcomes:**

Students will learn about different type of switch configuration and Installation.

**Introduction:**

A switch is used in a wired network to connect to other devices using Ethernet cables. The switch allows each connected device to talk to the others. Wireless-only networks do not use switches because devices such as wireless routers and adapters communicate directly with one another.

Although you can use the ports on the back of a router or modem to connect a few Ethernet devices together, switches offer a number of advantages:

* Switches allow you to connect dozens of devices.
* Switches keep traffic between two devices from getting in the way of your other devices on the same network.
* Switches allow you to control who has access to various parts of the network.
* Switches allow you to monitor usage.
* Switches allow communication (within your network) that's even faster than the Internet.
* High-end switches can be tailored to your network needs with pluggable modules.



## Configuration Requirements

## 

## Cables Connectivity

## 

## Switch model numbers

There are many switch models available in the market and few are mentioned below.

* First is the switch’s Ethernet capability:
  + FS: Fast Ethernet.
  + GS or JGS: Gigabit Ethernet.
  + GSS: Gigabit Ethernet ClickSwitch.
  + MS: Multigigabit Ethernet (5-speed).
  + XS: 10-Gigabit Ethernet.

#### Topology Diagram

#### Background / Preparation

In this activity, you will configure these settings on the customer Cisco Catalyst 2960 switch:

* + Host name
  + Console password
  + vty password
  + Privileged EXEC mode password
  + Privileged EXEC mode secret
  + IP address on VLAN1 interface
  + Default gateway

**Note:** Not all commands are graded by Packet Tracer.

##### Step 1: Configure the switch host name.

* 1. From the Customer PC, use a console cable and terminal emulation software to connect to the console of the customer Cisco Catalyst 2960 switch.
  2. Set the host name on the switch to **CustomerSwitch** using these commands.

Switch>**enable** Switch#**configure terminal**

Switch(config)#**hostname CustomerSwitch**

##### Step 2: Configure the privileged mode password and secret.

1. From global configuration mode, configure the password as **cisco**.

CustomerSwitch(config)#**enable password cisco**

1. From global configuration mode, configure the secret as **cisco123**.

CustomerSwitch(config)#**enable secret cisco123**

##### Step 3: Configure the console password.

1. From global configuration mode, switch to configuration mode to configure the console line.

CustomerSwitch(config)#**line console 0**

1. From line configuration mode, set the password to **cisco** and require the password to be entered at login.

CustomerSwitch(config-line)#**password cisco** CustomerSwitch(config-line)#**login** CustomerSwitch(config-line)#**exit**

##### Step 4: Configure the vty password.

1. From global configuration mode, switch to the configuration mode for the vty lines 0 through 15.

CustomerSwitch(config)#**line vty 0 15**

1. From line configuration mode, set the password to **cisco** and require the password to be entered at login.

CustomerSwitch(config-line)#**password cisco** CustomerSwitch(config-line)#**login** CustomerSwitch(config-line)#**exit**

##### Step 5: Configure an IP address on interface VLAN1.

From global configuration mode, switch to interface configuration mode for VLAN1, and assign the IP address 192.168.1.5 with the subnet mask of 255.255.255.0.

CustomerSwitch(config)#**interface vlan 1**

CustomerSwitch(config-if)#**ip address 192.168.1.5 255.255.255.0**

CustomerSwitch(config-if)#**no shutdown**

CustomerSwitch(config-if)#**exit**

##### Step 6: Configure the default gateway.

1. From global configuration mode, assign the default gateway to 192.168.1.1.

CustomerSwitch(config)#**ip default-gateway 192.168.1.1**

1. Click the **Check Results** button at the bottom of this instruction window to check your work.

##### Step 7: Verify the configuration.

The Customer Switch should now be able to ping the ISP Server at 209.165.201.10. The first one or two pings may fail while ARP converges.

CustomerSwitch(config)#**end** CustomerSwitch#**ping 209.165.201.10S**

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 209.165.201.10, timeout is 2 seconds:

Success rate is 60 percent (3/5), round-trip min/avg/max = 181/189/197 ms CustomerSwitch#

##### **Reflection**

1. What is the significance of assigning the IP address to the VLAN1 interface instead of any of the Fast Ethernet interfaces?
2. What command is necessary to enforce password authentication on the console and vty lines?
3. How many gigabit ports are available on the Cisco Catalyst 2960 switch that you used in the activity

 **LAB # 05 & 6**

**Lab Title:**

Introduction & Installation of Wireshark Network Monitor & Analysing Frame Header on Wireshark (Layer-2)

**Lab Objective:**

The basic purpose of this lab is to introduce you to Wireshark, a popular protocol analyzer. By the end of this lab you will be familiar to its environment and will know how to capture and interactively browse the traffic running on a computer network using it.

**Activity Outcomes:**

The student will understand the packet capturing method and packet encapsulation of headers at different layer’s.

**Introduction:**

A protocol analyzer is a tool that can be used to inspect what exactly is happening on a network with respect to traffic flow. For example, if your TCP/IP sessions are "hanging", a protocol analyzer can show which system sent the last packet, and which system failed to respond. If you are experiencing slow screen updates, a protocol analyzer can display delta time stamps and show which system is waiting for packets, and which system is slow to respond.

A protocol analyzer can show runaway traffic (broadcast or multicast storms) and its origin, system errors and retries, and whether a station is sending, trying to send, or only seeming to communicate. You will get information that is otherwise unavailable, which results in more efficient troubleshooting and better LAN health.=

1. **Introduction to Wireshark**

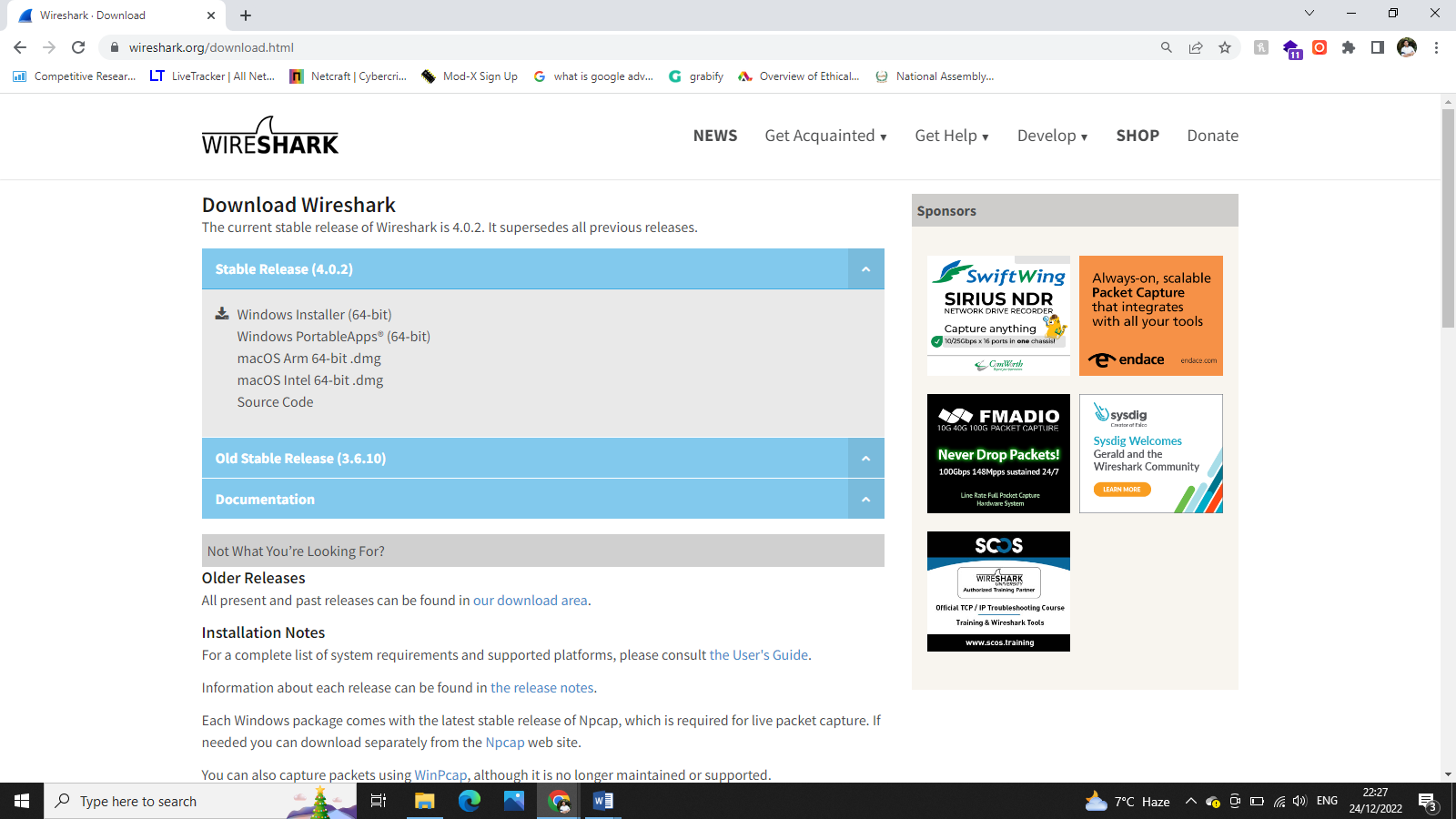
Wireshark is a free and open-source packet analyzer, used for network troubleshooting, analysis, software and communications protocol development, and education.

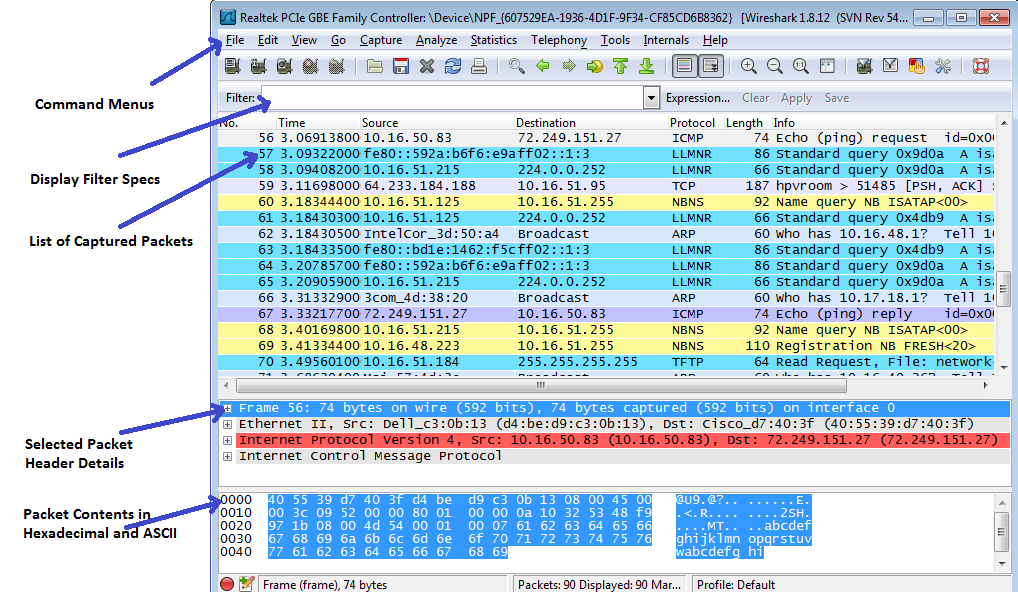
The basic tool for observing the messages exchanged between executing protocol entities is called a packet sniffer. As the name suggests, a packet sniffer captures (“sniffs”) messages being sent/received from/by your computer; it will also typically store and/or display the contents of the various protocol fields in these captured messages. A packet sniffer itself is passive. It observes messages being sent and received by applications and protocols running on your computer, but never sends packets itself. Similarly, received packets are never explicitly addressed to the packet sniffer. Instead, a packet sniffer receives a copy of packets that are sent/ received from/by application and protocols executing on your machine.

**Getting Wireshark**

a) www.wireshark.org/download.html

**Note:** First download and Install with default options

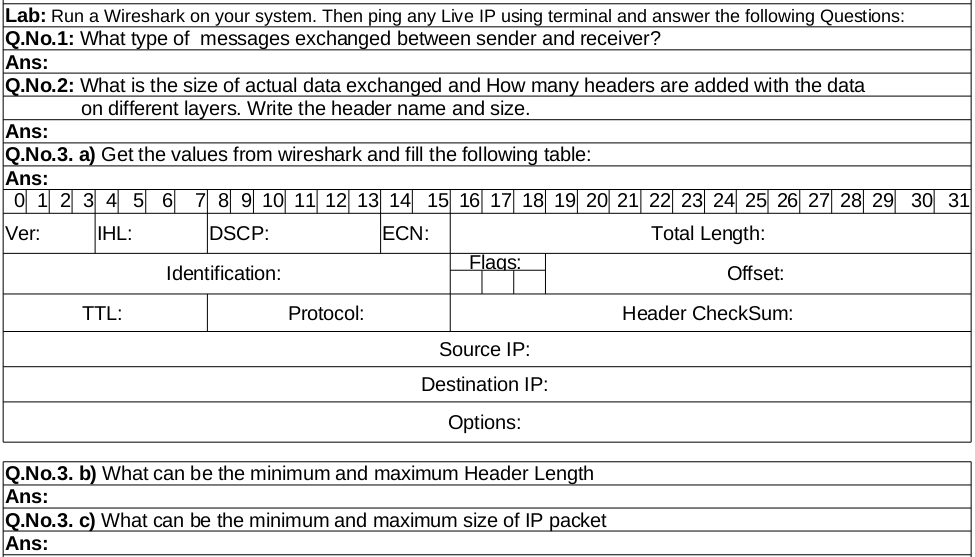




***Lab Assignment***

***1.Take a print of this page***

***2.Perform the following lab and answer the questions:***





**LAB # 07**

**Lab Title:**

Cisco Packet Tracer, Building LAN on Packet Tracer and message passing

**Lab Objective:**

The basic purpose of this lab is to introduce you to Packet Tracer, Get acquainted with Packet Tracer & Make some simple Packet Tracer scenarios

**Activity Outcomes:**

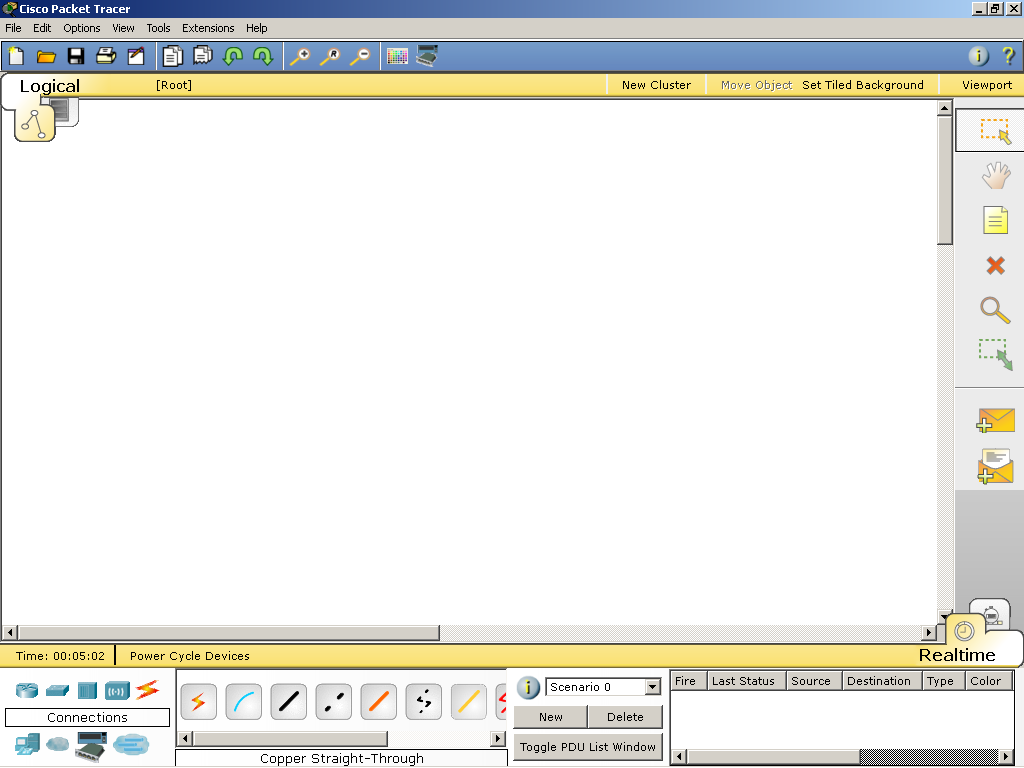
Students will have gained the basic understanding of Packet Tracer to see “protocols in action”. After this lab, students will have developed basic understanding of digging deep into the network protocols.

**Introduction:**

Packet Tracer is a protocol simulator developed by Dennis Frezzo and his team at Cisco Systems. Packet Tracer (PT) is a powerful and dynamic tool that displays the various protocols used in networking, in either Real Time or Simulation mode. The purpose of this lab is to become familiar with the Packet Tracer interface. Learn how to use existing topologies and build your own.

This activity will provide an opportunity to explore the standard lab setup using Packet Tracer simulator. Packet Tracer has two file formats it can create: .pkt files (network simulation model files) and .pka files (activity files for practice). When you create your own networks in Packet Tracer, or modify existing files from your instructor or your peers, you will often use the .pkt file format. When you launched this activity from the curriculum, these instructions appeared. They are the result of the .pka, Packet Tracer activity file format.

**Step 1:** Getting Packet Tracer



**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.

Single click on each group of devices and connections to display the various choices. The devices you see may differ slightly.

|  |  |
| --- | --- |
|  |  |
|  |  |
|  | |
|  |  |
|  |  |

1. Other than generic routers, name 3 router models available on the simulation software.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. What are the two types of serial cables available for WAN connectivity?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. What are the two types of copper cable connectors?

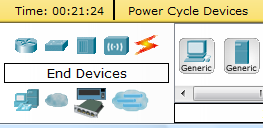
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Other than generic end devices, enumerate four end devices available.

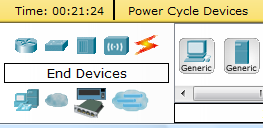
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Step 3**: Building the Topology – Adding Hosts

Single click on the End Devices.



Single click on the Generic host.



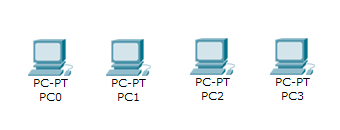
Move the cursor into topology area. You will notice it turns into a plus “+” sign.



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

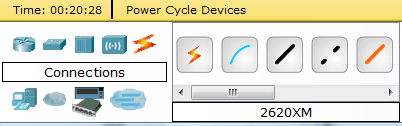
Select a hub, by clicking once on Hubs and once on a Generic hub.

|  |  |  |
| --- | --- | --- |
|  |  |  |

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.

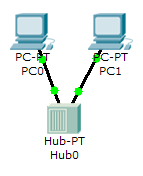


Perform the following steps to connect PC0 to Hub0:

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.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 |
|  |  |  |  |  |

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

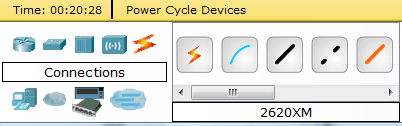
Select a switch, by clicking once on Switches and once on a 2950-24 switch.

|  |  |  |
| --- | --- | --- |
|  |  |  |

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.

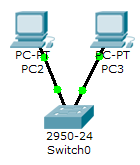


Perform the following steps to connect PC2 to Switch0:

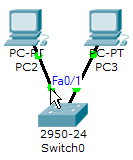
1. Click once on PC2
2. Choose FastEthernet
3. Drag the cursor to Switch0
4. Click once on Switch0 and choose FastEthernet0/1
5. Notice the green link lights on PC2 Ethernet NIC and amber light Switch0 FastEthernet0/1 port. The switch port is temporarily not forwarding frames, while it goes through the 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.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 |
|  |  |  |  |  |  |

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.)



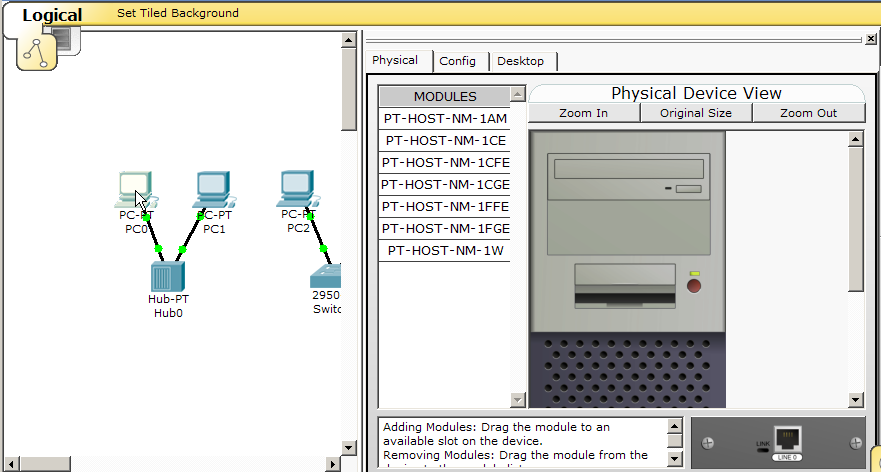
Move the cursor over the link light to view the port number. Fa means FastEthernet, 100 Mbps Ethernet.



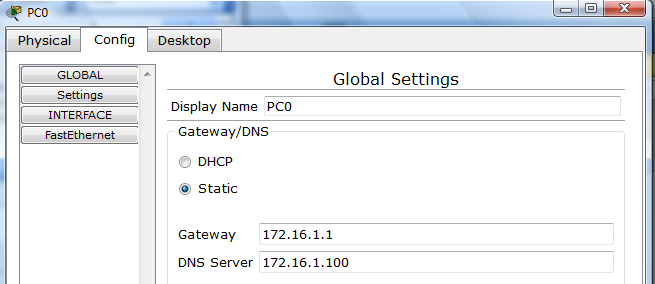
**Step 5:** Configuring IP Addresses and Subnet Masks on the Hosts

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

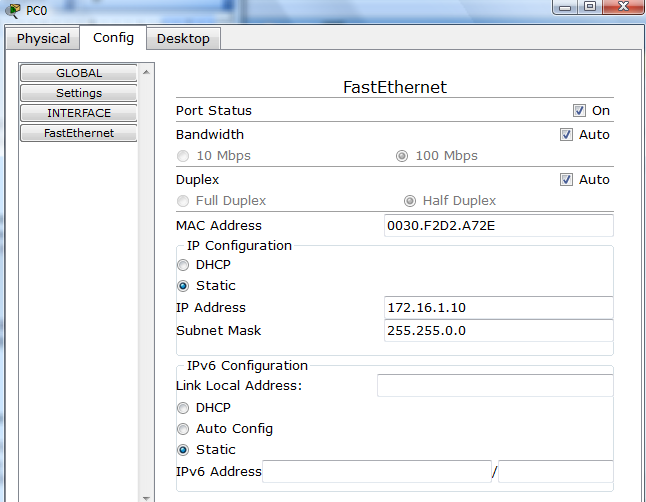
Click once on PC0.



Choose the Config tab and click on Settings. 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 and the DNS Server IP Address. We will discuss this later, but this would be the IP address of the local router. If you want, you can enter the Gateway IP Address 172.16.1.1 and DNS Server IP Address 172.16.1.100, although it will not be used in this lab.



Click on Interface and then 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.



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.

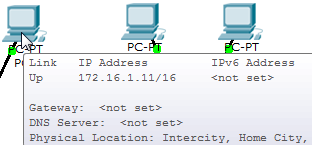


Repeat these steps for the other hosts. Use the information below for IP Addresses and Subnet Masks.

|  |  |  |
| --- | --- | --- |
| 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 |

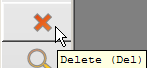
Verify the information

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



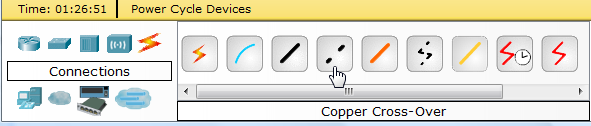
Deleting a Device or Link

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

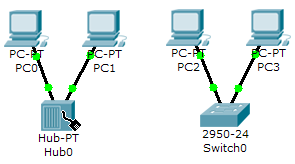


**Step 6**: Connecting Hub0 to Switch0

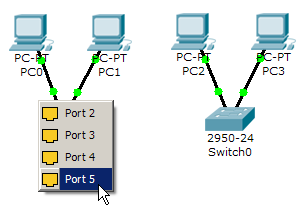
To connect like-devices, like a Hub and a Switch, we will use a Cross-over cable. Click once the Cross-over Cable from the Connections options.



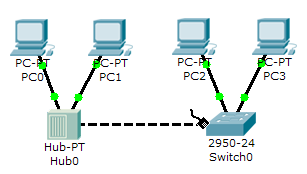
Move the Connections cursor over Hub0 and click once.



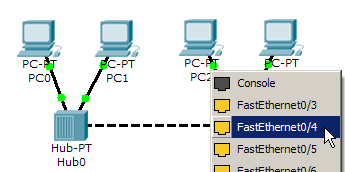
Select Port 5 (actual port does not matter).



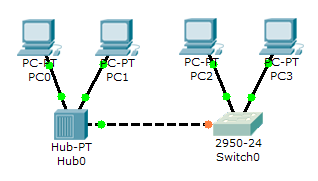
Move the Connections cursor to Switch0.

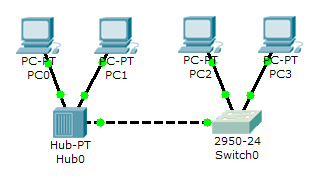


Click once on Switch0 and choose FastEthernet0/4 (actual port does not matter).



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.





**Step 7:** Verifying Connectivity in Realtime Mode

Be sure you are in Realtime mode.



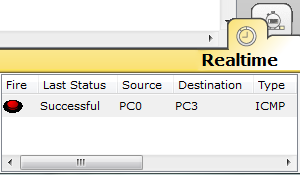
Select the Add Simple PDU tool used to ping devices.



Click once on PC0, then once on PC3.

|  |  |
| --- | --- |
|  |  |

The PDU Last Status should show as Successful.



Change the IP address of PC3 to 172.16.2.13. Perform a ping from PC0 to PC3. What is the ping result?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

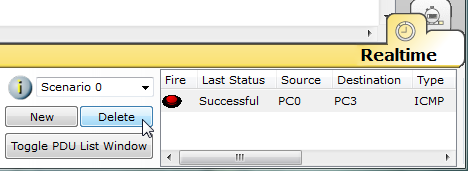
Return the IP address of PC3 to 172.16.1.13. Change the IP address of PC2 to 172.17.1.12. Perform a ping from PC0 to PC2. What is the ping result?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Resetting the Network

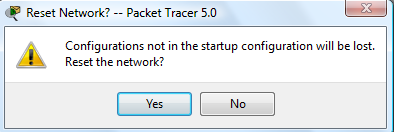
At this point we will want to reset the network, whenever you want to reset the network and begin the simulation again, perform the following tasks:

Click Delete in the PDU area.



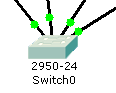
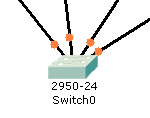
Now, Power Cycle Devices and confirm the action.





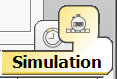
Waiting for Spanning Tree Protocol (STP)

Note: Because Packet Tracer also simulates the Spanning Tree Protocol, at times the switch may show amber lights on its interfaces. You will need to wait for the lights to turn green on the switches before they will forward any Ethernet frames.

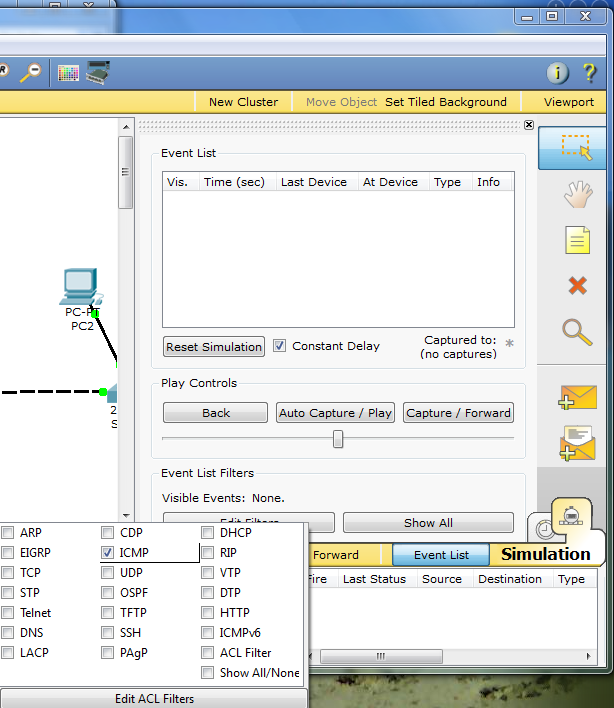


Step 8: Verifying Connectivity in Simulation Mode

Be sure you are in Simulation mode.



Deselect all filters (All/None) and select only ICMP.



**3**

**2**

**1**

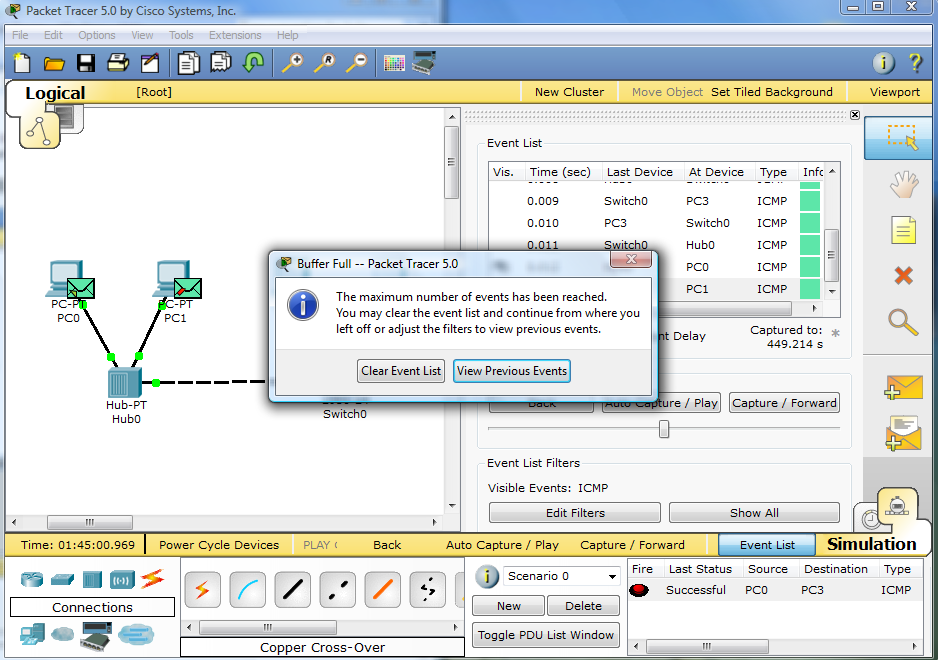
Select the Add Simple PDU tool used to ping devices..



Click once on PC0, then once on PC3.

|  |  |
| --- | --- |
|  |  |

Continue clicking Capture/Forward button until the ICMP ping is completed. You should see the ICMP messages move between the hosts, hub and switch. The PDU Last Status should show as Successful. Click on Clear Event List if you do not want to look at the events or click Preview Previous Events if you do. For this exercise it does not matter.



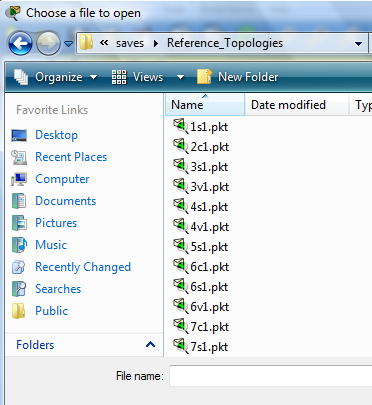
Step 9: Saving the Topology

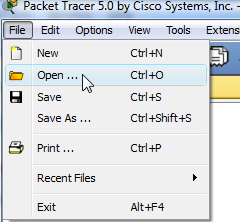
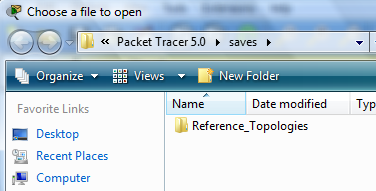
Perform the following steps to save the topology (uses .pkt file extension).

|  |  |
| --- | --- |
|  |  |

Opening Existing Topologies

|  |  |  |
| --- | --- | --- |
|  |  |  |

Opening Existing PT Topologies



 **LAB # 08**

**Lab Title:**

Configuration and Installation of Physical Switch and GUI Understanding

**Lab Objective:**

 Clear the configuration of a standalone switch to prepare it for a new lab.

**Activity Outcomes:**

Students will learn about Installation of Physical Switch

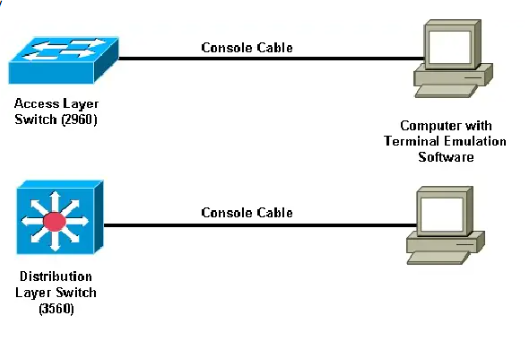
**Introduction:**

When working with a switch that has been previously configured, any new commands entered will be mergedwith the existing configuration, causing unpredictable results. In this lab you prepare a Catalyst 2960 or 3560switch for use with a lab. This is accomplished by erasing the startup configuration from NVRAM and deletingthe VLAN database.

**Note:**

 This lab uses the Cisco WS-C2960-24TT-L switch with the Cisco IOS image c2960-lanbasek9-mz.122-46.SE.bin and the Catalyst 3560-24PS switch with the Cisco IOS image c3560-advipservicesk9-mz.122-46.SE.bin. Other switches (such as a 2950 or a 3550), and Cisco IOS Software versions can be used if theyhave comparable capabilities and features. Depending on the switch model and Cisco IOS Software version,the commands available and output produced might vary from what is shown in this lab

**Basic Switch Configuration**

****

**SWITCH**

**Step 1:** Connect to the switch console port and enter privileged EXEC mode.

From a computer running a terminal emulation program, connect to the console port of the switch that youwant to clear using a console cable. You should see a console prompt that includes the switch’s hostname,followed by a

>  or #

. The default switch hostname is “Switch.”

Switch>

or

Switch#

If the prompt ends with a

>

, you are not in privileged EXEC mode. To enter privileged EXEC mode, type

enable

. This might require a password. If you are in a configuration mode, type

exit

 or

end

.If not enabled:

Switch>

**enable**

 Switch#

If in global configuration mode:

Switch(config)#

**exit**

 Switch#

**Step 2: Delete the VLAN database file.**

In privileged EXEC mode, type

delete flash:vlan.dat

 and press Enter. If you are asked to confirm, pressEnter until you are back to the original prompt.

Switch#

**delete flash:vlan.dat**

 Delete flash:vlan.dat? [confirm]Switch#

**Step 3: Erase the startup config from NVRAM.**

 After deleting the vlan.dat file, you can erase the startup configuration on the switch by typing

erase startup-config

. You again have to press Enter to confirm.

Switch#

**erase startup-config**

 Erasing the nvramfilesystemwill remove all configuration files! Continue?[confirm][OK]Erase of nvram: completeSwitch#

**Step 4:** Reload the device, but do not save the system configuration if prompted. After clearing the switch configuration, reload the switch by typing reload and pressing Enter. If you are askedwhether to save the current configuration, answer no

. Press Enter to confirm. The switch starts reloading.Your output might look different depending on the switch model that you are using. This step might take a fewminutes, because the switch needs time to reload.

Switch# reload

Systemconfiguration has been modified. Save? [yes/no]: no

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

Would you like to terminate autoinstall? [yes]: Enter

**Switch Configuration Commands**

Switch **>** (User mode)

Switch **>** enable

Switch **# (**Privileged EXEC mode)

Switch **# Configure Terminal**

Switch **(config)#** (Global Mode)

**Configure IP addresses for** Switch **Interfaces**

Switch (config)# interface GigabitEthernet 0/0

Switch(config-if)# ip address 100.100.100.1 255.255.255.252

Switch (config-if)# no shutdown

Switch (config-if)# exit

Switch (config)# interface GigabitEthernet 0/1

Switch (config-if)# ip address 192.168.10.1 255.255.255.0

Switch (config-if)# no shutdown

Switch (config-if)# exit

 **LAB # 09**

**Lab Title:**

Configuration and Installation of Physical Router and GUI Understanding

**Lab Objective:**

1. Understanding basic networking commands

2. Configuring the Router configuration commands

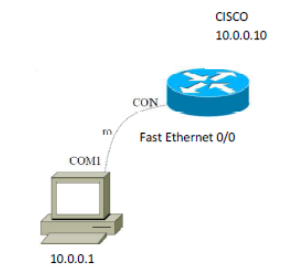
**Activity Outcomes:**

Students will learn about Installation of Physical Router

**Introduction:**

Cisco uses IOS which stands for Internetwork operating system. IOS is command line interface for configuring switch and router. Following are steps for connecting to router.

**Problem 1: Procedure to configure a Router with the PC**

****

1. Get a Console Cable

2. Plug the serial end into the back of the computer

3. Put the RJ-45 into the console port of Router.

4. Get a terminal program

- Hyperterminal

- Tera term

- Minicom

- Securecrt

5. Set it to connect via com port with

Baud rate=9600

Data bits=8

Parity=None

Stop bits=1

Flow Control:None

**Configure IP Address on Fast Ethernet 0/1:..**

Router(config)# hostname CISCO

CISCO(config)# int fastEthernet 0/1

CISCO(config-if)# ip address 10.0.0.10 255.0.0.0

CISCO(config-if)# no shutdown