**Data Communication and Networking**

Submitted by : **Fasih Ullah Khan Niazi**

Seat No : 1851015

Subject : Data Communication and Networking

Course No : CS-616

Submitted To: **Jahangir**

***1st Lab***

***(Theoretical Part)***

**Networking**

Networking refers to the total process of creating and using computer networks, with respect to hardware, protocols and software, including wired and wireless technology. It involves the application of theories from different technological fields, like IT, computer science and computer/electrical engineering.

# **Data Communication & Computer Network**

Data communications refers to the transmission of this digital data between two or more computers and a computer network or data network is a telecommunications network that allows computers to exchange data. The physical connection between networked computing devices is established using either cable media or wireless media. The best-known computer network is the Internet.

This tutorial should teach you basics of Data Communication and Computer Network (DCN) and will also take you through various advance concepts related to Data Communication and Computer Network

# **Network Devices (Hub, Repeater, Bridge, Switch, Router, Gateways and Brouter)**

**1. Repeater** – A repeater operates at the physical layer. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted so as to extend the length to which the signal can be transmitted over the same network. An important point to be noted about repeaters is that they do not amplify the signal. When the signal becomes weak, they copy the signal bit by bit and regenerate it at the original strength. It is a 2 port device.

**2. Hub** –  A hub is basically a multiport repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations. Hubs cannot filter data, so data packets are sent to all connected devices.  In other words, [collision domain](https://en.wikipedia.org/wiki/Collision_domain) of all hosts connected through Hub remains one.  Also, they do not have intelligence to find out best path for data packets which leads to inefficiencies and wastage.

**Types of Hub**

* **Active Hub :-**These are the hubs which have their own power supply and can clean , boost and relay the signal along the network. It serves both as a repeater as well as wiring center. These are used to extend maximum distance between nodes.
* **Passive Hub :-**These are the hubs which collect wiring from nodes and power supply from active hub. These hubs relay signals onto the network without cleaning and boosting them and can’t be used to extend distance between nodes.

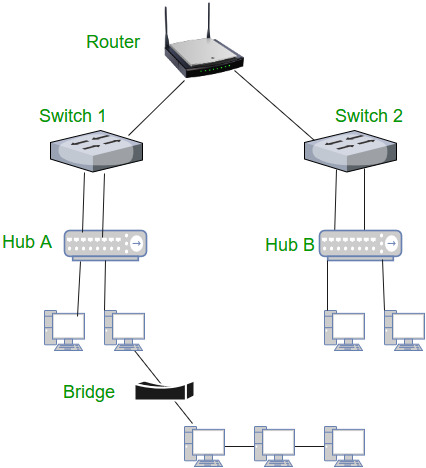
**3. Bridge** – A bridge operates at data link layer. A bridge is a repeater, with add on functionality of filtering content by reading the MAC addresses of source and destination. It is also used for interconnecting two LANs working on the same protocol. It has a single input and single output port, thus making it a 2 port device.

**Types of Bridges**

* **Transparent Bridges :-**These are the bridge in which the stations are completely unaware of the  
  bridge’s existence i.e. whether or not a bridge is added or deleted from the network , reconfiguration of  
  the stations is unnecessary. These bridges makes use of two processes i.e. bridge forwarding and bridge learning.
* **Source Routing Bridges :-**In these bridges, routing operation is performed by source station and the frame specifies which route to follow. The hot can discover frame by sending a specical frame called discovery frame, which spreads through the entire network using all possible paths to destination.

**4. Switch** – A switch is a multi port bridge with a buffer and a design that can boost its efficiency(large number of  ports imply less traffic) and performance. Switch is data link layer device. Switch can perform error checking before forwarding data, that makes it very efficient as it does not forward packets that have errors and  forward good packets selectively to correct port only.  In other words, switch divides collision domain of hosts, but [broadcast domain](https://en.wikipedia.org/wiki/Broadcast_domain) remains same.

**5. Routers** – A router is a device like a switch that routes data packets based on their IP addresses. Router is mainly a Network Layer device. Routers normally connect LANs and WANs together and have a dynamically updating routing table based on which they make decisions on routing the data packets. Router divide broadcast domains of hosts connected through it.



**6. Gateway** – A gateway, as the name suggests, is a passage to connect two networks together that may work upon different networking models. They basically works as the messenger agents that take data from one system, interpret it, and transfer it to another system. Gateways are also called protocol converters and can operate at any network layer. Gateways are generally more complex than switch or router.

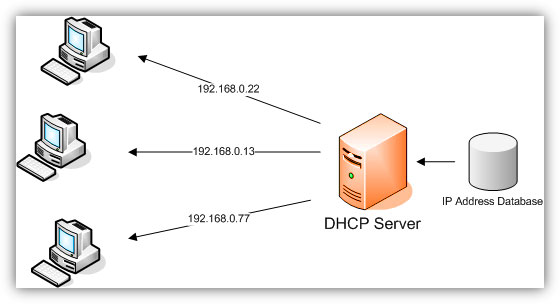
**7. Brouter** – It is also known as bridging router is a device which combines features of both bridge and router. It can work either at data link layer or at network layer. Working as router, it is capable of routing packets across networks and working as bridge, it is capable of filtering local area network traffic.

# **8. Firewall - (computing)**

In [computing](https://en.wikipedia.org/wiki/Computing), a **firewall** is a [network security](https://en.wikipedia.org/wiki/Network_security) system that [monitors](https://en.wikipedia.org/wiki/Network_monitoring) and controls incoming and outgoing [network traffic](https://en.wikipedia.org/wiki/Network_traffic) based on predetermined security rules.[[1]](https://en.wikipedia.org/wiki/Firewall_(computing)#cite_note-1) A firewall typically establishes a barrier between a trusted internal network and untrusted external network, such as the [Internet](https://en.wikipedia.org/wiki/Internet).[[2]](https://en.wikipedia.org/wiki/Firewall_(computing)#cite_note-Oppliger_1997_94-2)

Firewalls are often categorized as either **network firewalls** or **host-based firewalls**. Network firewalls filter traffic between two or more networks and run on network hardware. Host-based firewalls run on host computers and control network traffic in and out of those machines.

# **9. Dynamic Host Configuration Protocol**

The **Dynamic Host Configuration Protocol** (**DHCP**) is a [network management protocol](https://en.wikipedia.org/wiki/Network_protocol) used on [UDP/IP](https://en.wikipedia.org/wiki/UDP/IP) networks whereby a DHCP server dynamically assigns an [IP address](https://en.wikipedia.org/wiki/IP_address) and other network configuration parameters to each device on a network so they can communicate with other IP networks.[[1]](https://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol#cite_note-TechTarget-1) A DHCP server enables computers to request IP addresses and networking parameters automatically from the [Internet service provider](https://en.wikipedia.org/wiki/Internet_service_provider) (ISP), reducing the need for a [network administrator](https://en.wikipedia.org/wiki/Network_administrator) or a user to manually assign IP addresses to all network devices.[[1]](https://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol#cite_note-TechTarget-1) In the absence of a DHCP server, a computer or other device on the network needs to be manually assigned an IP address, or to assign itself an [APIPA](https://en.wikipedia.org/wiki/APIPA) address, which will not enable it to communicate outside its local subnet.

# **10. Domain Name Servers (DNS)**

Domain Name Servers (**DNS**) are the Internet's equivalent of a phone book. They maintain a directory of domain names and translate them to Internet Protocol (IP) addresses. This is necessary because, although domain names are easy for people to remember, computers or machines, access websites based on IP addresses

# **11. Subnetwork**

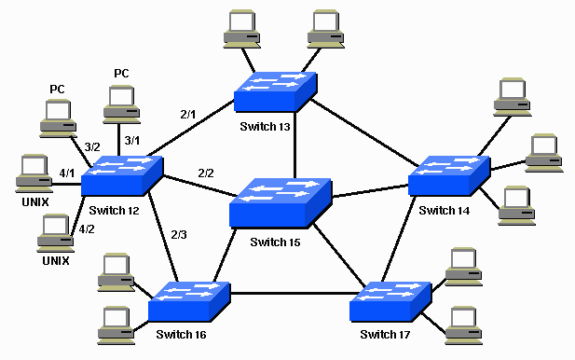
A **subnetwork** or **subnet** is a logical subdivision of an [IP network](https://en.wikipedia.org/wiki/IP_network).[[1]](https://en.wikipedia.org/wiki/Subnetwork#cite_note-rfc950-1):1,16 The practice of dividing a network into two or more networks is called **subnetting**.

Computers that belong to a subnet are addressed with an identical [most-significant bit](https://en.wikipedia.org/wiki/Most-significant_bit)-group in their [IP addresses](https://en.wikipedia.org/wiki/IP_address). This results in the logical division of an IP address into two fields, the *network number* or *routing prefix* and the *rest field* or *host identifier*. The *rest field* is an identifier for a specific [host](https://en.wikipedia.org/wiki/Host_(network)) or network interface.

The *routing prefix* may be expressed in [Classless Inter-Domain Routing](https://en.wikipedia.org/wiki/Classless_Inter-Domain_Routing) (CIDR) notation written as the first address of a network, followed by a slash character (*/*), and ending with the bit-length of the prefix. For example, *198.51.100.0/24* is the prefix of the [Internet Protocol version 4](https://en.wikipedia.org/wiki/Internet_Protocol_version_4) network starting at the given address, having 24 bits allocated for the network prefix, and the remaining 8 bits reserved for host addressing. Addresses in the range *198.51.100.0* to *198.51.100.255* belong to this subnet. The [IPv6](https://en.wikipedia.org/wiki/IPv6) address specification *2001:db8::/32* is a large address block with 296 addresses, having a 32-bit routing prefix

# **12. Spanning Tree Protocol**

The **Spanning Tree Protocol**(**STP**) is a [network protocol](https://en.wikipedia.org/wiki/Network_protocol) that builds a loop-free [logical topology](https://en.wikipedia.org/wiki/Logical_topology) for [Ethernet networks](https://en.wikipedia.org/wiki/Ethernet_network). The basic function of STP is to prevent [bridge loops](https://en.wikipedia.org/wiki/Bridge_loop) and the [broadcast radiation](https://en.wikipedia.org/wiki/Broadcast_radiation) that results from them. Spanning tree also allows a [network design](https://en.wikipedia.org/wiki/Network_planning_and_design) to include backup links to provide [fault tolerance](https://en.wikipedia.org/wiki/Fault_tolerance) if an active link fails.



***2nd Lab***

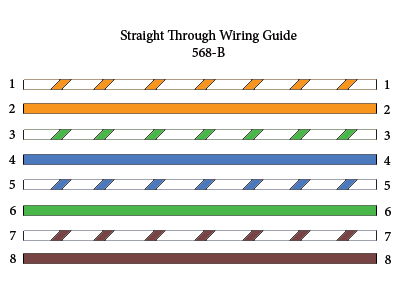
***(Theoretical Part)***

# **Straight-through, Crossover, and Rollover Wiring**

Straight-Through Wired Cables

Straight-Through refers to cables that have the pin assignments on each end of the cable. In other words Pin 1 connector A goes to Pin 1 on connector B, Pin 2 to Pin 2 ect. Straight-Through wired cables are most commonly used to connect a host to client. When we talk about cat5e patch cables, the Straight-Through wired cat5e patch cable is used to connect computers, printers and other network client devices to the router switch or hub (the host device in this instance).

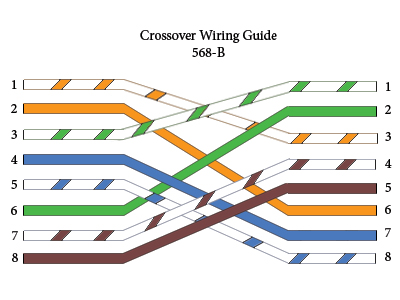
* **Connector A**
* Pin 1
* Pin 2
* Pin 3
* Pin 4
* Pin 5
* Pin 6
* Pin 7
* Pin 8
* **Connector B**
* Pin 1
* Pin 2
* Pin 3
* Pin 4
* Pin 5
* Pin 6
* Pin 7
* Pin 8



Crossover Wired Cables

Crossover wired cables (commonly called crossover cables) are very much like Straight-Through cables with the exception that TX and RX lines are crossed (they are at oposite positions on either end of the cable. Using the 568-B standard as an example below you will see that Pin 1 on connector A goes to Pin 3 on connector B. Pin 2 on connector A goes to Pin 6 on connector B ect. Crossover cables are most commonly used to connect two hosts directly. Examples would be connecting a computer directly to another computer, connecting a switch directly to another switch, or connecting a router to a router.*Note: While in the past when connecting two host devices directly a crossover cable was required. Now days most devices have auto sensing technology that detects the cable and device and crosses pairs when needed.*

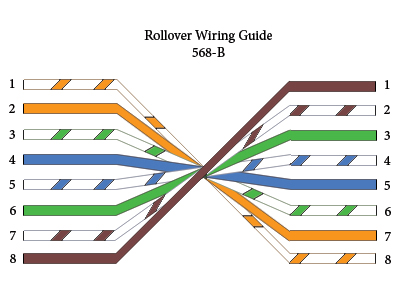
* **Connector A**
* Pin 1
* Pin 2
* Pin 3
* Pin 4
* Pin 5
* Pin 6
* Pin 7
* Pin 8
* **Connector B**
* Pin 1
* Pin 2
* Pin 3
* Pin 4
* Pin 5
* Pin 6
* Pin 7
* Pin 8



Rollover Wired Cables

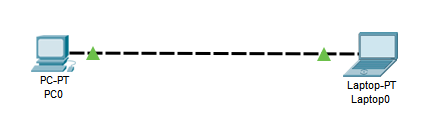
Rollover wired cables most commonly called rollover cables, have opposite Pin assignments on each end of the cable or in other words it is "rolled over". Pin 1 of connector A would be connected to Pin 8 of connector B. Pin 2 of connector A would be connected to Pin 7 of connector B and so on. Rollover cables, sometimes referred to as Yost cables are most commonly used to connect to a devices console port to make programming changes to the device. Unlike crossover and straight-wired cables, rollover cables are not intended to carry data but instead create an interface with the device.

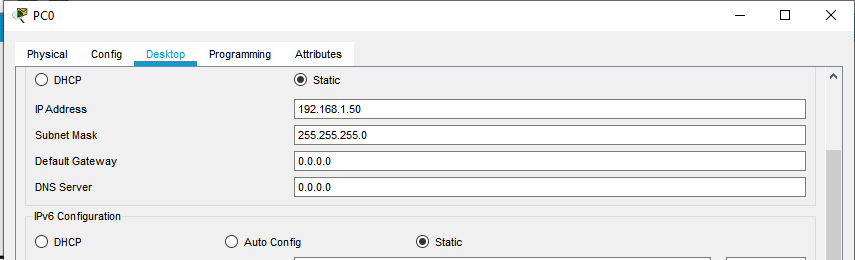
* **Connector A**
* Pin 1
* Pin 2
* Pin 3
* Pin 4
* Pin 5
* Pin 6
* Pin 7
* Pin 8
* **Connector B**
* Pin 1
* Pin 2
* Pin 3
* Pin 4
* Pin 5
* Pin 6
* Pin 7
* Pin 8

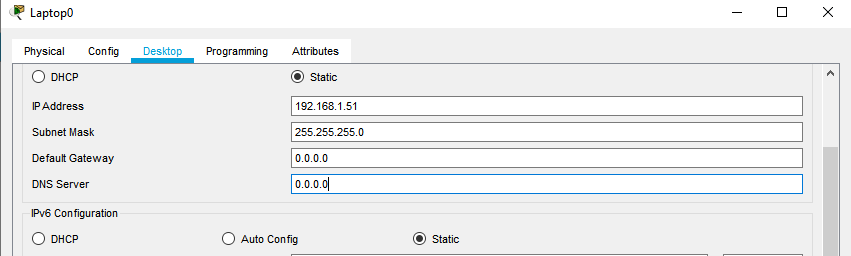


***3rd Lab***

* Connectivity of 2 PC’s peer to peer by Using Cross Cable ?





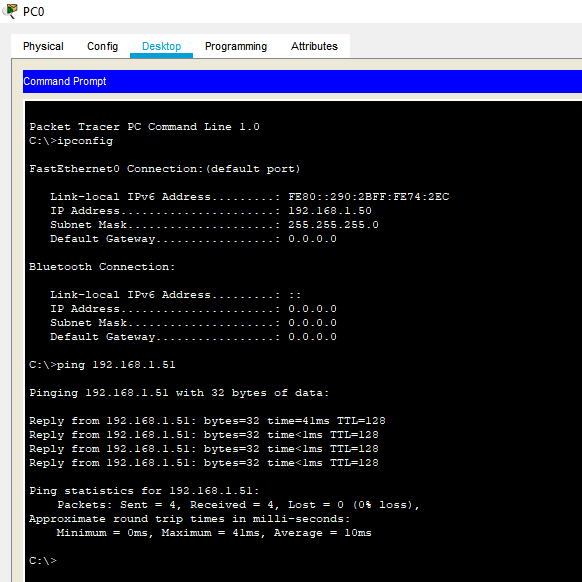
* We have to select static Ip for Pc with Subnet Mask.
* Remember there is not required gateway because we just check the connectivity of two pcs. Gateway means (It’s a way of internet) Through router or any Network Device according to situations.
* This IP assign to laptop

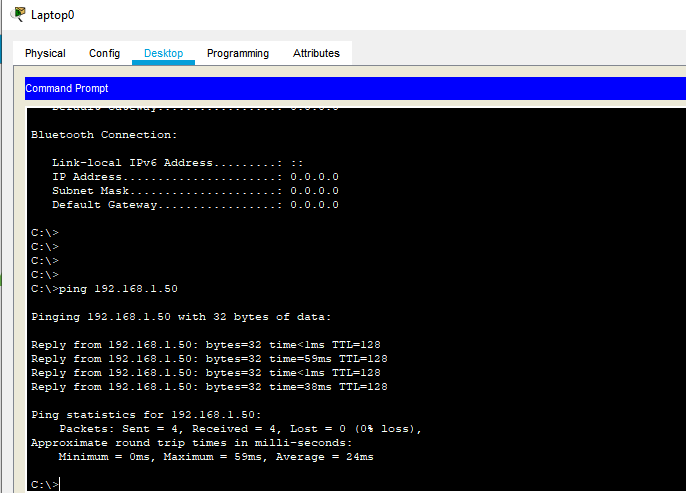
Now we check these two pc’s are connected to each other ? or ping able ?

Here,

we Use P2P Services and Guntella Protocol.

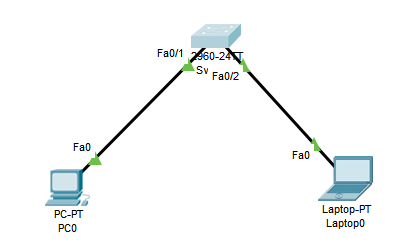
Guntella protocol Defines 5 Different Packets here we use only 1.

**Ping** This is for Device Discovery.

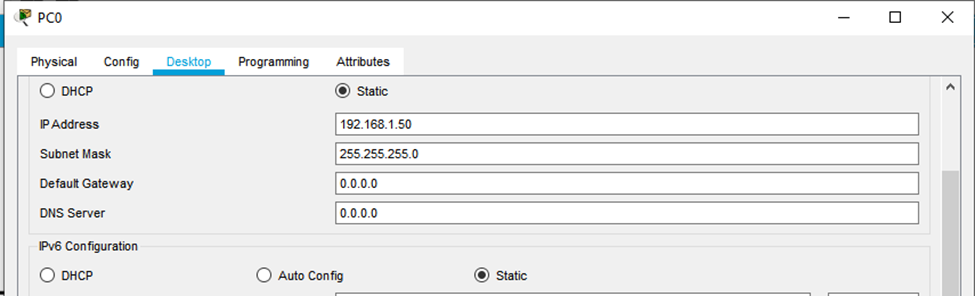
* First we check what is your pc IP and then ping your connect laptop to check the connectivity here is show the packets are sending on the 192.168.1.51 Address so its mean Connectivity is Good.
* Laptop pings also be Fine.

***4th Lab***

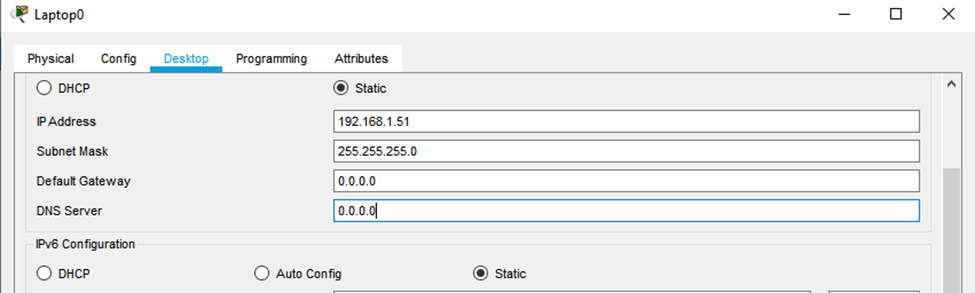
Connectivity of 2 Pcs through Switch.



Here,

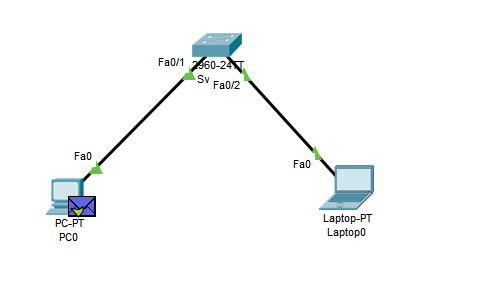
 Is also doing same work Firstly we assign the IPs of both Pcs

This is For Pc



This is for Laptop.

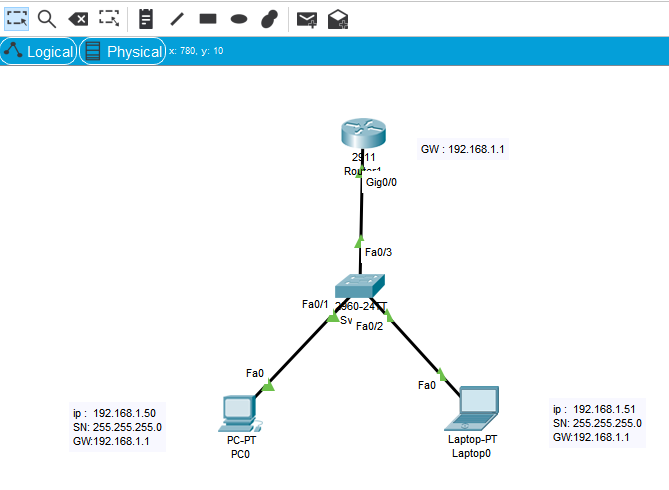
Now i sent the packet of 1 pc to another pc then we have to get the Result as shown below.

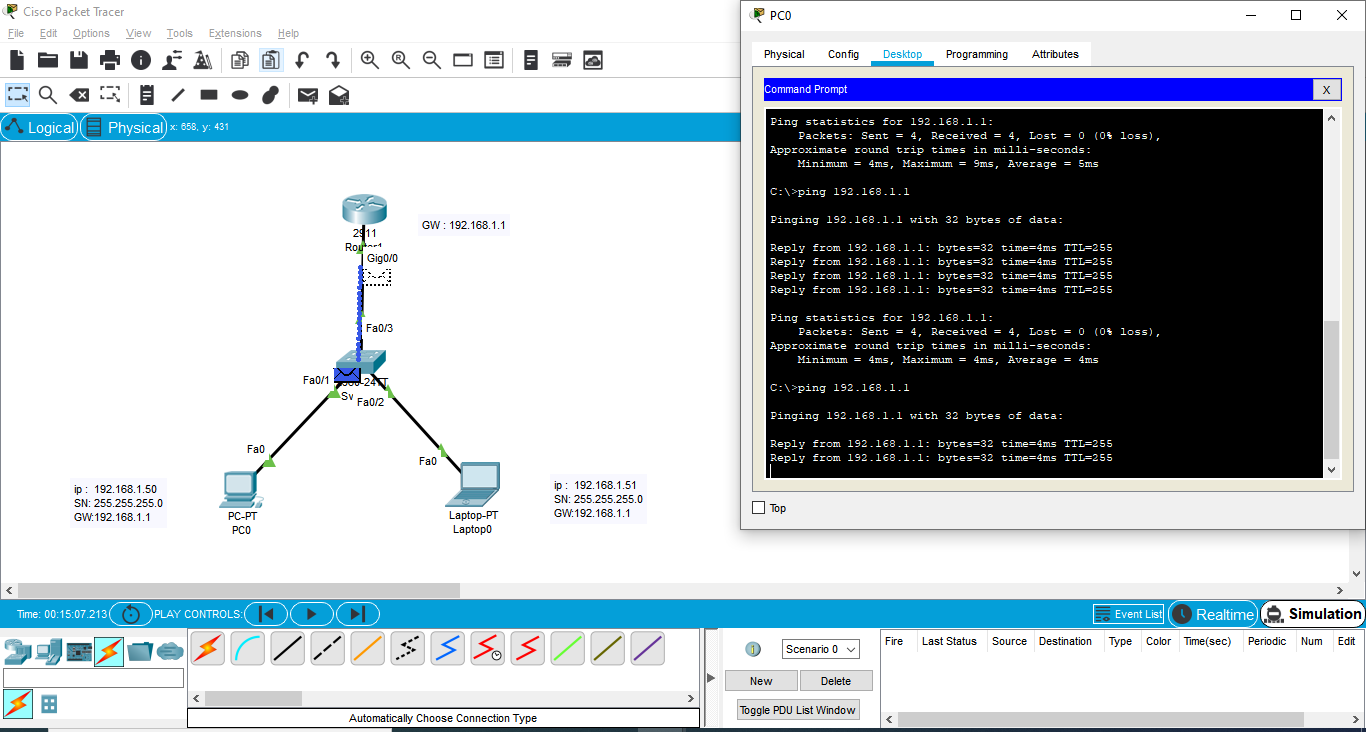


The Purple Packet means the packet are transfer from laptop and then gives the conformation check for user.

***5th Lab***

Connectivity of 2 pcs through 1 switch and 1 router.





As we know that the both Pcs Configuration are same like a previous labs.

Now we have to New Configuration for **Router** as below.

**Router:**

Router> //User Mode Used

Router# //Privileged Mode

Router(config)#interface gigabitEthernet 0/0 //Configuration Mode

Router(config-if)#ip address 192.168.1.1 255.255.255.0

Router(config-if)#no shut?

shutdown

Router(config-if)#no shutdown

Router(config-if)#do wr

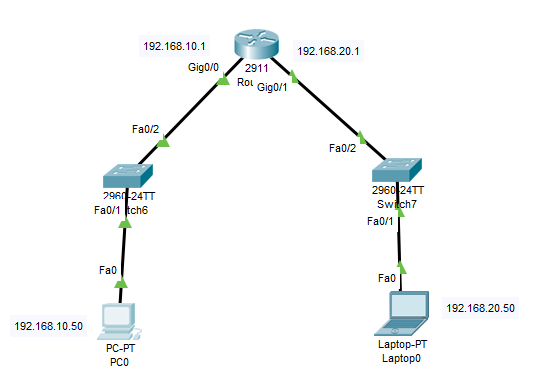
Building configuration...

[OK]

Router(config-if)#exit

***6th Lab***

Connectivity of 2 pcs through 2 switch and 1 router.



This is the Configured diagram.

Configuration Commands:

Router>en

Router#conf

Router#configure

Configuring from terminal, memory, or network [terminal]?

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#interface ?

//Dialer Dialer interface

//Dot11Radio Dot11 interface

//Ethernet IEEE 802.3

//FastEthernet FastEthernet IEEE 802.3

//GigabitEthernet GigabitEthernet IEEE 802.3z

//Loopback Loopback interface

//Port-channel Ethernet Channel of interfaces

//Serial Serial

//Tunnel Tunnel interface

//Virtual-Template Virtual Template interface

//Vlan Catalyst Vlans

//range interface range command

Router(config)#interface GigabitEthernet0/0

Router(config-if)#ip address 192.168.10.1 255.255.255.0

Router(config-if)#

Router(config-if)#no shu

Router(config-if)#no shutdown

Router(config-if)#

Router(config-if)#do wr

Building configuration...

[OK]

Router(config-if)#

Router(config-if)#exit

Router(config)#

Router(config)#interface giga

Router(config)#interface gigabitEthernet 0/1

Router(config-if)#ip address 192.168.20.1 255.255.255.0

Router(config-if)#

Router(config-if)#no shutdown

Router(config-if)#do wr

Building configuration...

[OK]

Router(config-if)#

Router(config-if)#

Router(config-if)#exit

Router(config)#^Z

Router#

The End