EXP 01: To study the working of Basic Networking Commands.

Basic networking commands are essential for troubleshooting and managing network connections. They allow you to diagnose network issues, configure network settings, and gather information about network devices. Here are some commonly used networking commands:

1. ***Ping:*** Ping is used to test the reachability of a network device or a remote host. It sends an ICMP echo request to the target and waits for an ICMP echo reply. To use ping, open the command prompt or terminal and type `ping <IP address or hostname>`. For example, `ping 192.168.0.1` or `ping www.google.com`.
2. ***Traceroute:*** Traceroute (or tracert on Windows) is used to trace the route that packets take from your computer to a destination host. It shows the IP addresses of each hop along the path. To use traceroute, open the command prompt or terminal and type `tracert <IP address or hostname>`. For example, `tracert 192.168.0.1` or `tracert www.google.com`.
3. ***Ipconfig/ifconfig***: Ipconfig (Windows) or ifconfig (Linux/Unix) displays the IP configuration information for all network interfaces on your computer. It provides details such as IP address, subnet mask, default gateway, and DNS servers. To use ipconfig or ifconfig, open the command prompt or terminal and type `ipconfig` (Windows) or `ifconfig` (Linux/Unix).
4. ***Netstat:*** Netstat displays active network connections and listening ports on your computer. It provides information about established connections, listening ports, and network statistics. To use netstat, open the command prompt or terminal and type `netstat`. Additional options can be used to filter the output based on specific criteria.
5. **Nslookup**: Nslookup is used to query DNS (Domain Name System) servers and retrieve information about domain names and their corresponding IP addresses. It can also perform reverse DNS lookups. To use nslookup, open the command prompt or terminal and type `nslookup <domain name or IP address>`. For example, `nslookup www.google.com` or `nslookup 192.168.0.1`.
6. **Route:** Route (or route print on Windows) displays and manipulates the IP routing table. It shows the network destinations and the associated gateway addresses. To use route, open the command prompt or terminal and type `route` (Linux/Unix) or `route print` (Windows).
7. C:\>arp –a: ARP is short form of address resolution protocol, It will show the IP address of your computer along with the IP address and MAC address of your router.
8. C:\>hostname: This is the simplest of all TCP/IP commands. It simply displays the name of your computer.
9. C:\>ipconfig: The ipconfig command displays information about the host (the computer

10. your sitting at) computer TCP/IP configuration.
11. C:\>ipconfig /all: This command displays detailed configuration information about your TCP/IP connection including Router, Gateway, DNS, DHCP, and type of Ethernet adapter in your system.
12. C:\>Ipconfig /renew: Using this command will renew all your IP addresses that you are currently (leasing) borrowing from the DHCP server. This command is a quick problem solver if you are having connection issues, but does not work if you have been configured with a static IP address.
13. C:\>Ipconifg /release: This command allows you to drop the IP lease from the DHCP server.
14. C:\>ipconfig /flushdns: This command is only needed if you're having trouble with your networks DNS configuration. The best time to use this command is after network configuration frustration sets in, and you really need the computer to reply with flushed.
15. C:\>nbtstat –a: This command helps solve problems with NetBIOS name resolution. (Nbt stands for NetBIOS over TCP/IP)
16. C:\>netdiag: Netdiag is a network testing utility that performs a variety of network diagnostic tests, allowing you to pinpoint problems in your network. Netdiag isn't installed by default, but can be installed from the Windows XP CD after saying no to the install. Navigate to the CD ROM drive letter and open the support\tools folder on the XP CD and click the setup.exe icon in the support\tools folder.
17. C:\>netstat: Netstat displays a variety of statistics about a computers active TCP/IP connections. This tool is most useful when you're having trouble with TCP/IP applications such as HTTP, and FTP.

These are just a few examples of basic networking commands. There are many more commands available depending on your operating system and specific networking requirements. You can refer to the documentation or help pages for your operating system to learn more about the available commands and their usage.

Exp2: Installation and introduction of simulation tools packet tracer/GNS3

Sure! I can provide you with an introduction to two popular simulation tools: Cisco Packet Tracer and GNS3.

Cisco Packet Tracer:

Cisco Packet Tracer is a network simulation and visualization tool developed by Cisco Systems. It is primarily designed for educational purposes and allows users to create virtual networks and simulate network devices.

Packet Tracer Features:

1. Network Topology Creation: Packet Tracer enables you to design and create network topologies using a drag-and-drop interface. You can add routers, switches, PCs, servers, and other network devices to build your virtual network.
2. Device Simulation: It provides a simulation environment where you can configure network devices and simulate their behavior. You can configure device settings, set up routing protocols, implement security features, and test network connectivity.
3. Visualizations and Animations: Packet Tracer offers visual representations of network devices and their activities. You can view real-time data flow, packet transmissions, and network traffic animations to better understand network operations.
4. Collaboration and Sharing: It allows collaboration with others by sharing network topologies and project files. This feature is particularly useful for educational purposes, allowing instructors and students to share and work on network designs.
5. Integration with Cisco Networking Academy: Packet Tracer is often used as a learning tool in Cisco Networking Academy courses. It provides an interactive environment for students to practice networking concepts and complete hands-on exercises.

To access Cisco Packet Tracer, you can enroll in the Cisco Networking Academy program, which provides free access to the tool for educational purposes. Cisco also offers Packet Tracer for download to individuals who have a valid Cisco account.

GNS3:

GNS3 (Graphical Network Simulator-3) is an open-source network simulation and emulation software. It allows users to create complex network topologies using virtualization technologies and actual operating systems.

GNS3 Features:

1. Network Emulation: GNS3 allows the emulation of real network devices, such as routers, switches, firewalls, and virtual machines. It can utilize actual operating system images (e.g., Cisco IOS) to replicate the behavior of physical network devices.

2. Virtualization Integration: GNS3 can integrate with popular virtualization technologies like VirtualBox, VMware, and QEMU. This enables you to run virtual machines alongside emulated network devices, providing a more realistic network environment.
3. Advanced Network Configuration: GNS3 provides a high degree of flexibility in network configuration. You can configure advanced routing protocols, experiment with network designs, and test complex scenarios.
4. Community Support and Resource Sharing: GNS3 has an active community where users share network topologies, templates, and configuration

examples. This allows users to learn from others and benefit from a wide range of network designs.

GNS3 is available as a free download from the official GNS3 website (https://www.gns3.com/). You will also need to obtain the necessary operating system images from the respective vendors, such as Cisco, to use with GNS3.

Both Cisco Packet Tracer and GNS3 offer valuable features for network simulation and learning. While Packet Tracer is more user-friendly and suitable for basic network simulations, GNS3 provides a more advanced and flexible environment for complex network configurations and integrations.

Exp3: To construct a simple network topology on Packet Tracer.

To construct a simple network topology using Cisco Packet Tracer, you can follow these steps:

Step 1: Launch Cisco Packet Tracer: Open Cisco Packet Tracer on your computer. If you do not have it installed, you can download it from the Cisco Networking Academy or Cisco's official website.

Step 2: Create a New Project: Click on "File" in the top menu bar and select "New". Choose "Blank Activity" and click "OK" to create a new project.

Step 3: Add Devices: In the left pane, you will find a list of network devices. Drag and drop the desired devices (such as routers, switches, and PCs) onto the workspace area. You can select the devices from the "End Devices," and "Switches" categories.
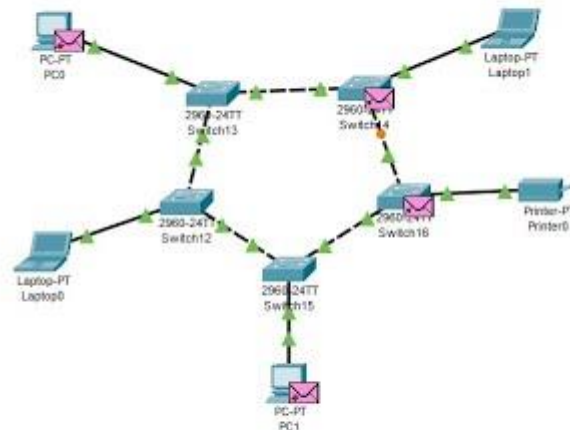
Step 4: Connect the Devices: Use the "Copper Straight Through" or "Copper Cross Over" cable options available in the bottom left corner to connect the devices. Click on the cable type, and then click on the interface of one device and connect it to the interface of another device.

Step 5: Configure Devices: Double-click on each device to open its configuration window. Depending on the device type, you can configure settings like IP addresses, subnet masks, default gateways, and other parameters

Step 6: Set IP Addresses: For PCs or other end devices, double-click on the device to open the configuration window. Go to the "Desktop" tab and select the "IP Configuration" option. Assign the appropriate IP address, subnet mask, and default gateway for each PC.

Step 7: Test Connectivity: Once you have set up the network topology and configured the devices, you can test the connectivity. Use the "Simulation" mode to interact with the devices. Try to ping between different devices to verify network connectivity.

By following these steps, you can construct a simple ring network topology using Cisco Packet Tracer.

Exp4: To configure a Network Topology constitutes Routers and Switches using Packet Tracer.

To configure a network topology with routers and switches using Cisco Packet Tracer, you can follow these steps:

Step 1: Launch Cisco Packet Tracer: Open Cisco Packet Tracer on your computer and create a new project or open an existing one.

Step 2: Add Devices: Drag and drop routers and switches from the device list on the left-hand side onto the workspace area. Place them according to your desired network topology.

Step 3: Connect Devices: Use copper straight-through or crossover cables to connect the devices. Click on the "Copper Cross Over" cable option in the bottom left corner, then click on the interface of one device and connect it to the interface of another device.

Step 4: Configure Routers: Double-click on a router to open its configuration window. Configure the router's interfaces by setting IP addresses, subnet masks, and enabling them.

Step 5: Configure Switches: Double-click on a switch to open its configuration window. Configure VLANs.

Step 6: Verify Connectivity: Once you have configured the routers and switches, you can test network connectivity. Use the "Simulation" mode to interact with the devices. Try pinging between different devices to verify connectivity and ensure proper routing and switching functionality.

Step 7: Save and Export: After configuring the network topology, save your project by clicking on "File" and selecting "Save." You can also export the topology as an image or share the Packet Tracer project file.

By following these steps, you can configure a network topology with routers and switches using Cisco Packet Tracer.

EXP 05: Install and test Router, Repeater and Bridge.

1. Install and Configure a Router:

- Drag and drop a router from the "Routers" category in the device list onto the workspace.
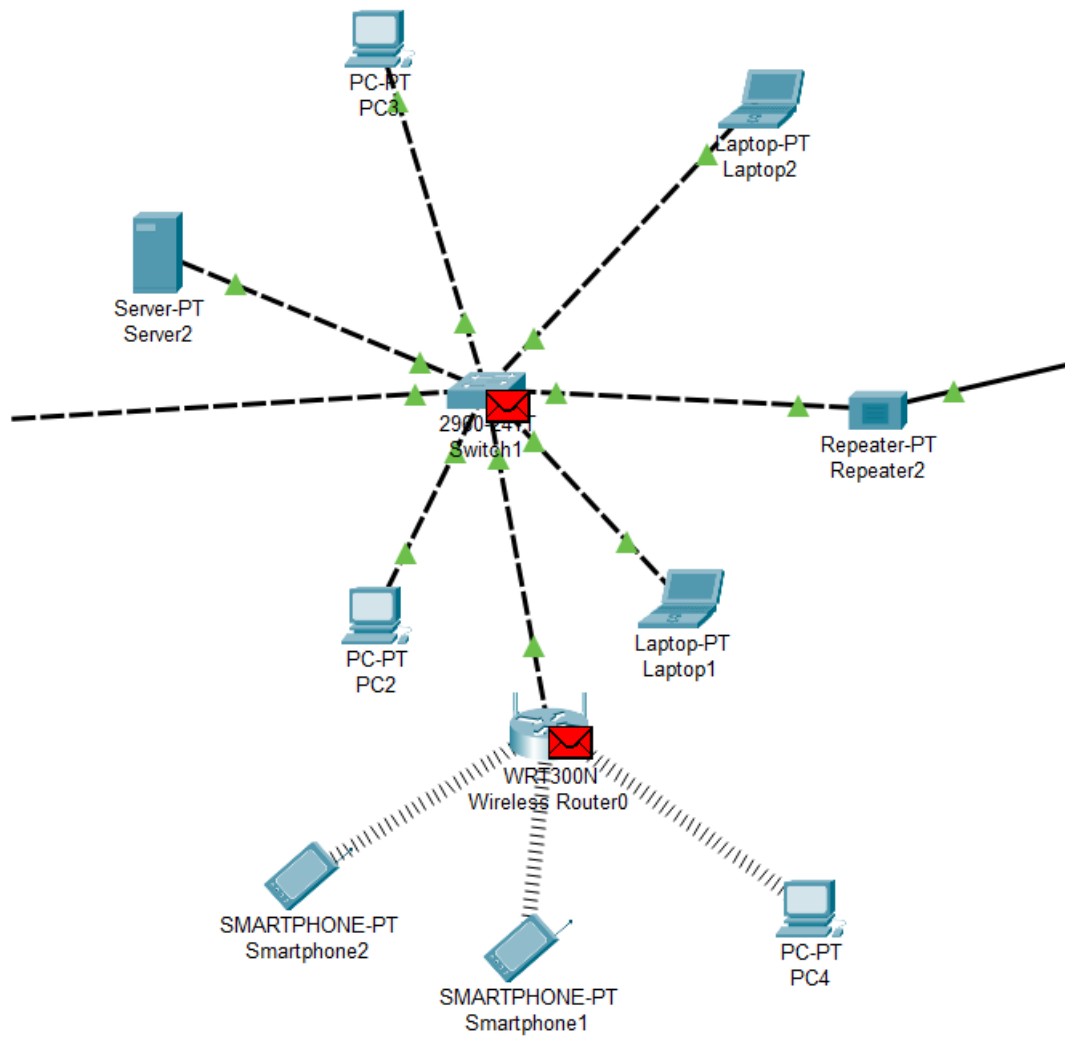- Double-click on the router to open its configuration window.
- Configure the router's interfaces by setting IP addresses, subnet masks, and enabling them.
- Connect PCs or other devices to the router's interfaces using Copper Straight Through cables.
- Test connectivity by pinging between devices connected to different interfaces of the router.

2. Install and Configure a Repeater (Wireless Access Point):

- Drag and drop a wireless router from the "Wireless Devices" category in the device list onto the workspace.
- Double-click on the wireless router to open its configuration window.
- Configure the wireless settings, including SSID (network name), security settings (password or encryption type), and channel.
- Connect a PC or laptop to the wireless router using a Copper Straight Through cable.
- Test connectivity by connecting to the wireless network from the PC and verifying internet access.

3. Install and Configure a Bridge:

- Drag and drop two switches from the "Switches" category in the device list onto the workspace.
- Connect the switches using a Copper Straight Through cable to create a basic network.
- Drag and drop a bridge from the "Wireless Devices" category in the device list onto the workspace.
- Connect one interface of the bridge to one of the switches using a Copper Straight Through cable.
- Connect a PC or laptop to the other interface of the bridge using a Copper Straight Through cable.
- Double-click on the bridge to open its configuration window.

- Configure the bridge to bridge the two interfaces, allowing communication between the connected PC and the switch network.
- Test connectivity by pinging between devices connected to the switch and the bridged PC.
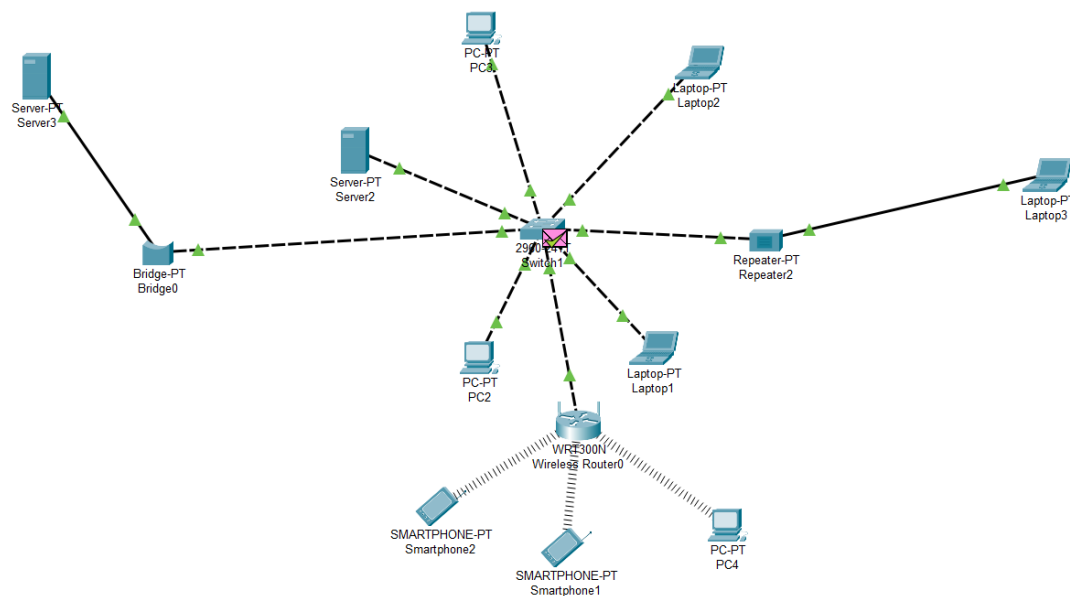
EXP 09: Assign IP address to the PC connected to the internet.

To assign an IP address to a PC connected to the internet in Cisco Packet Tracer, you can follow these steps:

1. Drag and drop a PC from the "End Devices" category in the device list onto the workspace.
2. Click on the PC to select it, and a configuration panel will appear on the right side of the screen.
3. In the configuration panel, click on the "Desktop" tab.
4. Under the "IP Configuration" section, select the "Static" option.
5. Enter the desired IP address, subnet mask, and default gateway in the respective fields.
    a. The IP address should be compatible with your network's IP addressing scheme.
    b. The subnet mask determines the network portion of the IP address.
    c. The default gateway is the IP address of the router or gateway that provides access to the internet.
6. Optionally, you can configure DNS settings by entering the IP address of a DNS server in the "DNS Server" field.
7. Click the "OK" button to save the configuration.

Once assigned the IP address to the PC, it will be able to communicate with other devices on the network and access the internet through the configured default gateway.
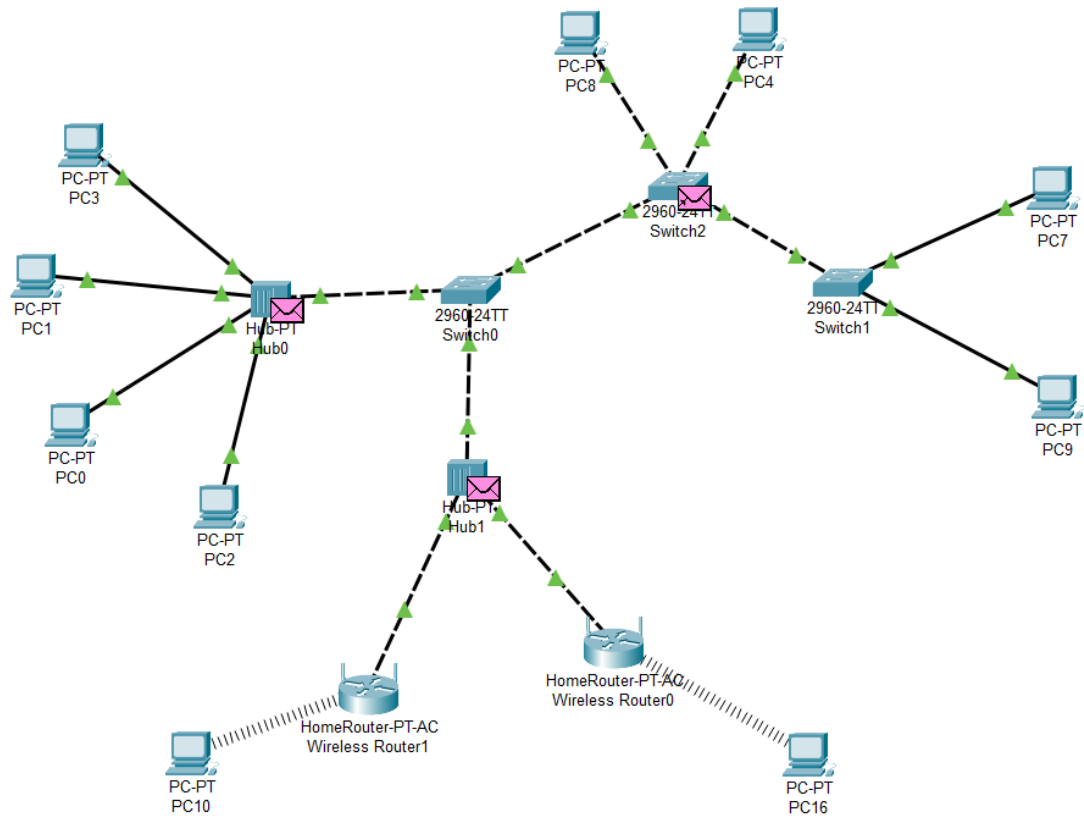
Exp21&22: Implementation of TCP and UDP.

Implementing TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) in Cisco Packet Tracer allows to simulate the behaviour and functionality of these transport layer protocols.

Implementation of TCP:

1. Create a network topology: Drag and drop the desired devices (such as PCs, routers, and switches) from the device list onto the workspace. Connect them using appropriate cables.
2. Configure IP addresses: Assign IP addresses to the devices in the network topology. This can be done through the "Desktop" tab of each PC's configuration panel in Packet Tracer.
3. Configure applications: Select the PCs involved in TCP communication and open their configuration panels. Add network applications (e.g., FTP, HTTP) to simulate TCP traffic. Configure the applications with the desired port numbers.
4. Test TCP communication: Use the configured applications to initiate TCP connections between the PCs. For example, you can use an FTP client on one PC to connect to an FTP server on another PC using the appropriate IP address and port number. Monitor the communication using Packet Tracer's simulation mode or examine the application output for successful TCP transmission.

Implementation of UDP:

1. Create a network topology: Like the TCP implementation, set up the desired network topology with the required devices and connections.
2. Configure IP addresses: Assign IP addresses to the devices in the network topology.
3. Configure applications: Select the PCs involved in UDP communication and open their configuration panels. Add network applications (e.g., DNS, DHCP) to simulate UDP traffic. Configure the applications with the desired port numbers.
4. Test UDP communication: Use the configured applications to send UDP packets between the PCs. For example, you can use a DNS client on one PC to send DNS queries to a DNS server on another PC using the appropriate IP address and port number. Monitor the communication

using Packet Tracer's simulation mode or examine the application output
for successful UDP transmission.
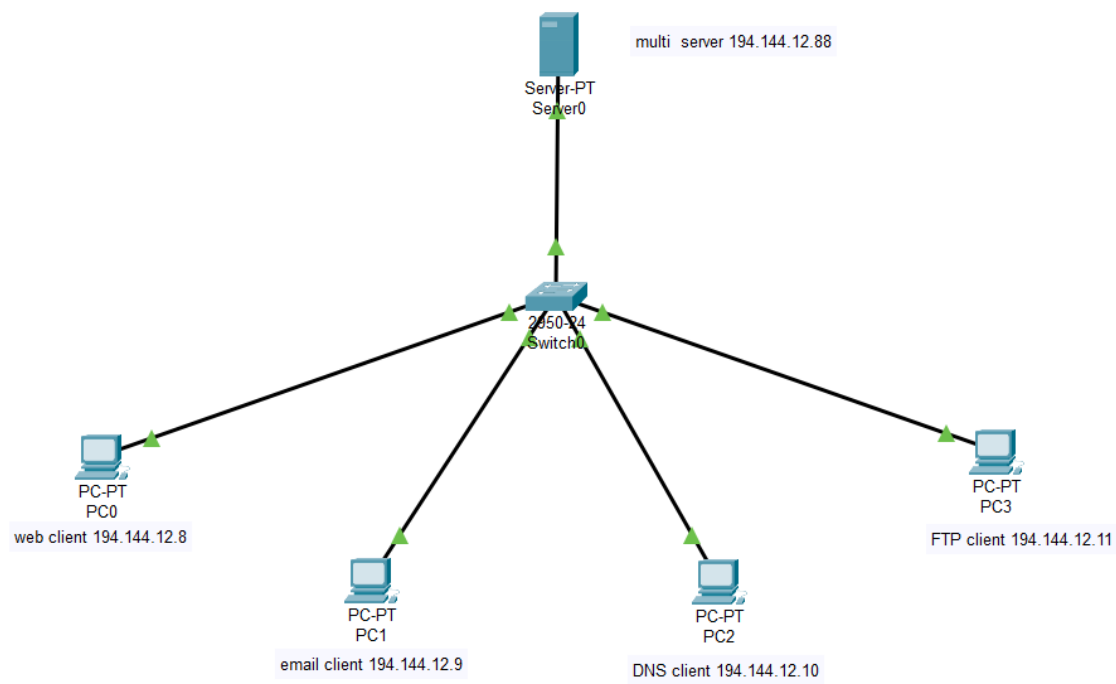
Event List				
Vis.	Time(sec)	Last Device	At Device	Type
	2.602	PC0	Switch0	TCP
	2.602	Switch0	PC0	DNS
	2.602	--	PC0	TCP
	2.603	Switch0	Server0	TCP
	2.603	PC0	Switch0	TCP
	2.604	Server0	Switch0	TCP
	2.604	Switch0	Server0	TCP
	2.605	Switch0	PC0	TCP
	2.605	Server0	Switch0	TCP
	2.606	PC0	Switch0	TCP
	2.606	Switch0	PC0	TCP
	2.606	--	PC0	HTTP
	2.607	Switch0	Server0	TCP
	2.607	PC0	Switch0	TCP
	2.607	--	PC0	HTTP
	2.608	PC0	Switch0	HTTP
	2.608	Switch0	Server0	TCP
Visible	2.609	Switch0	Server0	HTTP

EXP 23,24,25,26:

File Transfer Protocol, Implementation of Domain name Service (DNS), Learning about Configuration of sharing the files/Desktop ,Share a Printer and Folder in Network using packet tracer.

File Transfer Protocol (FTP):

FTP is a standard network protocol used for transferring files between a client and a server over a TCP/IP network. It allows users to upload, download, and manage files on a remote server. To implement FTP in a real-world scenario, you would typically need an FTP server software installed on a server and FTP client software on the client devices. The server and client would communicate using FTP commands and data transfer over TCP connections.

Domain Name Service (DNS):

DNS is a system that translates domain names (e.g., www.example.com) into IP addresses. It is responsible for resolving human-readable domain names to their corresponding IP addresses, allowing users to access websites and other network resources. DNS operates using a hierarchical structure with DNS servers that store and distribute domain name information. Implementing DNS requires setting up DNS servers and configuring domain name records (e.g., A records, CNAME records) to associate domain names with IP addresses.

Configuration of Sharing Files/Desktop:

To configure file or desktop sharing in a network, you can follow these general steps:

1. Enable file or desktop sharing on the desired device (e.g., PC) by accessing the sharing settings or preferences.

2. Specify the files or folders you want to share by selecting them and granting appropriate sharing permissions.

3. Assign a shared name or share path to the files or folders.

4. Configure network permissions to control access to the shared files or folders, such as setting read-only or read/write permissions.

5. Once configured, other devices in the network can access the shared files or desktop by browsing or mapping the network share using the shared name or share path.

Sharing a Printer and Folder in a Network:

To share a printer and folder in a network, you can follow these steps:

1. Connect the printer to a device (e.g., PC) in the network and install the necessary printer drivers.

2. Enable printer sharing on the device by accessing the printer settings or preferences.

3. Specify a shared name for the printer.

4. On other devices in the network, add the shared printer by searching for network printers and selecting the shared printer.

5. To share a folder, follow the steps mentioned earlier for configuring file sharing. Specify the folder to be shared, assign a shared name, or share path, and configure appropriate network permissions for access control.

Please note that the specific steps and options may vary depending on the operating system and network configuration you are using. It's always recommended to refer to the documentation and support resources of the specific software and devices you are working with for detailed instructions on configuring file sharing, printer sharing, and other network services.

DNS :

PC0

Physical Config Desktop Programming Attributes

Web Browser

< > URL http://www.ankit.web   Go   Stop

Home About Portfolio Contact

Welcome to My Portfolio

I am a web developer passionate about creating amazing websites.

About Me

I have several years of experience in web development and have worked on various projects.

Portfolio

Project 1

Project 1
Description of Project 1

Project 2

Project 2
Description of Project 2

Contact Me

Name:

Email:

Message:

Top

FTP

PC2

Physical Config Desktop Programming Attributes

Command Prompt

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ftp 194.144.12.88
Trying to connect...194.144.12.88
Connected to 194.144.12.88
220- Welcome to PT Ftp server
Username:ankit
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>dir

Listing /ftp directory from 194.144.12.88:
0    : asa842-k8.bin                           5571584
1    : asa923-k8.bin                           30468096
2    : c1841-advipservicesk9-mz.124-15.T1.bin  33591768
3    : c1841-ipbase-mz.123-14.T7.bin           13832032
4    : c1841-ipbasek9-mz.124-12.bin            16559160
5    : c1900-universalk9-mz.SPA.155-3.M4a.bin  33591768
6    : c2600-advipservicesk9-mz.124-15.T1.bin  33591768
7    : c2600-i-mz.122-28.bin                   5571584
8    : c2600-ipbasek9-mz.124-8.bin             13169700
9    : c2800nm-advipservicesk9-mz.124-15.T1.bin 50938004
10   : c2800nm-advipservicesk9-mz.151-4.M4.bin 33591768
11   : c2800nm-ipbase-mz.123-14.T7.bin         5571584
12   : c2800nm-ipbasek9-mz.124-8.bin           15522644
13   : c2900-universalk9-mz.SPA.155-3.M4a.bin  33591768
14   : c2950-i6q412-mz.121-22.EA4.bin          3058048
15   : c2950-i6q412-mz.121-22.EA8.bin          3117390
16   : c2960-lanbase-mz.122-25.FX.bin          4414921
17   : c2960-lanbase-mz.122-25.SEE1.bin        4670455
18   : c2960-lanbasek9-mz.150-2.SE4.bin        4670455
19   : c3560-advipservicesk9-mz.122-37.SE1.bin 8662192
20   : c3560-advipservicesk9-mz.122-46.SE.bin  10713279
21   : c800-universalk9-mz.SPA.152-4.M4.bin    33591768
22   : c800-universalk9-mz.SPA.154-3.M6a.bin   83029236
23   : cat3k_caa-universalk9.16.03.02.SPA.bin  505532849
24   : cgr1000-universalk9-mz.SPA.154-2.CG     159487552
25   : cgr1000-universalk9-mz.SPA.156-3.CG     184530138
26   : ir800-universalk9-bundle.SPA.156-3.M.bin 160968869
27   : ir800-universalk9-mz.SPA.155-3.M        61750062
28   : ir800-universalk9-mz.SPA.156-3.M        63753767
29   : ir800_yocto-1.7.2.tar                   2877440
30   : ir800_yocto-1.7.2_python-2.7.3.tar      6912000
31   : name.txt                                17
32   : pt1000-i-mz.122-28.bin                  5571584
33   : pt3000-i6q412-mz.121-22.EA4.bin         3117390
ftp>get name.txt

Reading file name.txt from 194.144.12.88:
File transfer in progress...

[Transfer complete - 17 bytes]
```
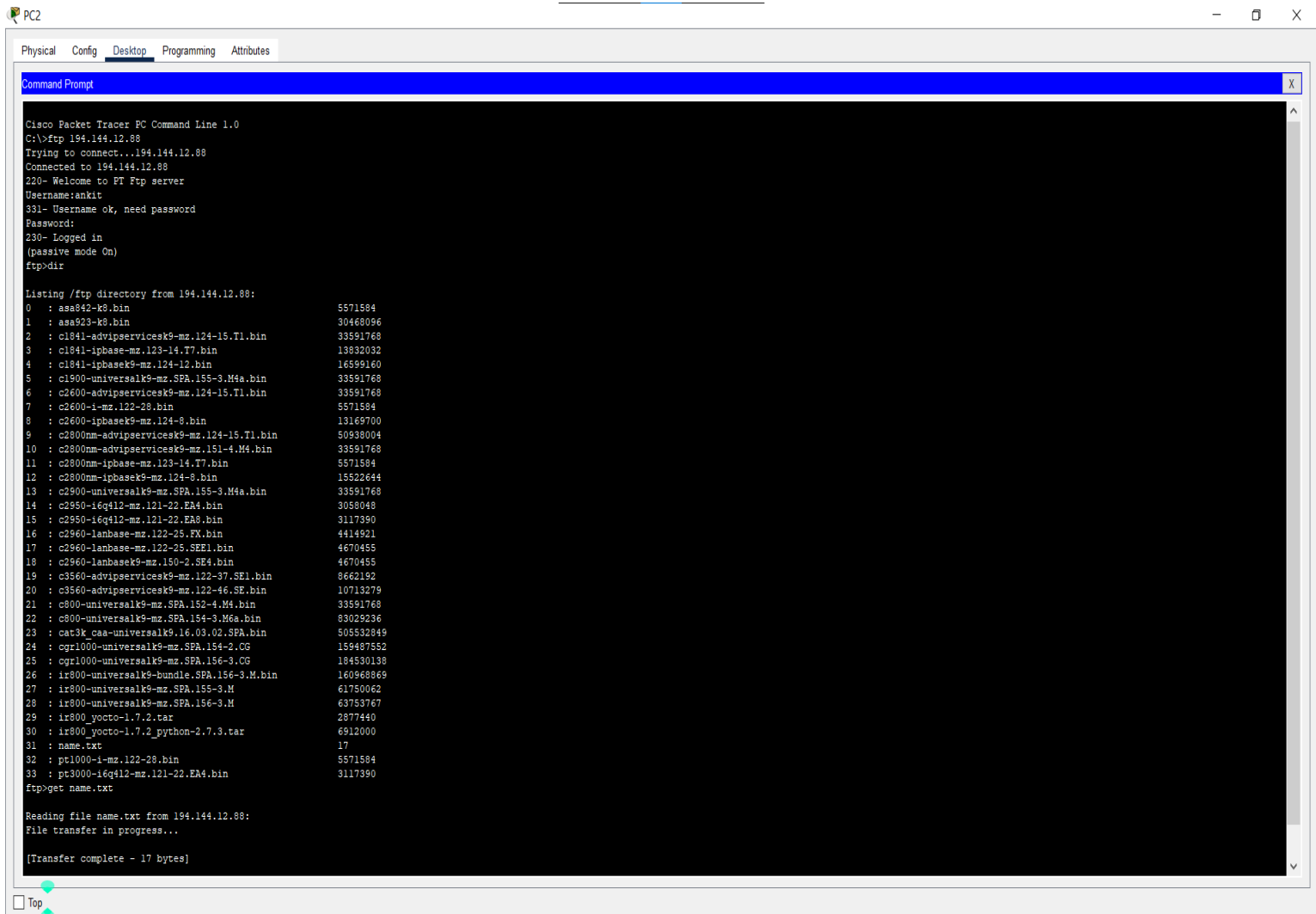
Top

Sharing a Printer and Folder in a Network: