

Worksheet Number – 1.3

NAME –

UID –

SEC –

BRANCH – BTECH CSE

SUB – COMPUTER NETWORK

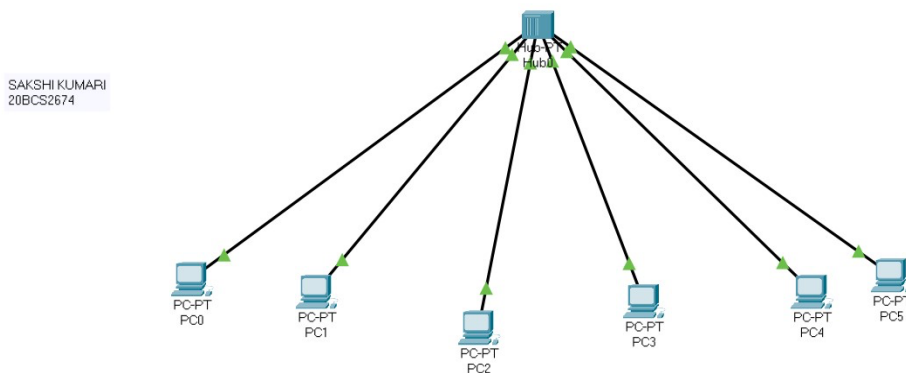
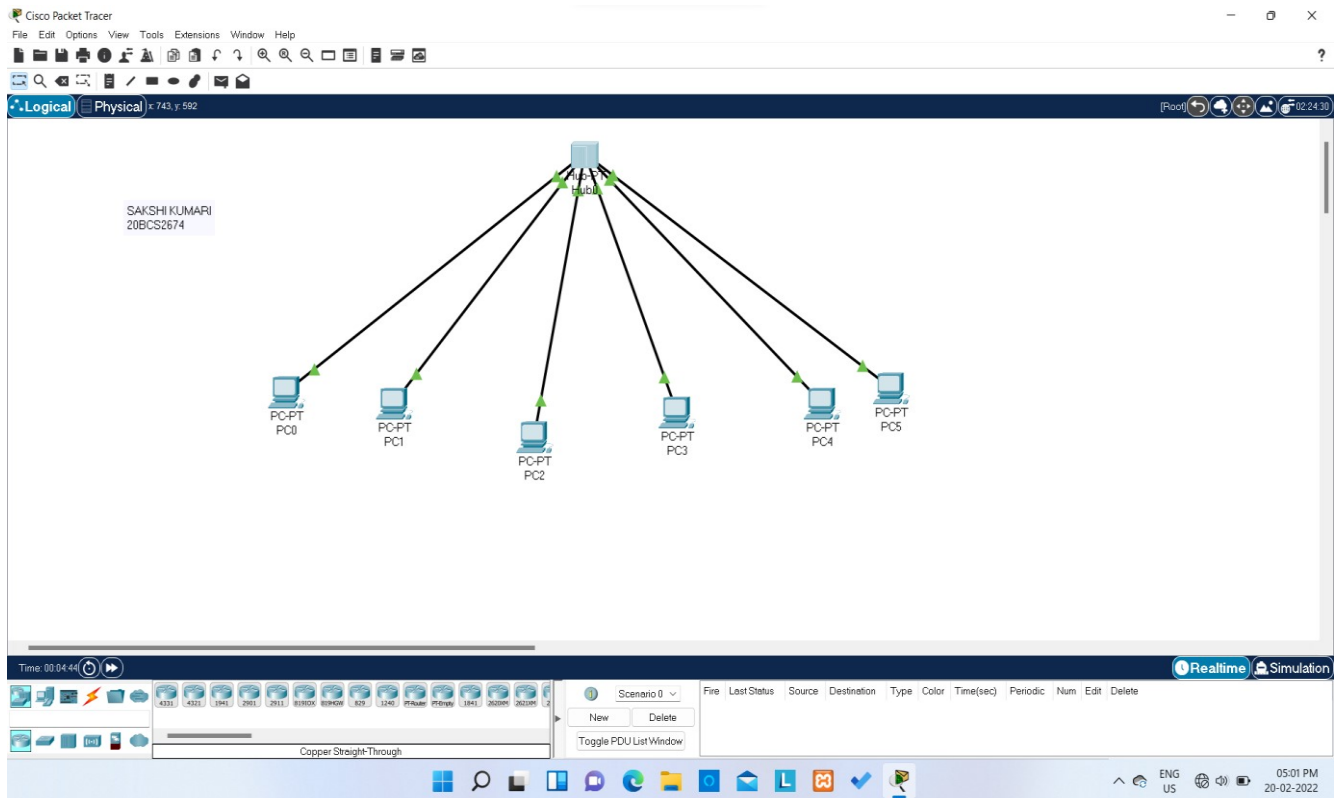
D.O.S – 05/03/2022

Configure and understand working of network devices Hub, Switch, Routers

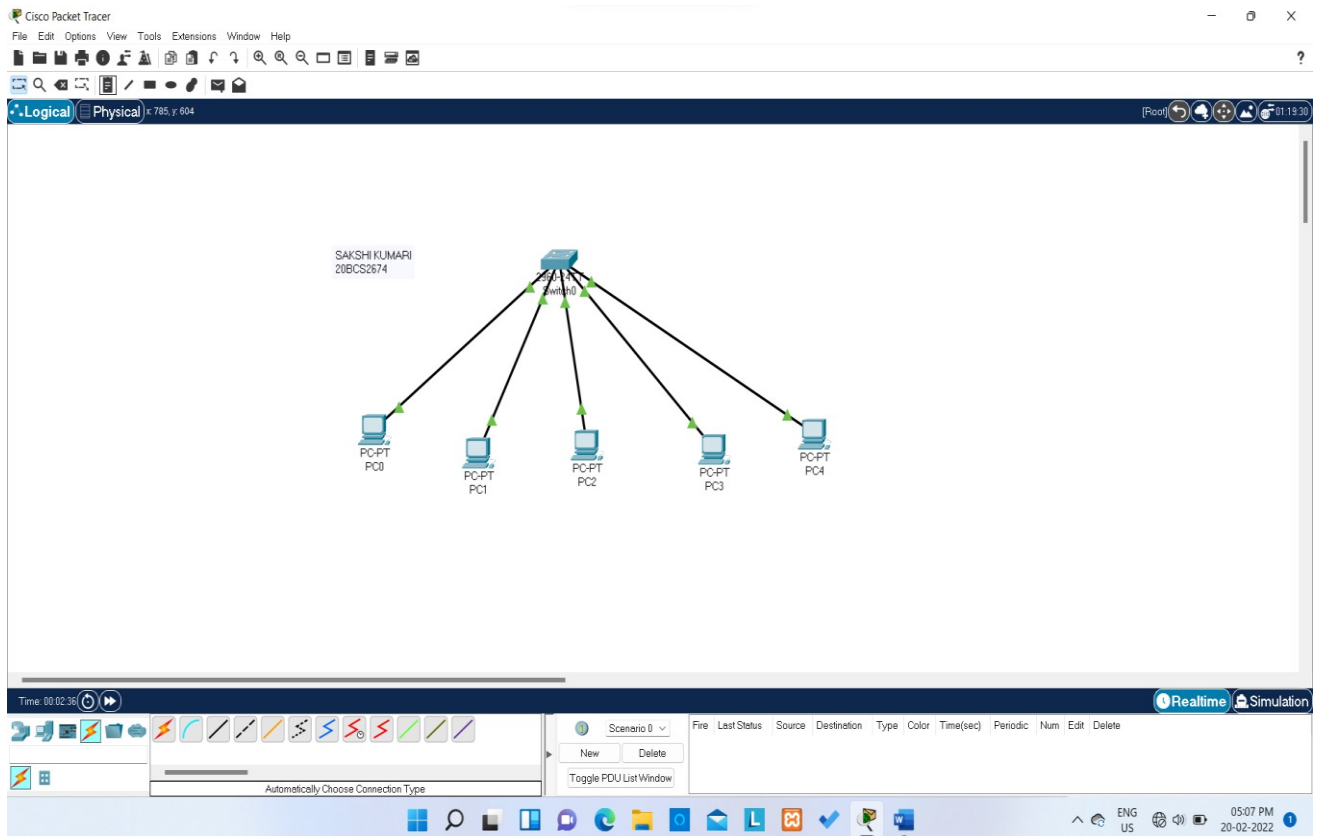
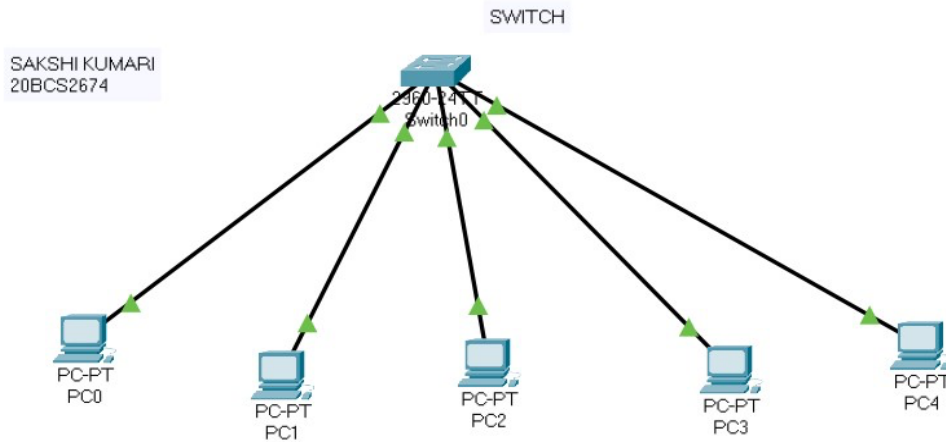
Hub – A hub is basically a multiport repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations. Hubs cannot filter data, so data packets are sent to all connected devices. In other words, the collision domain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

Types of Hub

- **Active Hub:-** These are the hubs that have their own power supply and can clean, boost, and relay the signal along with the network. It serves both as a repeater as well as a wiring center. These are used to extend the maximum distance between nodes.
- **Passive Hub :-** These are the hubs that collect wiring from nodes and power supply from the active hub. These hubs relay signals onto the network without cleaning and boosting them and can't be used to extend the distance between nodes.
- **Intelligent Hub :-** It works like active hubs and includes remote management capabilities. They also provide flexible data rates to network devices. It also enables an administrator to monitor the traffic passing through the hub and to configure each port in the hub.



Switch – A switch is a multiport bridge with a buffer and a design that can boost its efficiency(a large number of ports imply less traffic) and performance. A switch is a data link layer device. The switch can perform error checking before forwarding data, which makes it very efficient as it does not forward packets that have errors and forward good packets selectively to the correct port only. In other words, the switch divides the collision domain of hosts, but broadcast domain remains the same.



Step 1: Inspect your hardware

Check the model number of your shiny new switch. Or, if you are using a spare, check the device hardware and its connected cables for any damages. If everything checks out, power on the switch and verify that all the indicator lights are in working order. Next, use a rollover cable to console into the switch from your computer. To do this, you will need to download and install Putty (or a similar, fun-named software tool). Run Putty and select the 9600 speed serial connection. You are now connected to the switch and ready to check the output of the following commands:

- show version
- show running-config
- show VLAN brief
- show VTP status
- (config)# IP domain-name routerfreak.com
- (config)# hostname Switch01
- (config)# interface VLAN1
- (config)# description Management VLAN
- (config)# IP address 192.168.101.1 255.255.255.0
- vtp [client | server | transparent]
- vtp domain name
- description *** DESCRIPTION ***
- switchport access vlan ###
- sswitchport mode access
- power inline consumption ###
- queue-set 2
- mls qos trust dscp
- storm-control multicast level 50.00
- no cdp enable
- spanning-tree portfast
- spanning-tree bpduguard enable
- Interface GigabitEthernet1/0/1
- description *** UPLINK ***
- switchport trunk encapsulation dot1q

- switchport mode trunk
- speed 1000
- duplex full
- Switch01(config)# crypto key generate rsa
- The name for the keys will be:
- Switch01.routerfreak.com
- How many bits in the modulus [512]: 1024
- % Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
- # line vty 0 4
- (config-line)# transport input ssh
- (config-line)# login local
- (config-line)# password routerfreak
- (config-line)# exit
- # line console 0
- (config-line)# logging synchronous
- (config-line)# login local
- Switch01# service password-encryption
- remote-computer# ssh 192.168..101.1
- Log in as: username
- Password:
- Switch01>en
- Password:
- Switch01#

For spare switches, make sure to delete the flash:vlan.dat file to erase the previous configuration.

Step 2: Set up management IP

Unlike with that punny name you gave your home Wi-Fi network, when setting up the hostname for your switch you should probably stick to a more professional and standard naming convention. Follow any preset naming assignment your company is using and then assign an IP address on the management VLAN. Next, make sure your switch has a set hostname and domain name:

Step 3: Check VTP revision number

Hit the `show vtp status` command to reveal your Virtual Trunking Protocol (VTP) revision numbers. The VTP revision numbers determine which updates are to be used in a VTP domain. When you set a VTP domain name, the revision number is set to zero—after which each change to the VLAN database increases the revision number by one. Your switch will only process data from a neighboring switch coming from the same domain and if the revision number of the neighboring switch is higher than its own. This means that the switches will update their VLAN configuration based on the VTP information being sent by the switch with the highest revision number.

So, before you add your switch to the network, you're going to want to set its revision number to zero. To easily reset the domain back to zero, change the config mode to transparent:

Step 4: Configure access ports

You might already have a template ready for access port configuration, but in case you don't, here are some commands you should use:

Step 5: Configure trunk ports

Enter the command `sh int g0/1` capabilities and check the trunking protocol supported. If ISL is supported, you have to issue the `switchport trunk encapsulation dot1q` on the trunk port configuration. If not, simply type `switchport mode trunk`. It means there is no other encapsulation supported so there is no need for an encapsulation command. It only supports 802.1Q.

Step 6: Configure access ports

After already performing basic network switch configurations, it's time to generate RSA keys to be used during the SSH process, using the crypto commands shown here:

Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes.

Step 7: Set up VTY line config

If you have not set the console line yet, you can easily input these values:

Set the enable password using the `enable secret password` command. Then, set the `privilege exec password` with `username name privilege 15 secret password`. Make sure that the password-encryption service is activated.

Verify SSH access by typing `'sh ip ssh'` to confirm that the SSH is enabled. You can now try to log in from a remote machine to verify that you can ssh to your Cisco switch.



DEPARTMENT OF ACADEMIC AFFAIRS

Discover. Learn. Empower.

NAAC
GRADE A+
ACCREDITED UNIVERSITY