1. Network Topology Setup
   i. Create the Network
      - Open Cisco Packet Tracer
      - Add devices: 1 Router, 1 Server - Acts as DHCP Server, 2 PCs - Rename to PC0 and PC1, 1 Switch
   ii. Connect Devices
      - Connect PC0, PC1, and Server to Switch using Copper Straight-Through cables
      - Connect Switch to Router's GigabitEthernet 0/0 using Copper Straight-Through cable
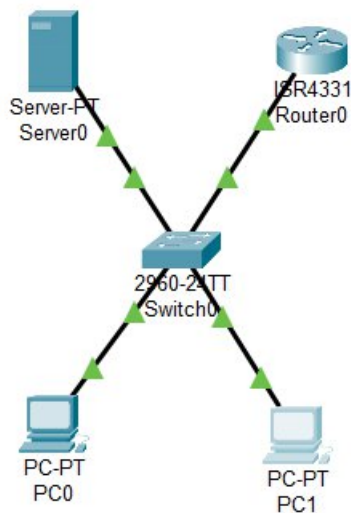
2. IP Address Configuration using DHCP
   i. Configure Router Interface
      - Allocate ip 192.168.47.1 to router and set it's subnet mask to 255.255.255.0
   ii. Configure DHCP Server
      - Server Configuration: IP Address: 192.168.47.2, Default Gateway: 192.168.47.1
      - DHCP Pool: Default Gateway: 192.168.47.1, DNS Server: 192.168.47.2, Start IP: 192.168.47.1, Subnet Mask: 255.255.255.0
   iii. Configure PCs for DHCP
      - PC0 → Config Tab → FastEthernet → Select DHCP

- PC1 → Config Tab → FastEthernet → Select DHCP

3. Router Configuration for Remote Access
   i. Basic Router Configuration
      - Router> enable
      - Router# configure terminal
      - Router(config)# hostname HQ
      - HQ(config)# interface gigabitethernet 0/0
      - HQ(config-if)# ip address 192.168.X.1 255.255.255.0
      - HQ(config-if)# no shutdown
      - HQ(config-if)# exit

   ii. SSH Configuration
      - HQ(config)# ip domain-name cns-assignment.com
      - HQ(config)# crypto key generate rsa
      - (Choose 1024 bits modulus)
      - HQ(config)# ip ssh version 2
      - HQ(config)# ip ssh time-out 60
      - HQ(config)# ip ssh authentication-retries 2
   iii. User and Line Configuration
      - HQ(config)# username admin secret admin123
      - HQ(config)# enable secret class123
      - HQ(config)# line vty 0 4
      - HQ(config-line)# login local

- HQ(config-line)# transport input telnet ssh
- HQ(config-line)# exit
- HQ(config)# exit
- HQ# write memory

Router0

Physical   Config   CLI   Attributes

IOS Command Line Interface

```
HQ>enable
Password:
Password:
HQ#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
HQ(config)#ip domain-name cns-assignment.com
HQ(config)#crypto key generate rsa
% You already have RSA keys defined named HQ.cns-assignment.com .
% Do you really want to replace them? [yes/no]: yes
The name for the keys will be: HQ.cns-assignment.com
Choose the size of the key modulus in the range of 360 to 4096 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

HQ(config)#ip ssh version 2
*Mar 1 0:11:10.325: %SSH-5-ENABLED: SSH 2 has been enabled
HQ(config)#ip ssh time-out 60
HQ(config)#ip ssh authentication-returies 2
                                       ^
% Invalid input detected at '^' marker.

HQ(config)#ip ssh authentication-retries 2
HQ(config)#username admin secret admin123
HQ(config)#line vty 0 4
HQ(config-line)#login local
HQ(config-line)#transport input ssh
HQ(config-line)#transport local telnet
                          ^
% Invalid input detected at '^' marker.

HQ(config-line)#transport input telnet
HQ(config-line)#exec-timeout 5 0
HQ(config-line)#exit
HQ(config)#enable secret class123
HQ(config)#exit
HQ#
%SYS-5-CONFIG_I: Configured from console by console
write memory
Building configuration...
```

4. Access Remote Device – Telnet
   i.   Access Telnet from PC1
        - Go to PC1 → Desktop Tab → Command Prompt
        - Enter telnet 192.168.47.1
        - Use Username: admin
        - Enter Password: admin123
        - HQ> enable
        - Password: class123

5. Access Remote Device – SSH
   i.   PC0 → Desktop Tab → Command Prompt
        - C:\> ssh -l admin 192.168.47.1
        - Password: admin123
        - HQ> enable

- Password: class123

PC1 — Command Prompt

```
C:\>telnet 192.168.47.1
Trying 192.168.47.1 ...Open


User Access Verification

Username: admin
Password:
HQ>enable
Password:
HQ#
HQ#
```

PC0 — Command Prompt

```
C:\>ssh -l admin 192.168.47.1

Password:



HQ>enable
Password:
HQ#
HQ#
```

PC1 — Command Prompt

```
C:\>ping 192.168.47.1

Pinging 192.168.47.1 with 32 bytes of data:

Reply from 192.168.47.1: bytes=32 time=19ms TTL=255
Reply from 192.168.47.1: bytes=32 time<1ms TTL=255
Reply from 192.168.47.1: bytes=32 time<1ms TTL=255
Reply from 192.168.47.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.47.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 19ms, Average = 4ms

C:\>
```

PC0 — Command Prompt

```
C:\>
C:\>ping 192.168.47.1

Pinging 192.168.47.1 with 32 bytes of data:

Reply from 192.168.47.1: bytes=32 time<1ms TTL=255
Reply from 192.168.47.1: bytes=32 time<1ms TTL=255
Reply from 192.168.47.1: bytes=32 time<1ms TTL=255
Reply from 192.168.47.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.47.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```
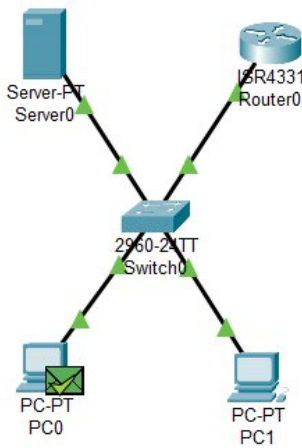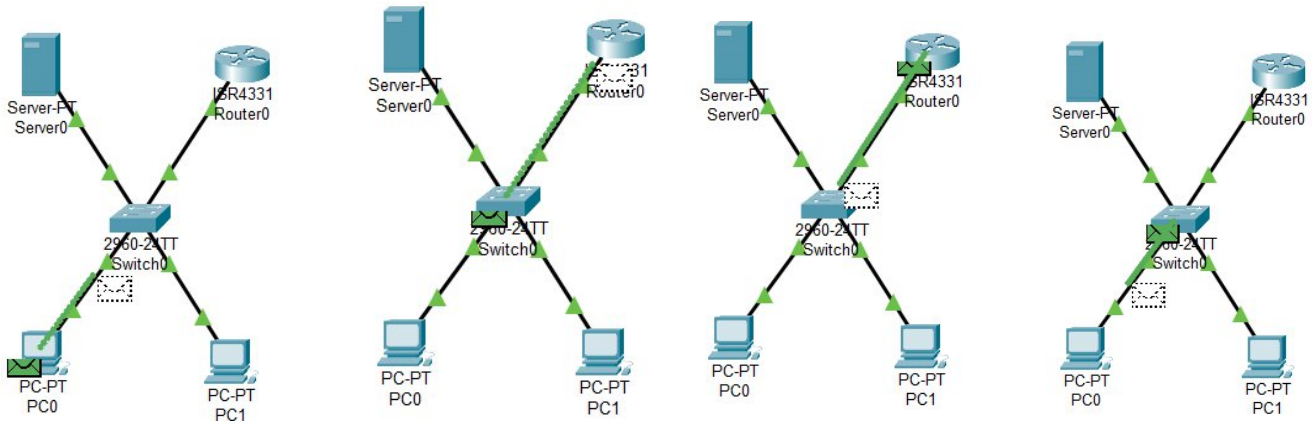
6. Real Mode and Event Simulation
   i.   Real Mode

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC0	Router0	ICMP		0.000	N	0	(edit)	(delete)
	Successful	PC1	Router0	ICMP		0.000	N	1	(edit)	(delete)
	Successful	Router0	PC0	ICMP		0.000	N	2	(edit)	(delete)
	Successful	Router0	PC1	ICMP		0.000	N	3	(edit)	(delete)

ii.   Event Simulation

Vis.	Time(sec)	Last Device
	0.000	--
	0.002	PC0
	0.004	Switch0
	0.006	Router0
	0.008	Switch0
👁	1.999	--

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
●	Successful	PC0	Router0	ICMP	■	0.000	N	0	(edit)	(delete)