

## Practical No: 01

**Aim:** Configuring WEP on a Wireless Router

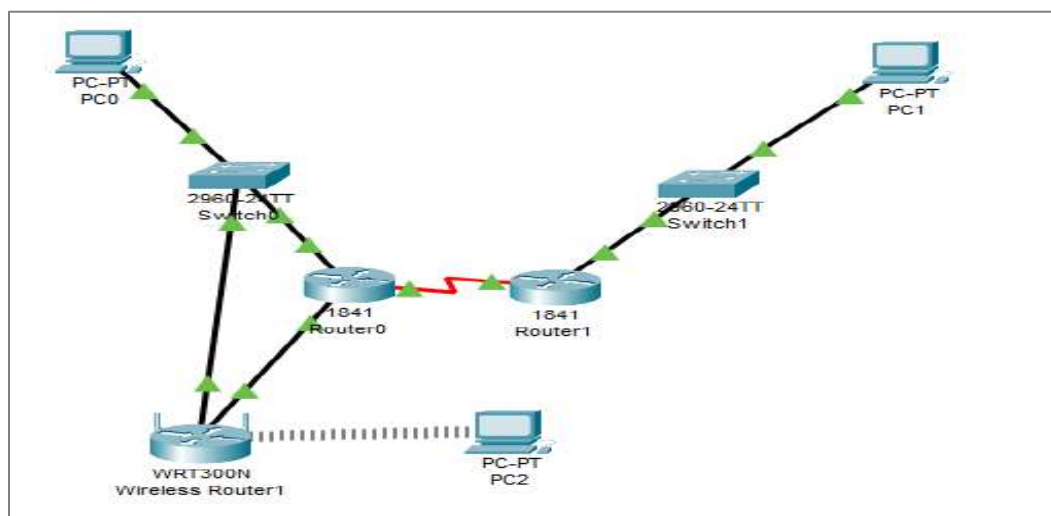
**Components:** Wireless Router, Router, Switch, Device (PC)

**Theory:** Wired Equivalent Privacy (WEP) is a security protocol, specified in the IEEE Wireless Fidelity (Wi-Fi) standard, 802.11b. That standard is designed to provide a wireless local area network (WLAN) with a level of security and privacy comparable to what is usually expected of a wired LAN.

**Cisco Packet Tracer Setup:-**

**Implementation:**

**Step 1:** Creating connections using Ethernet and serial cable between devices



**Step 2:** Configuring all devices according to the table below

Device	Interface	IPv4 address	Other
PC0	IP configuration in desktop	192.168.1.2	Default Gateway: 192.168.1.1
PC1	IP configuration in desktop	192.168.2.2	Default Gateway: 192.168.2.1
Router0	FastEthernet0/0	192.168.1.1	
Router0	FastEthernet0/1	20.0.0.1	
Router0	Serial0/0/0	10.0.0.1	Clock rate: 64000
Router1	FastEthernet0/0	192.168.2.1	
Router1	Serial0/0/0	10.0.0.2	Clock rate: 64000
PC2	IP Config in desktop		Set to DHCP

### Step 3: Configuring wireless router

# Click on wireless router > GUI and set the address

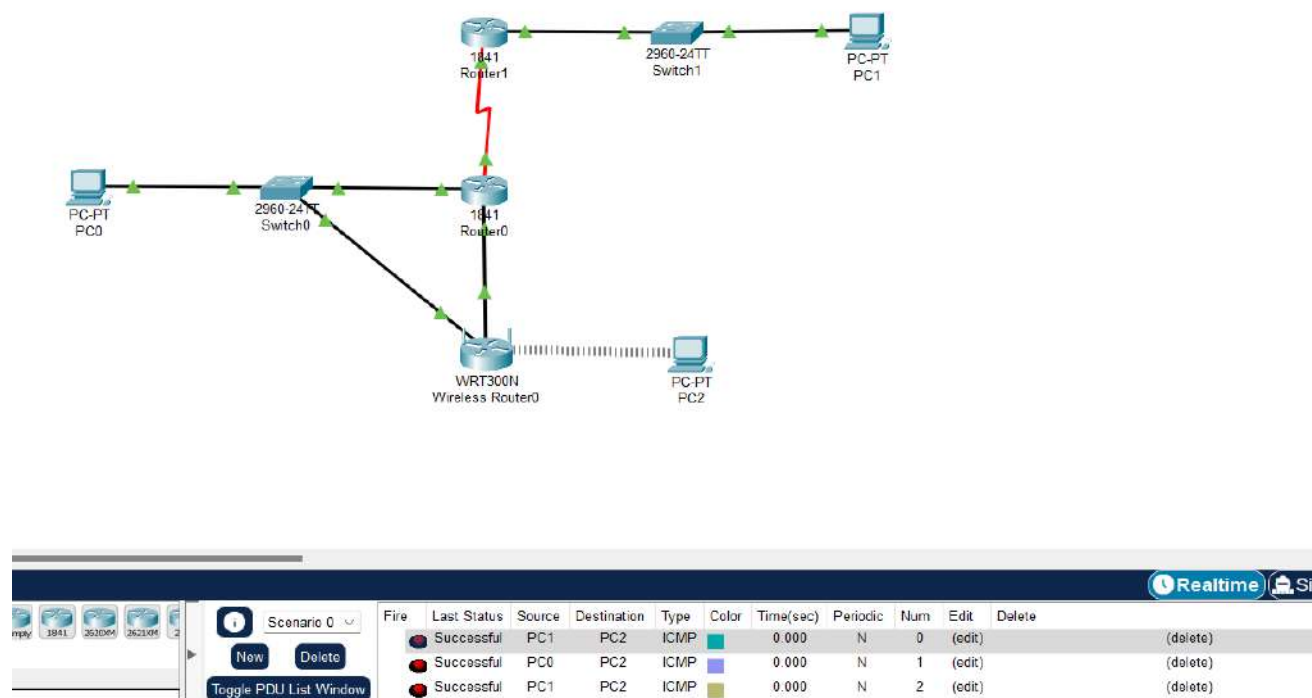
IP Address:  .  .  .

Subnet Mask:

DHCP Server: ☒ Enabled ☐ Disabled

### Step 4: Adding security mode as **WEP** and setting up key as **2a2a2a2a2a**

Output:



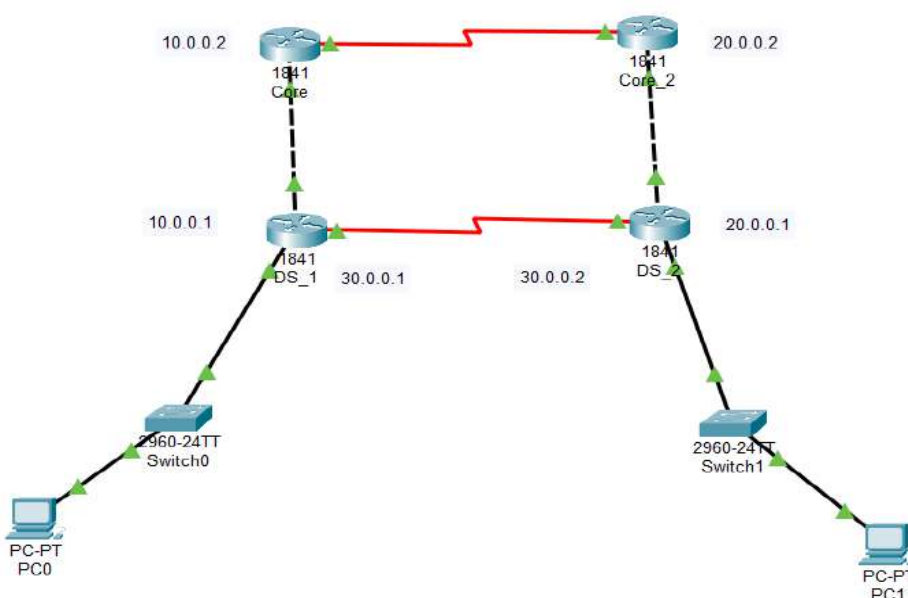
## Practical No: 02

**Aim:** Demonstrating Distribution Layer Functions

**Components:** Router, Switch, Device (PC)

**Theory:** The distribution layer is the smart layer in the three-layer model. Routing, filtering, and QoS policies are managed at the distribution layer. Distribution layer devices also often manage individual branch-office WAN connections. This layer is also called the Workgroup layer.

**Cisco Packet Tracer Setup:-**

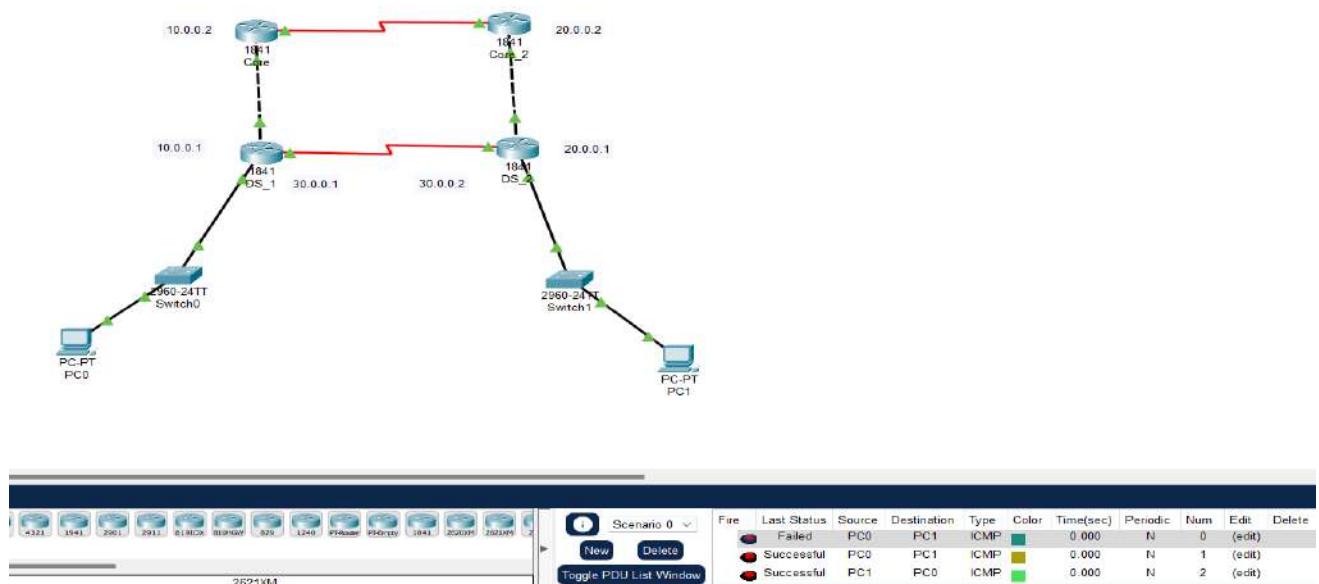


**Implementation:**

**Step 1:** Arranging devices and creating connections using Ethernet and serial cable between devices according to the image above

**Step 2:** Configuring all devices according to the table below

Device	Interface	IPv4 address	Other
PC0	IP config	172.16.1.2	Default Gateway: 172.16.1.1
PC1	IP config	192.168.1.2	Default Gateway: 192.168.1.1
DS_1	F0/0	172.16.1.1	
	F0/1	10.0.0.1	
	S0/0/0	30.0.0.1	Clock rate: 64000
	RIP v2	10.0.0.0 30.0.0.0 172.16.0.0	
DS_2	F0/0	192.168.1.1	
	F0/1	20.0.0.1	
	S0/0/0	30.0.0.2	Clock rate: 64000
	RIP v2	20.0.0.0 30.0.0.0 192.168.1.0	
Core_1	F0/0	10.0.0.2	
	S0/0/0	40.0.0.1	
	RIP v2	10.0.0.0 40.0.0.0	
Core_2	F0/0	20.0.0.2	
	S0/0/0	40.0.0.2	Clock rate: 64000
	RIP v2	20.0.0.0 40.0.0.0	

**Output:**

## Practical No: 03

**Aim:** Placing ACLs

**Components:** PC, switch, router, server

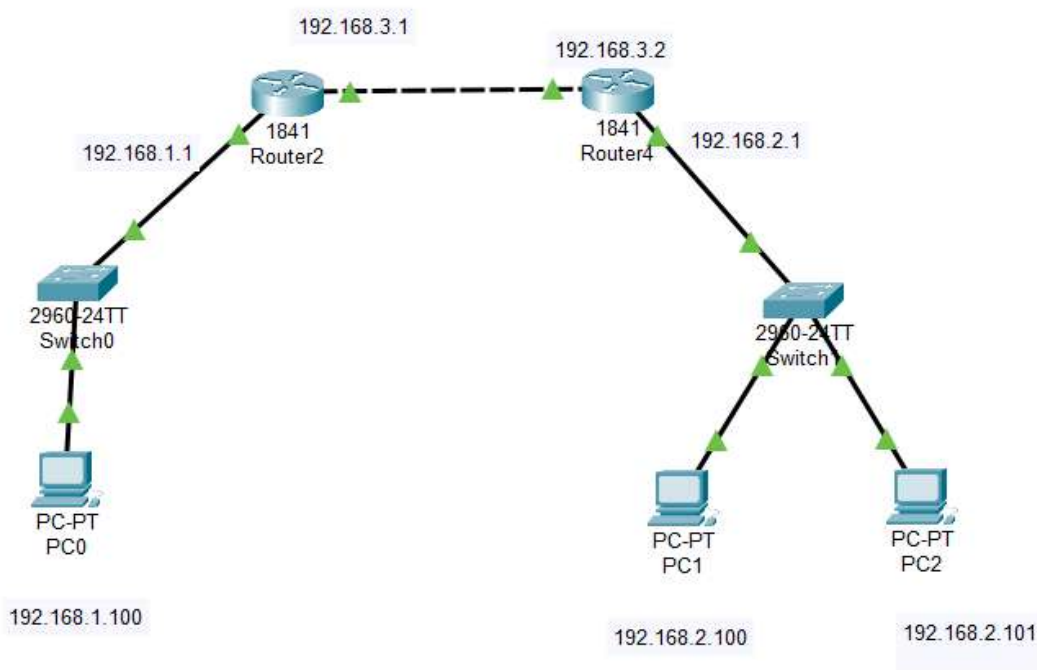
**Theory:** A network access control list (ACL) is made up of rules that either allow access to a computer environment or deny it. In a way, an ACL is like a guest list at an exclusive club. Only those on the list are allowed in the doors. This enables administrators to ensure that, unless the proper credentials are presented by the device, it cannot gain access.

### Cisco Packet Tracer Setup:-

A) Standard ACL

### Implementation:

**Step 1:** Arranging devices and creating connections and assign IP address as shown below



**Step 2:** creating access-list in router2 CLI as shown below

```

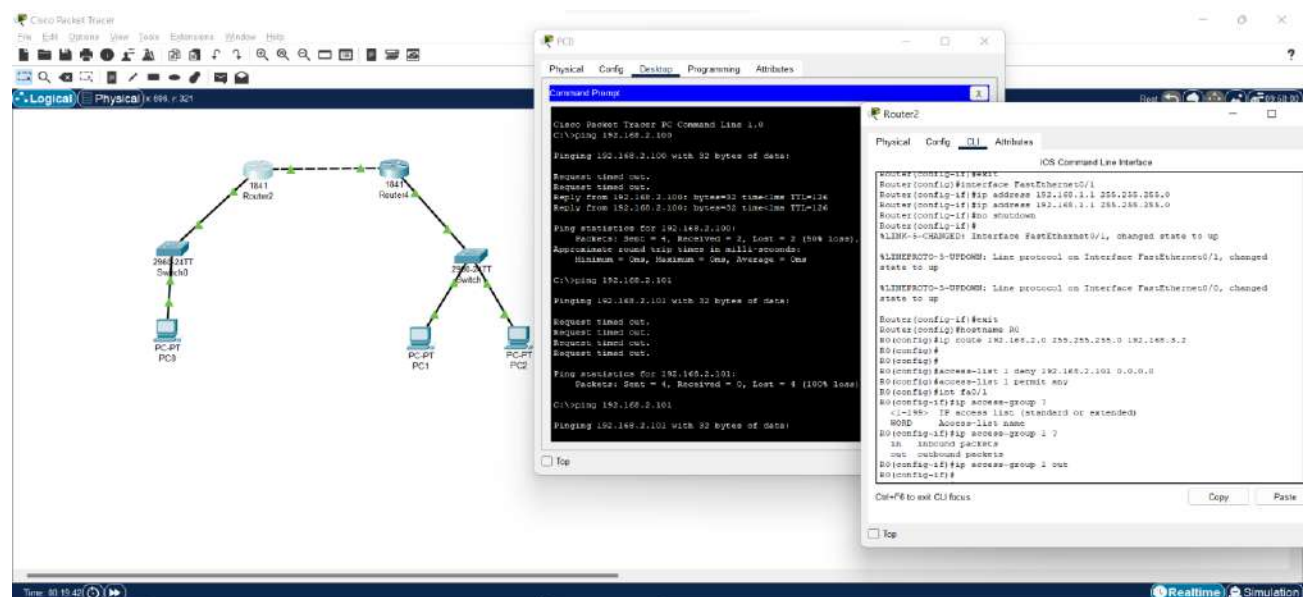
Router(config-if)#exit
Router(config)#hostname R0
R0(config)#ip route 192.168.2.0 255.255.255.0 192.168.3.2
R0(config)#
R0(config)#
R0(config)#access-list 1 deny 192.168.2.101 0.0.0.0
R0(config)#access-list 1 permit any
R0(config)#int fa0/1
R0(config-if)#ip access-group ?
    <1-199> IP access list (standard or extended)
    WORD    Access-list name
R0(config-if)#ip access-group 1 ?
    in      inbound packets
    out     outbound packets
R0(config-if)#ip access-group 1 out
R0(config-if)#

```

Ctrl+F6 to exit CLI focus

Copy Paste

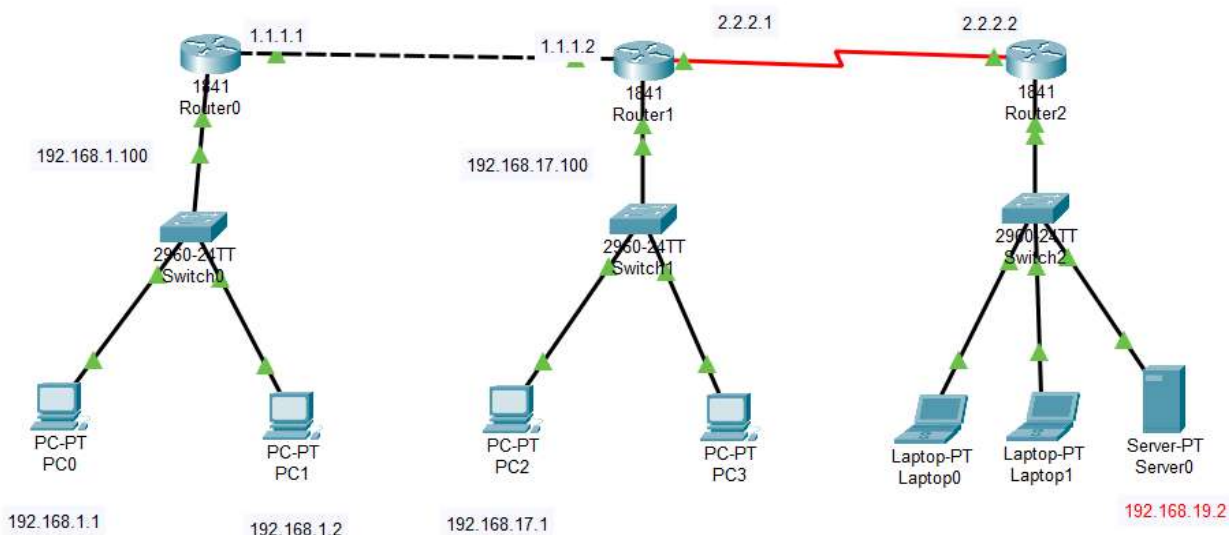
**Output:**



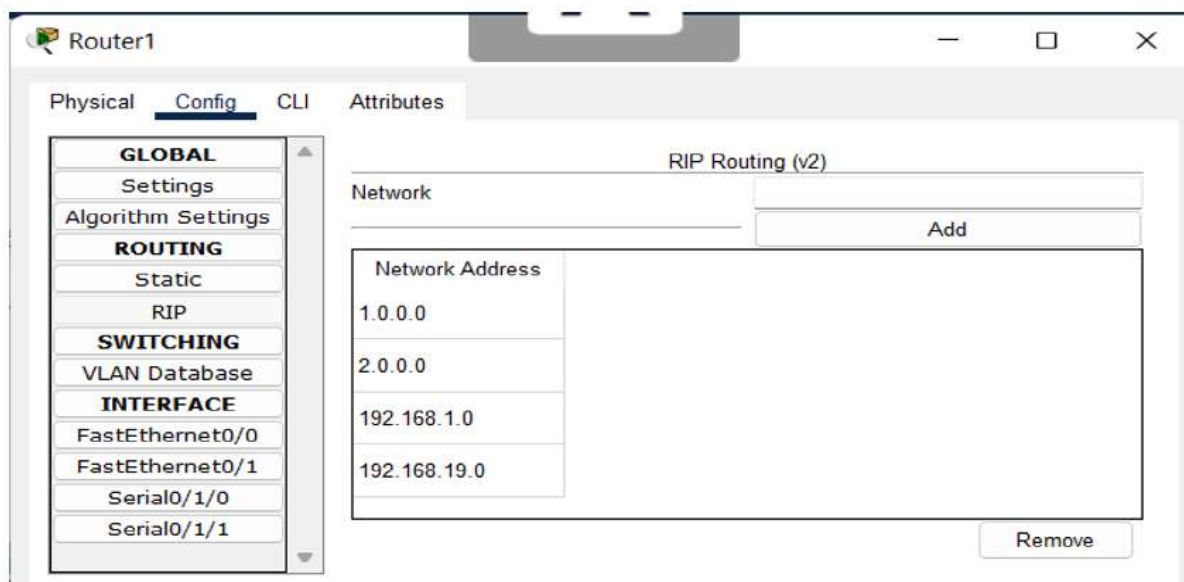
## B) Extended ACL

### Implementation

**Step 1:** Create the layout shown below and set the IP address accordingly



**Step 2:** configuring the RIP protocol

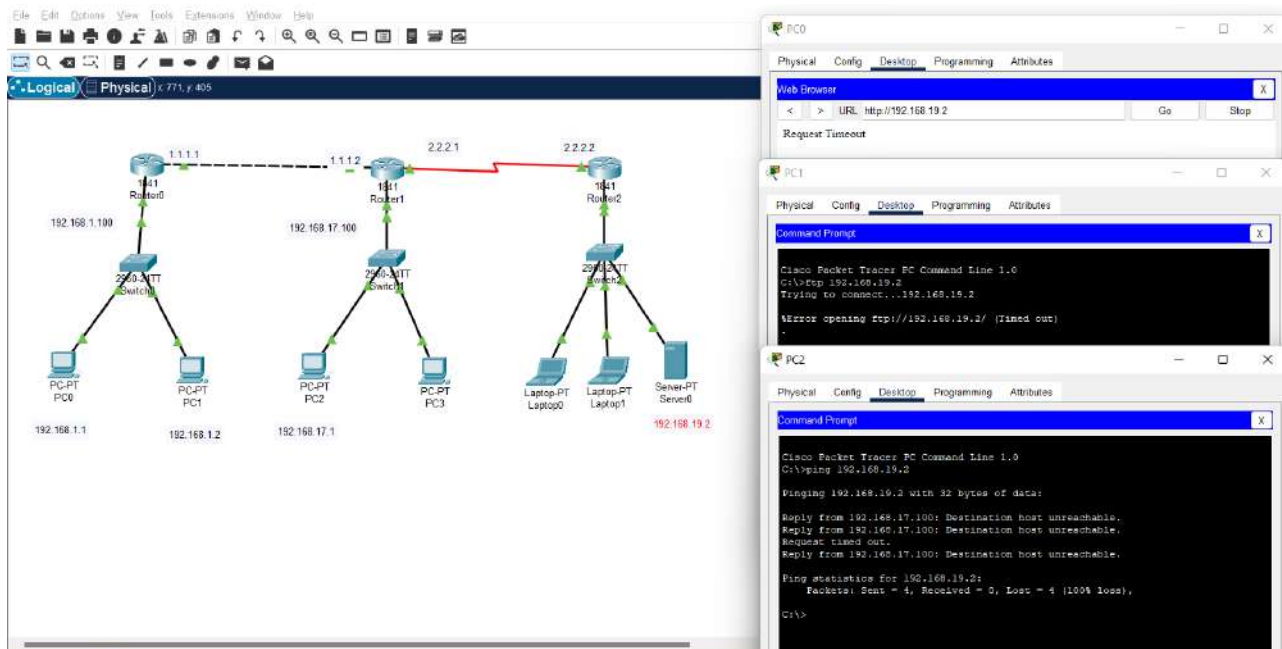


### Step 3: Setting the access list in Router0 > CLI

```
Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#access-list 100 deny tcp host 192.168.1.1
Router(config)#access-list 100 deny tcp host 192.168.1.1 host 192.168.19.2 eq
www
Router(config)#access-list 100 deny tcp host 192.168.17.1 host 192.168.19.2
eq ftp
Router(config)#access-list 100 deny icmp host 192.168
                                     ^
% Invalid input detected at '^' marker.

Router(config)#access-list 100 deny icmp host 192.168.1.2 host 192.168.19.1
Router(config)#access-list 100 permit ip any any
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#int se0/1/0
Router(config-if)#ip access-group 100 out
Router(config-if)#
```

**Output:**





## Practical No: 04

**Aim:** Planning Network-based Firewalls

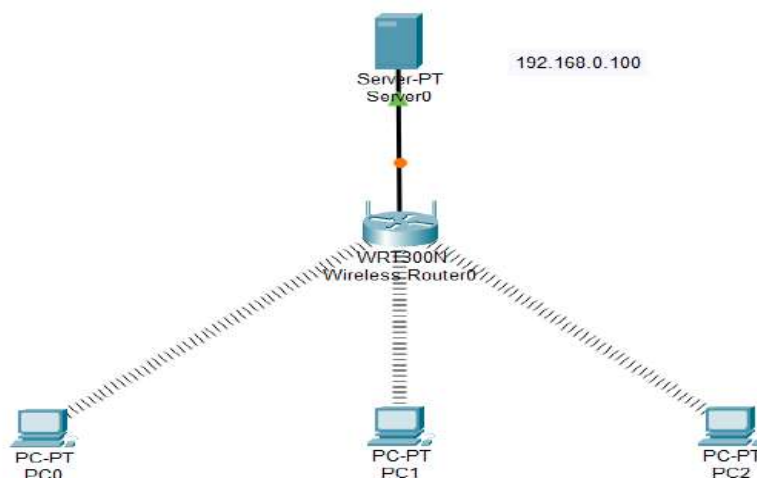
**Components:** Wireless Router, Server, PC

**Theory:** Network firewalls are security devices used to stop or mitigate unauthorized access to private networks connected to the Internet, especially intranets. The only traffic allowed on the network is defined via firewall policies – any other traffic attempting to access the network is blocked.

### Cisco Packet Tracer Setup:-

#### Implementation:

**Step 1:** Arranging devices and creating connections



**Step 2:** Configure wireless router and connect server to wireless router using Ethernet cable

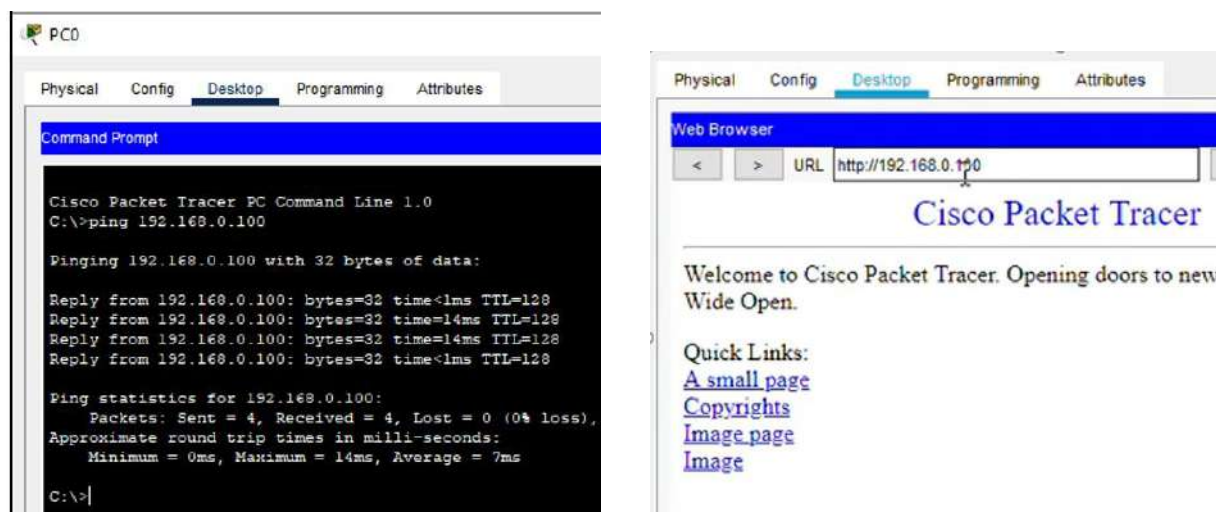
**Step 3:** Configure Server by setting IP Config in Server0 to DHCP

**Step 4:** Configure and connect all PC's to wireless router

**Step 5:** Changing port to wireless adapter of all PC's

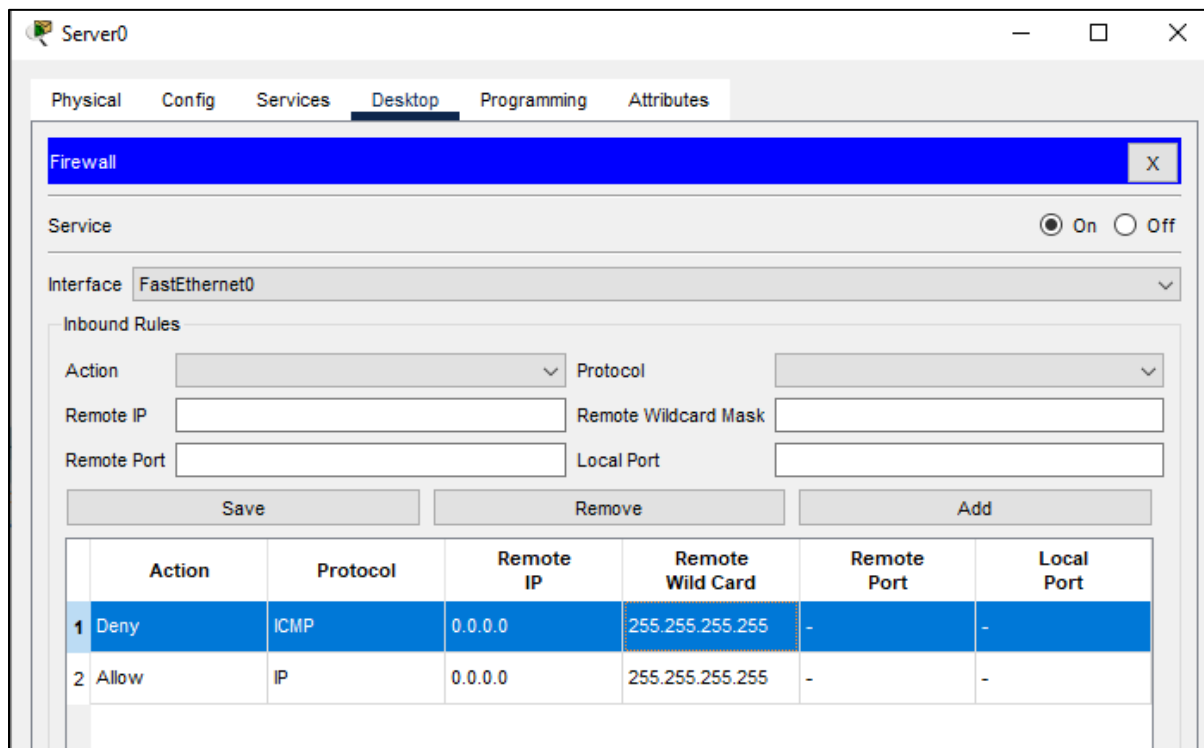
After adding wireless adapter of all PC's they will automatically get connected with wireless router because of DHCP

### Step 6: Checking connection of pc's with server



If receiving response from server our connection is done successfully

### Step 7: Configure IPv4 firewall to setup networks based firewall and add conditions



**Output:**

After the configuration is done for firewall we are unable to ping to server

```
Approximate round trip times in milli-seconds:
  Minimum = 26ms, Maximum = 41ms, Average = 32ms

C:\>ping 192.168.0.100

Pinging 192.168.0.100 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.0.100:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

But we can access the server data (view)



## Practical No: 05

**Aim:** Configuring Auto Profiles ACU Utilities

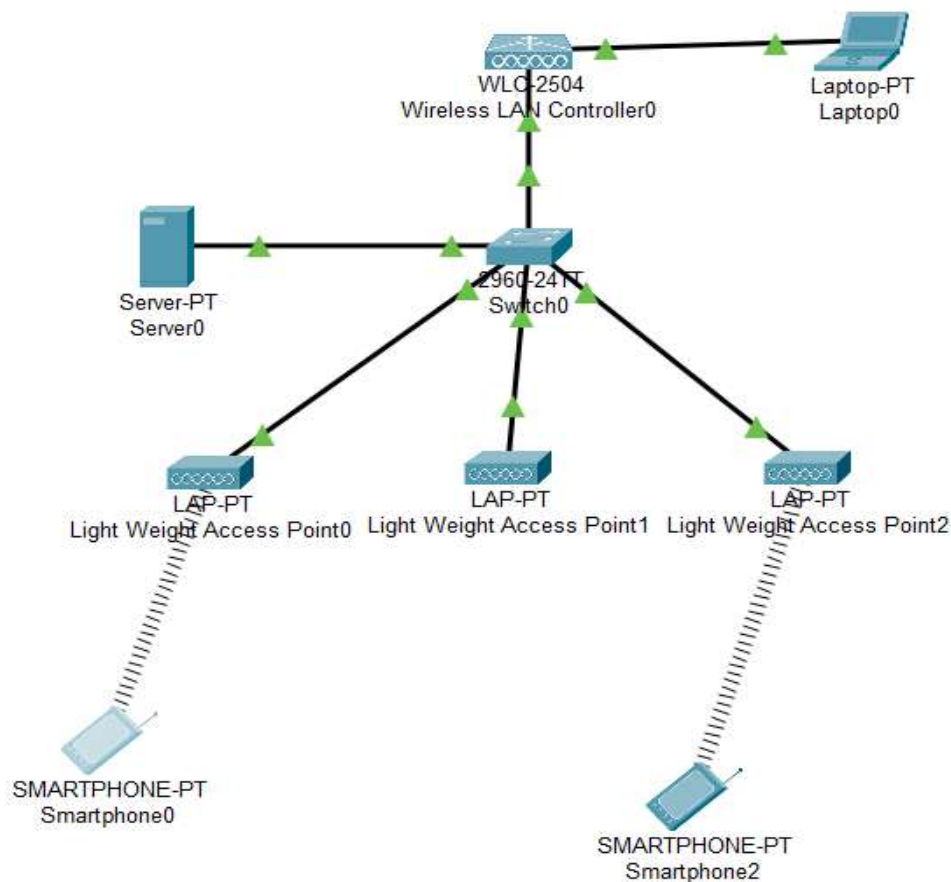
**Components:** WLC (Wireless LAN Controller), AP (Access point), Switch, Server, Laptop, Smartphone, Tablet

**Theory:** A network access control list (ACL) is made up of rules that either allow access to a computer environment or deny it. In a way, an ACL is like a guest list at an exclusive club. Only those on the list are allowed in the doors. This enables administrators to ensure that, unless the proper credentials are presented by the device, it cannot gain access.

### Cisco Packet Tracer Setup: -

#### Implementation:

#### Step 1: Arranging devices and creating connections



**Step 2: WLC (Wireless LAN Controller):**

Config > Management

IPv4 address: 10.10.10.5

Default Gateway: 10.10.10.1

DNS Server: 10.10.10.2

**Step 3: Configuring Laptop and server and checking connection:**

In Laptop IP Config,

IPv4 address: 10.10.10.10

Default Gateway: 10.10.10.1

DNS Server: 10.10.10.2

In Server0 Config > FastEthernet0,

IPv4 address: 10.10.10.3

Port Status: On

In Server0 > Services > DHCP

Interface: (FastEthernet) Service: ON

Default Gateway: 10.10.10.1

DNS Server: 10.10.10.2

Start IP Address: 10.10.10.100

Subnet Mask: 255.0.0.0

Max no. of users: 100

Click on 'Add' and then 'Save'

Check the connection from laptop0 command prompt with

C:\> ping 10.10.10.1

**Step 4: Configuring Admin settings using address (<http://10.10.10.5>) in the web browser of Laptop2:**

1. Create a new username and password and remember it for further steps
2. In the next page, (Set up your Controller)
 

System Name: GJCCS	Management IP Address: 10.10.10.5
Subnet Mask: 255.0.0.0	Default Gateway: 10.10.10.1
Management VLAN ID: 0	
3. In the Create your Wireless Networks,
 

Network name: STUDENT	Security: WPA2 Personal
-----------------------	-------------------------

Passphrase: student

4. Click Next in the Advanced Setting section and Apply in the final section

**Step 5:** Login back to Admin Panel using address (<https://10.10.10.5>) with the new Admin name and password:

Make sure the 3 Access points are present in the Wireless section,

If not, then re-plug all the access points in the physical section and hit refresh on the top right of the web browser of Laptop0

Go to WLAN make SSID for STUDENT to Student

**Step 6:** Add new wireless LAN as TEACHER with SSID Teacher and apply and make sure the status is enabled:

**Step 7:** Create AP Groups for TEACHER and STUDENT:

1. In the WLAN tab, select AP Group on the left of the page, below the Advanced section
2. Inside, enter  
 AP Group Name: STUDENT                      Description: Student AP  
 And click 'add'
3. In the WLAN section, select WLAN SSID as Student and add
4. Go to the APs section and select the first 2 access points and add them to this AP Group
5. Now Repeat above the steps for the TEACHER AP Group and in the access point selection, add the one access point that was left out

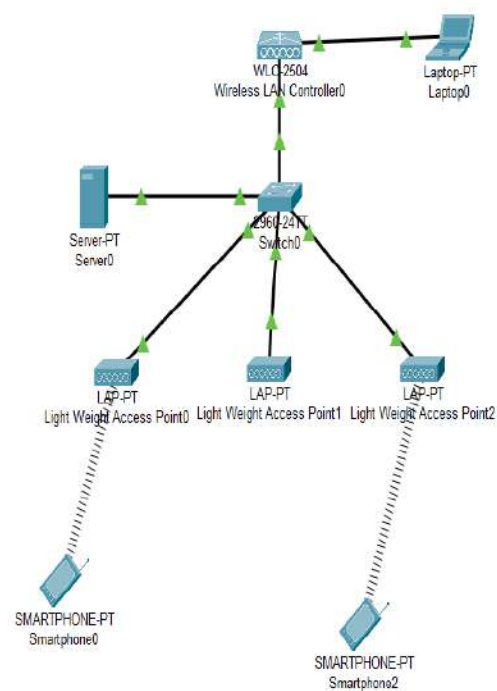
**Step 8:** Take Smartphone to connect Student AP group with wireless connection using SSID

**Step 9:** Take another smartphone to connect Teachers AP group with wireless connection using SSID

*Wait for some time (min 30sec to 1min) after that re-plug the adapters of all Access points*

**Step 10:** Send packets from one smartphone to the other

## Output:



4321

3941

3901

2911

81980X

81940Y

829

1240

PfRouter

PfEgmp

1841

26200Y

26210Y

2

Scenario 0

New

Delete

Toggle PDU List Window

Realtime

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
Successful	Smart...	Smartpho...	ICMP		0.000	N	0	(edit)	(delete)	
Successful	Smart...	Smartpho...	ICMP		0.000	N	1	(edit)	(delete)	

(Select a Device to Drag and Drop to the Workspace)

## Practical No: 06

**Aim:** Creating an Adhoc Network

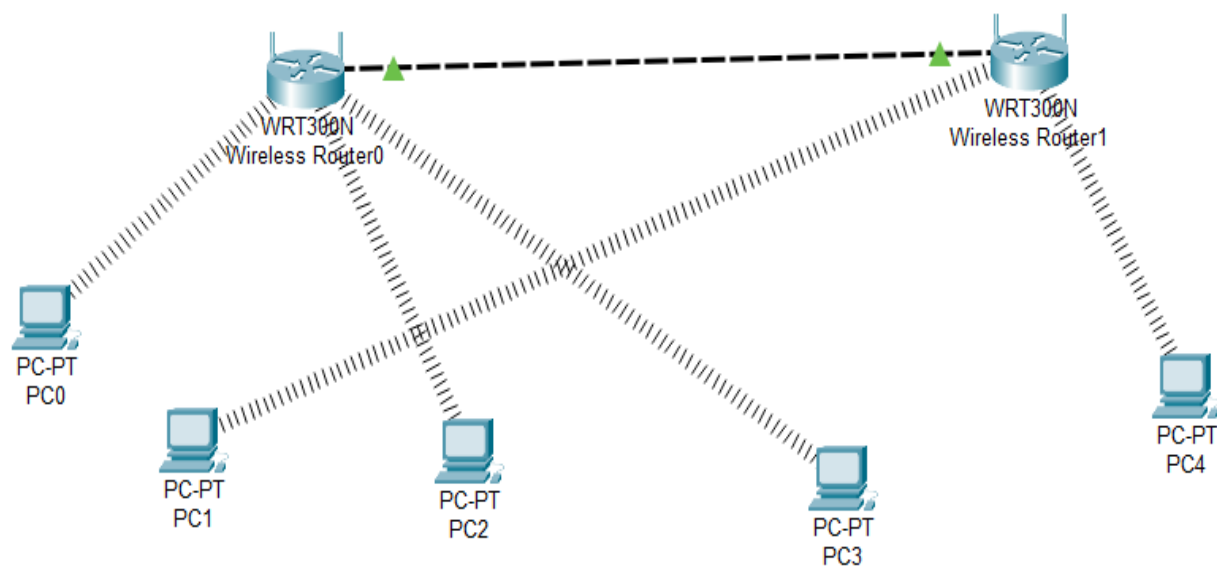
**Components:** Wireless Router, PC

**Theory:** Ad hoc networks are mostly wireless local area networks (LANs). The devices communicate with each other directly instead of relying on a base station or access points as in wireless LANs for data transfer co-ordination. Each device participates in routing activity, by determining the route using the routing algorithm and forwarding data to other devices via this route.

**Cisco Packet Tracer Setup:-**

**Implementation: -**

**Step1:** Arrange all components i.e., Wireless Router and PC's





**Step 2:** Configure wireless routers and connect both of them to each other using Ethernet ports:

In Router0, go to GUI > Wireless > basic wireless settings

Network SSID: CS and set SSID broadcast to enabled

Now, click on wireless security,

Security Mode: WPA2 Personal, Passphrase: ciscorouter1

Go to the bottom and save settings

In Router1, go to GUI > Wireless > basic wireless settings

Network SSID: IT and set SSID broadcast to enabled

Now, click on wireless security,

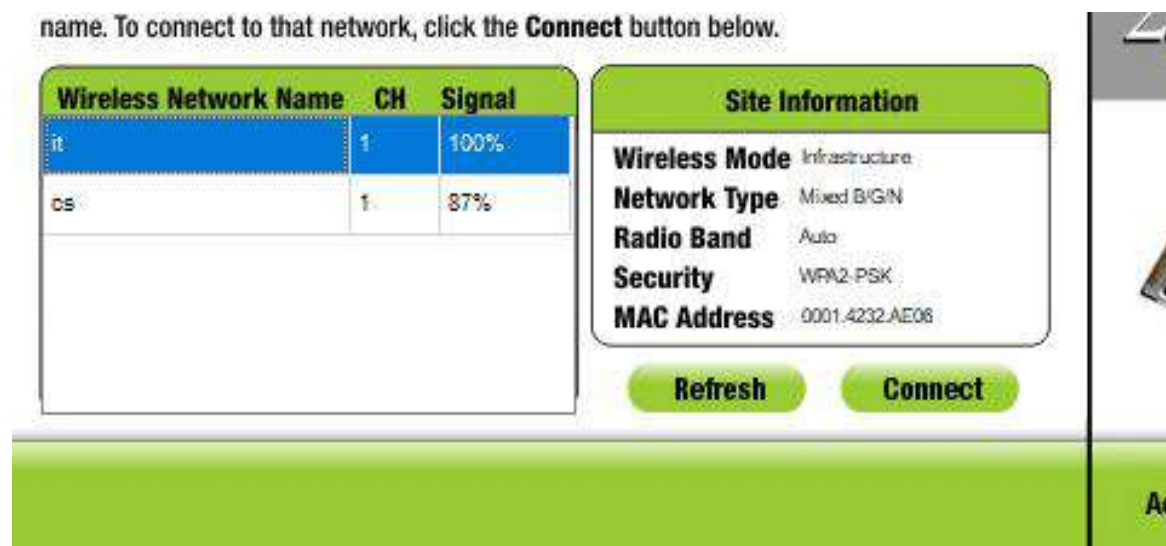
Security Mode: WPA Personal, Passphrase: ciscorouter2

**Step 3:** Connect all machines/devices (PC's) to respective router as per our requirements.

Change the Port of all pc's with wireless adapter

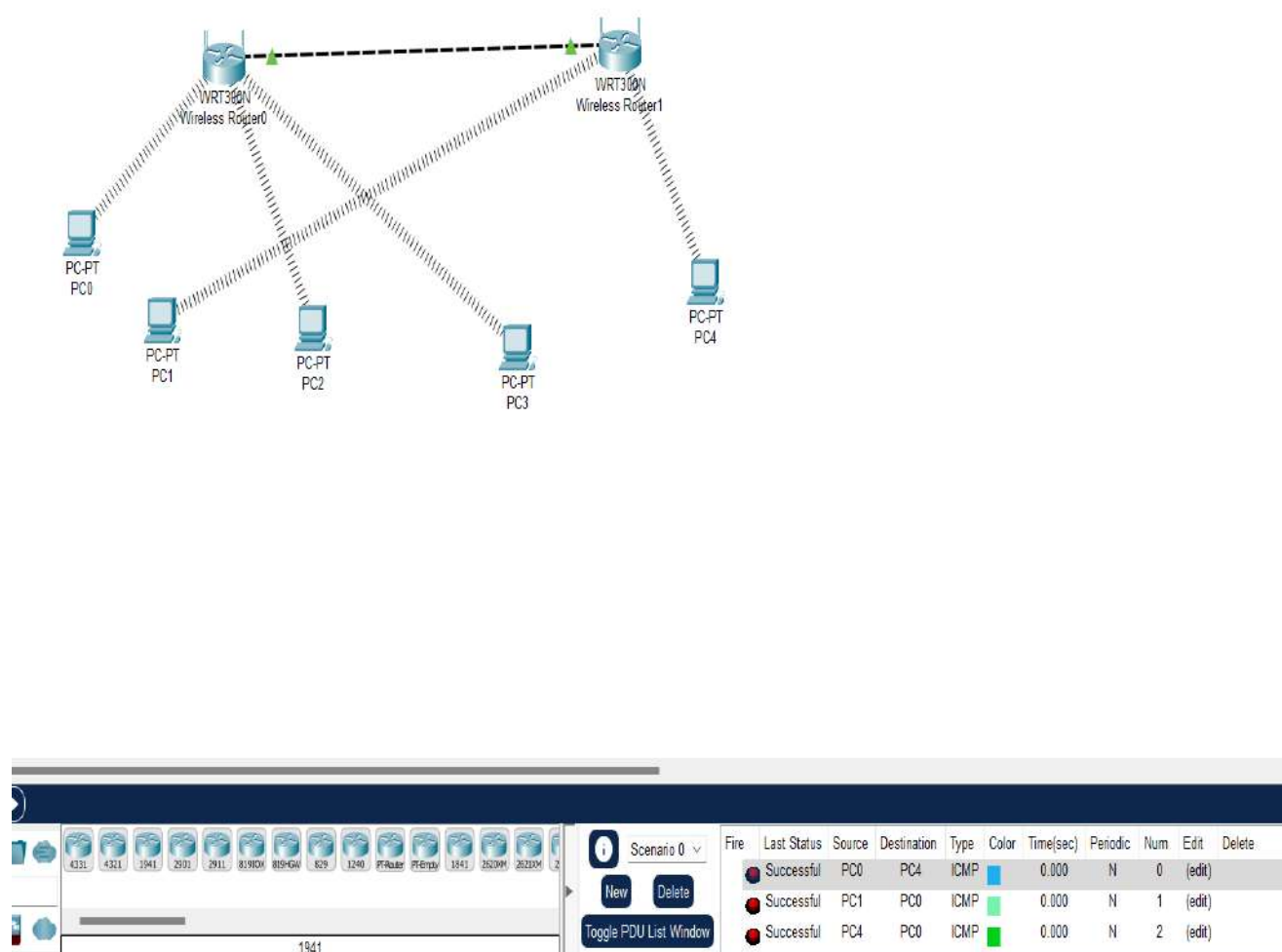
Configure Wireless connection: Click on PC0 > Desktop > PC Wireless

Click on Connect tab > click on refresh > Select CS/IT > Enter Password and connect



Do similar configuration to all respective PC's

**Output:**



## Practical No: 07

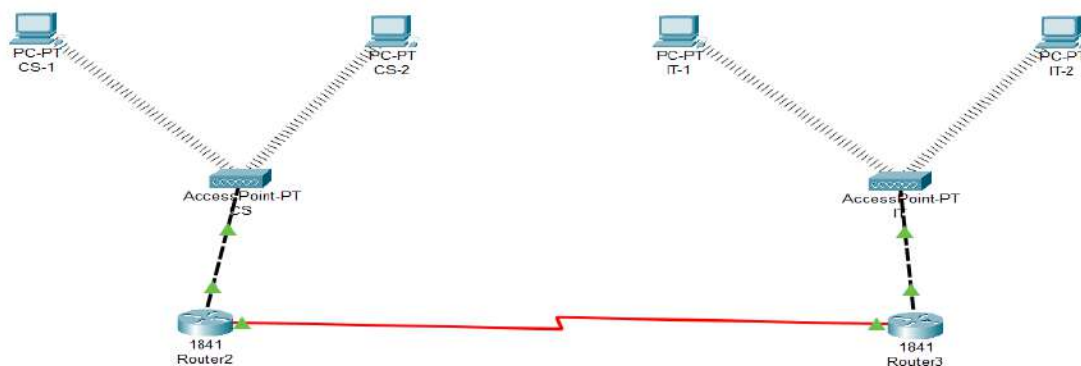
**Aim:** Configuring Basic AP Settings

**Components:** Router, Access points, PC's

**Theory:** A wireless access point (WAP), or more generally just access point (AP), is a networking hardware device that allows other Wi-Fi devices to connect to a wired network. An access point is a device that creates a wireless local area network, or WLAN, usually in an office or large building.

**Cisco Packet tracer Setup:**

**Step 1:** Arrange all devices as following



**Step 2:** Configure Access Points (A)

In Access point CS

Port 0, set

Port Status: on, Bandwidth: 100 Mbps, Duplex: Half Duplex

Port 1, set

SSID: CS, select WPA2-PSK and password to ciscopacket1

In Access point IT

Port 0, set

Port Status: on, Bandwidth: 100 Mbps, Duplex: Half Duplex

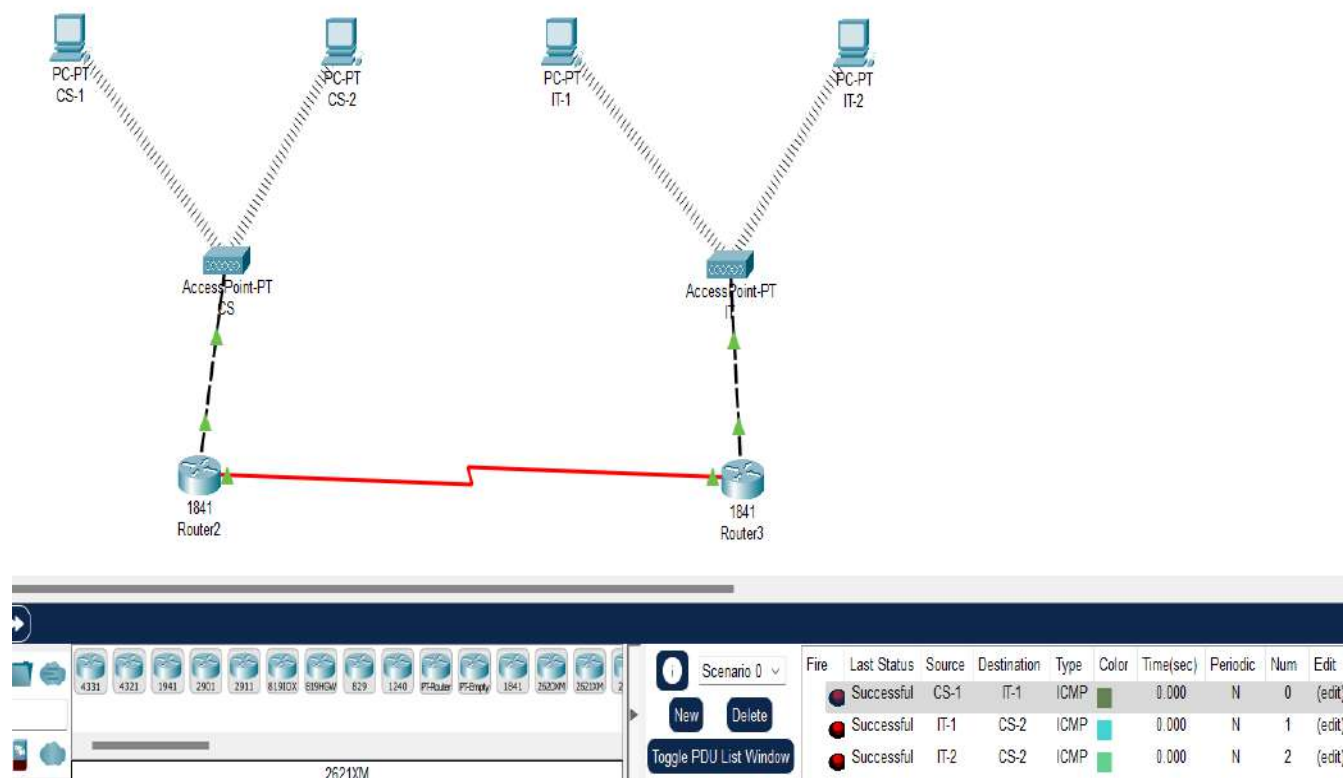
Port 1, set

SSID: IT, select WPA2-PSK and password to ciscopacket2

### Step 3: Configure and Setup IP Address for all devices (PC's)

Device	Interface	IPv4 address	Other
CS-1	IP config	192.168.1.3	Default Gateway: 192.168.1.1
CS-2	IP config	192.168.1.4	Default Gateway: 192.168.1.1
IT-1	IP config	171.16.10.2	Default Gateway: 171.16.10.1
IT-2	IP config	171.16.10.3	Default Gateway: 171.16.10.1
CS-1 and CS-2	Wireless0		SSID: CS WPA2-PSK password: ciscopacket1
IT-1 and IT-2	Wireless0		SSID: IT WPA2-PSK password: ciscopacket2
Router2	F0/0	192.168.1.1	
	S0/0/0	20.0.0.1	
	RIP v2	20.0.0.0 192.168.1.0	
Router3	F0/0	171.16.10.1	
	S0/0/0	20.0.0.2	
	RIP v2	20.0.0.0 171.16.10.0	

Note: Change all port adapters with wireless adapter for all PC's

**Output:**

## Practical No: 08

**Aim:** Configure fast Ethernet on router using packet tracer

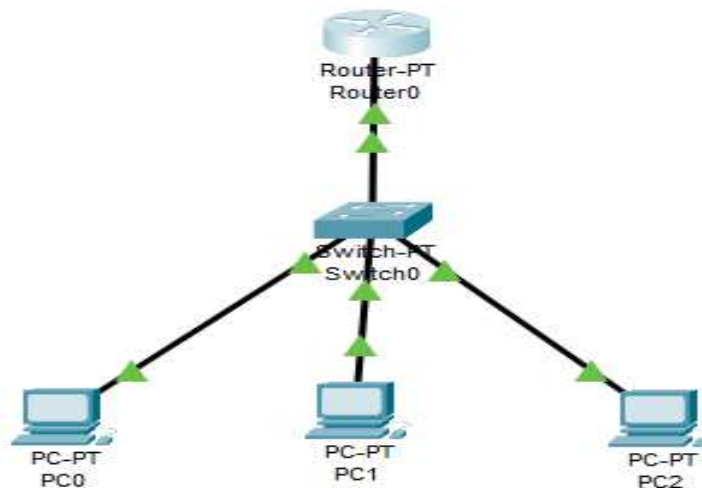
**Components:** Router, Switches, PC's

**Theory:** Fast Ethernet is used for departmental backbones, connections to high-speed servers, and connections to workstations running bandwidth-intensive software such as CAD or multimedia applications.

### Cisco Packet tracer Setup:

#### Implementation:

**Step 1:** Arrange all devices as shown below:



**Step 2:** Configure Router using CLI, using following commands:

```
configure t
hostname R1
enable password cisco
interface fa0/0
ip address 192.168.2.1 255.255.255.0
no shutdown
exit
Exit
```

```
R1(config)#enable password cisco
```

```

R1>enable
Password:
R1#R1#R1#
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#interface FastEthernet0/0
R1(config-if)#ip address 192.168.2.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#exit
R1#

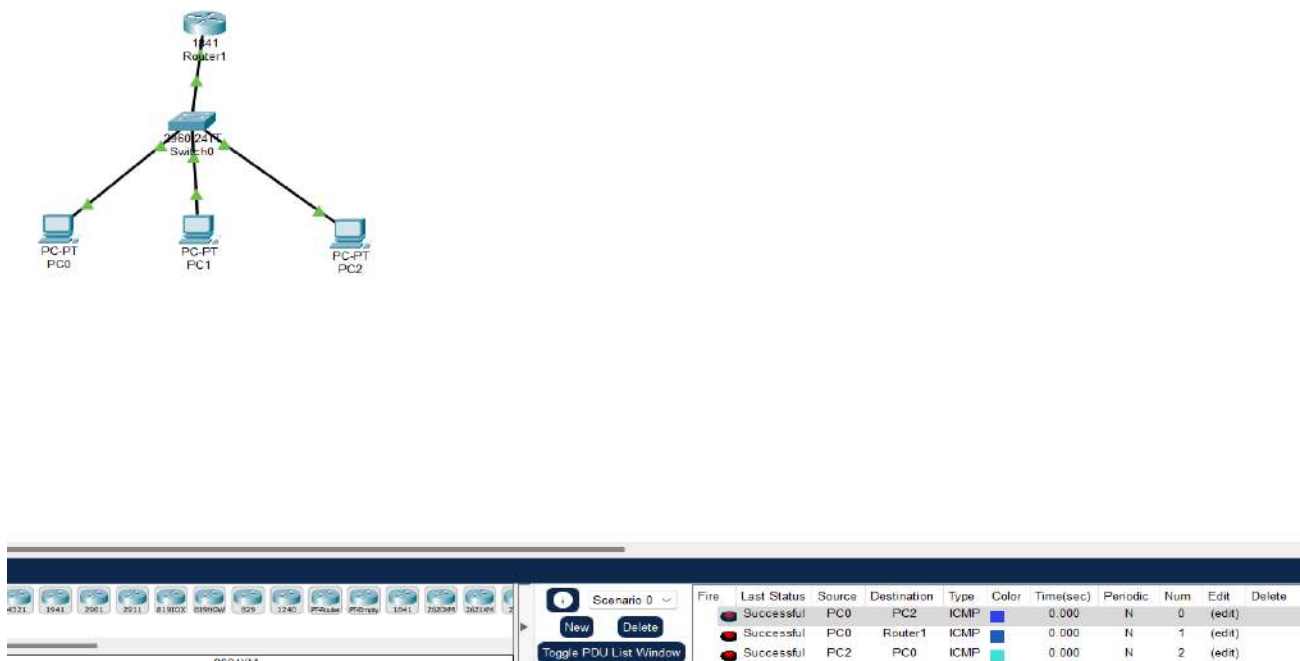
```

**Step 3:** Configure All PC's and check the connection.

Device	Interface	IPv4 address	Other
PC0	IP config	192.168.2.2	Default Gateway: 192.168.2.1
PC1	IP config	192.168.2.3	Default Gateway: 192.168.2.1
PC2	IP config	192.168.2.4	Default Gateway: 192.168.2.1

**Step 4:** Ping 192.168.2.1 with all the PCs.

**Output:**



## Practical No: 09

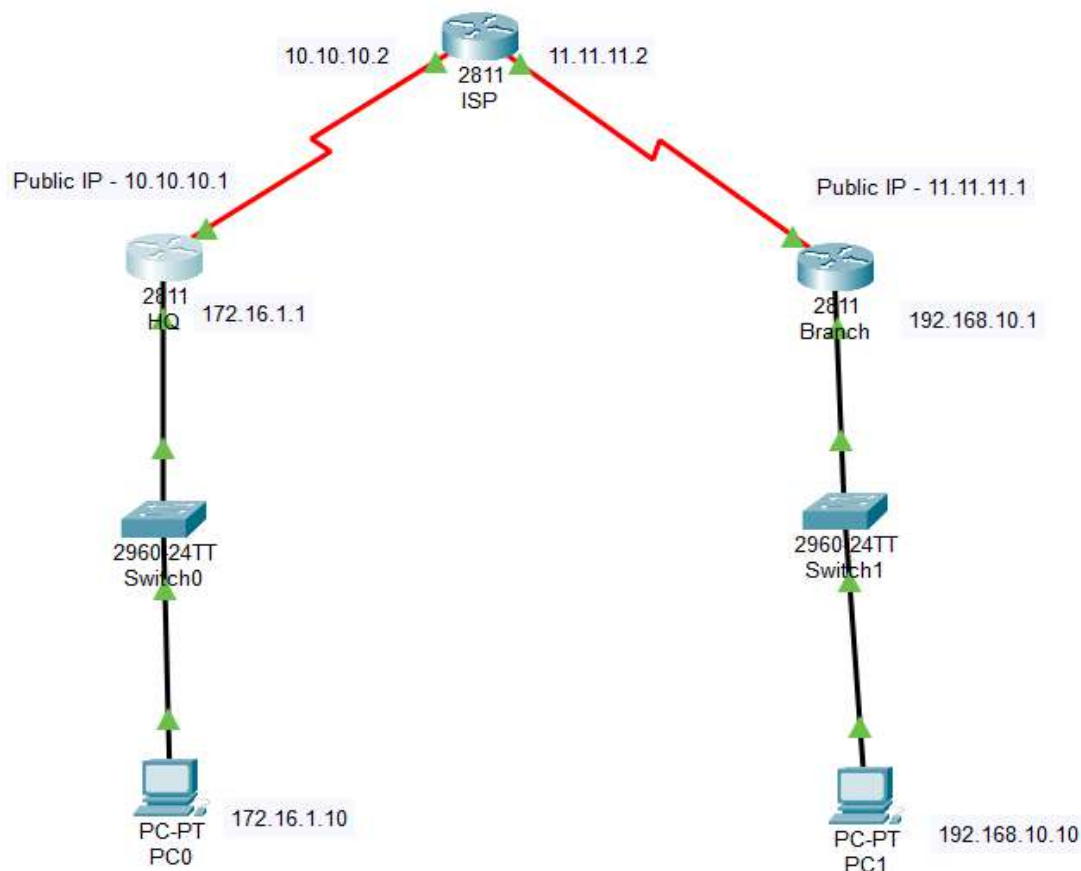
**Aim:** Configure Site-to-Site Wireless Link

**Components:** Routers, Switch, PC

**Theory:** A site-to-site VPN connects users in different locations within an entire network. Through this network, the users can exchange data from their own locations while that information is encrypted and secured through the VPN. Users working in separate offices can still be connected to one another and all of their internal resources. This keeps all users connected even when they are working remotely while securing the information exchanged between them.

**Cisco Packet tracer Setup:**

**Step 1:** Connect all devices and assign IP addresses as shown below





**Step 2:** Set IP route as shown below in the ISP router

```
ISP(config-if)#exit
ISP(config)#ip route
ISP(config)#ip route 172.16.1.0 255.255.255.0 10.10.10.1
ISP(config)#ip route 192.168.10.0 255.255.255.0 11.11.11.1
% Invalid input detected at '^' marker.
ISP(config)#ip route 192.168.10.0 255.255.255.0 11.11.11.1
ISP(config)#
ISP(config)#
```

Copy Paste

**Step 3:** Try pinging from PC0 or PC1 to check the connection.

In Desktop, Command prompt

C:\> ping 192.168.10.10

**Step 4:** Configure isakmp policy and define IPsec transform set by entering the commands given below in the HQ router

1-Configure ISAKMP policy to establish the IKE(Internet Key Exchange) tunnel

```
HQ(config)#crypto isakmp enable

HQ(config)# crypto isakmp policy 20
HQ(config-isakmp)#authentication pre-share
HQ(config-isakmp)#encryption 3des
HQ(config-isakmp)#hash md5
HQ(config-isakmp)#group 1
HQ(config-isakmp)#lifetime 3600
HQ(config-isakmp)#exit

HQ(config)#crypto isakmp key cisco123 address 11.11.11.1
```

2-Define IPsec Transform Set

```
HQ(config)#crypto ipsec transform-set myset esp-3des esp-md5-hmac
```

**Step 5:** Create access list and crypto map in the HQ router CLI

### 3-Create Accesslist

```
R1(config)# access-list 100 permit ip 172.16.1.0 0.0.0.255 192
4-Crete Crypto map for IPsec
```

```
HQ(config)#crypto map mymap 20 ipsec-isakmp
HQ(config-crypto-map)#set peer 11.11.11.1
HQ(config-crypto-map)#set transform-set myset
HQ(config-crypto-map)# match address 100
HQ(config-crypto-map)# exit
```

### 5-Apply the crypto map to the outgoing interface of the VPN device

```
HQ(config)#int s0/0/0
HQ(config)#crypto map mymap
```

**Step 6:** Perform the above 2 steps for the Branch router and change the IP addresses accordingly

### Output:

Verify the created isakmp policies with the following command

The screenshot shows the HQ router's CLI interface with the following output:

```

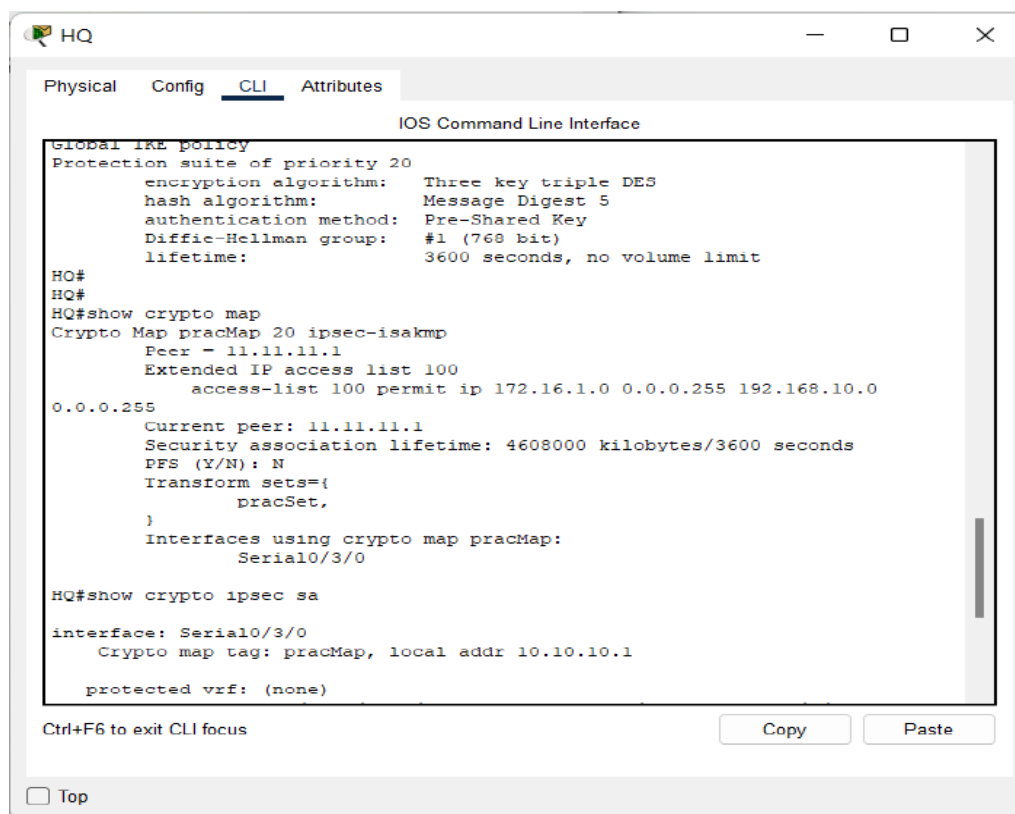
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed
state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/3/0, changed state to
up

HQ>enable
HQ#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst          src          state          conn-id slot status
11.11.11.1   10.10.10.1   QM_IDLE        1023      0  ACTIVE

IPv6 Crypto ISAKMP SA

HQ#show crypto isakmp policy
Global IKE policy
Protection suite of priority 20
  encryption algorithm: Three key triple DES
  hash algorithm:       Message Digest 5
  authentication method: Pre-Shared Key
  Diffie-Hellman group:  #1 (768 bit)
  lifetime:              3600 seconds, no volume limit
HQ#
HQ#
HQ#
  
```

At the bottom of the window, there are buttons for "Copy" and "Paste", and a "Top" link.



Global IKE policy  
Protection suite of priority 20  
  encryption algorithm: Three key triple DES  
  hash algorithm: Message Digest 5  
  authentication method: Pre-Shared Key  
  Diffie-Hellman group: #1 (768 bit)  
  lifetime: 3600 seconds, no volume limit

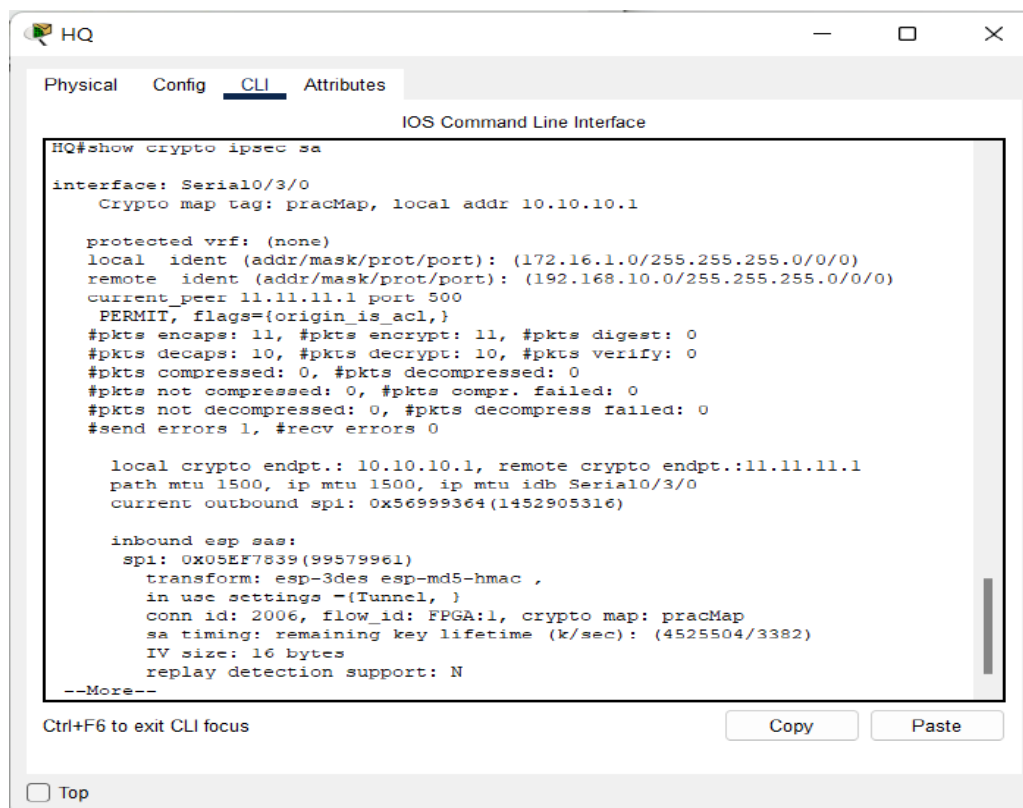
HQ#  
HQ#  
HQ#show crypto map  
Crypto Map pracMap 20 ipsec-isakmp  
  Peer = 11.11.11.1  
  Extended IP access list 100  
    access-list 100 permit ip 172.16.1.0 0.0.0.255 192.168.10.0 0.0.0.255  
    Current peer: 11.11.11.1  
    Security association lifetime: 4608000 kilobytes/3600 seconds  
    PFS (Y/N): N  
    Transform sets={  
      pracSet,  
    }  
  Interfaces using crypto map pracMap:  
    Serial0/3/0

HQ#show crypto ipsec sa  
interface: Serial0/3/0  
  Crypto map tag: pracMap, local addr 10.10.10.1  
  protected vrf: (none)

Ctrl+F6 to exit CLI focus

Copy Paste

☐ Top



HQ#show crypto ipsec sa  
interface: Serial0/3/0  
  Crypto map tag: pracMap, local addr 10.10.10.1  
  protected vrf: (none)  
  local ident (addr/mask/prot/port): (172.16.1.0/255.255.255.0/0/0)  
  remote ident (addr/mask/prot/port): (192.168.10.0/255.255.255.0/0/0)  
  current\_peer 11.11.11.1 port 500  
    PERMIT, flags={origin\_is\_acl,}  
  #pkts encaps: 11, #pkts encrypt: 11, #pkts digest: 0  
  #pkts decaps: 10, #pkts decrypt: 10, #pkts verify: 0  
  #pkts compressed: 0, #pkts decompressed: 0  
  #pkts not compressed: 0, #pkts compr. failed: 0  
  #pkts not decompressed: 0, #pkts decompress failed: 0  
  #send errors 1, #rcv errors 0  
  
  local crypto endpt.: 10.10.10.1, remote crypto endpt.: 11.11.11.1  
  path mtu 1500, ip mtu 1500, ip mtu idb Serial0/3/0  
  current outbound spi: 0x56999364(1452905316)  
  
  inbound esp sas:  
    spi: 0x05EF7839(99579961)  
    transform: esp-3des esp-md5-hmac ,  
    in use settings -(Tunnel, )  
    conn id: 2006, flow\_id: FPGA:1, crypto map: pracMap  
    sa timing: remaining key lifetime (k/sec): (4525504/3382)  
    IV size: 16 bytes  
    replay detection support: N  
  --More--

Ctrl+F6 to exit CLI focus

Copy Paste

☐ Top