**CCNA - CISCO CERTIFIED NETWORK ASSOCIATE**

**PROMPT INFOTECH**

| **S.No** | **TOPICS** | **Pg.No** |
| --- | --- | --- |
| **1.** | **OSI LAYERS** | **3** |
| **2.** | **NETWORKING PROTOCOLS** | **4** |
| **3.** | **IP ADDRESS** | **6** |
| **4.** | **SUBNETTING** | **12** |
| **5.** | **ROUTER** | **16** |
| **6.** | **ROUTING** | **19** |
| **7.** | **SWITCH-SWITCHING** | **23** |
| **8.** | **VLAN** | **25** |
| **9.** | **PORT SECURITY** | **27** |
| **10.** | **ACL** | **29** |
| **11.** | **BGP** | **32** |
| **12.** | **NAT** | **33** |
| **13.** | **PAT** | **34** |
| **14.** | **FTP** | **37** |
| **15.** | **SMTP** | **39** |
| **16.** | **SSH** | **41** |
| **17.** | **SNMP** | **44** |
| **18.** | **FIREWALL** | **46** |
| **19.** | **DNS & DHCP** | **50** |

| **20.** | **DNS RECORDS** | **52** |
| --- | --- | --- |
| **21.** | **DNS QUERIES** | **55** |
| **22.** | **REVERSE DNS** | **57** |
| **23.** | **CIDR** | **58** |

**OSI LAYERS**

- Open System Interconnect

**Explains :**

How data is transferred from source to destination and how data gets

converted into a different format before reaching the destination.

**Function :**

It is a universal standard which all manufacturers should follow in order to

connect with the internet.

OSI - 7 layer and each layer has a device placed

| LAYERS | DEVICES | ENCAPSULATED DATA | FUNCTIONS |
| --- | --- | --- | --- |
| APPLICATION | COMPUTER | DATA | IN BUILT SYSTEM APP OR 3RD PARTY APPLICATION |
| PRESENTATION | COMPUTER | DATA | ENCRYPTION AND DECRYPTION |
| SESSION | COMPUTER | DATA | AUTHENTICATION, AUTHORISATION |
| TRANSPORT | CABLES | SEGMENTS | SEGMENTATION,  FLOW CONTROL, ERROR CONTROL |
| NETWORK | ROUTER | PACKETS | IP ADDRESSING,PATH DETERMINATION |
| DATA LINK | SWITCH | FRAMES | MAC ADDRESSING, MULTIPLEXING |
| PHYSICAL | NIC OR HUB | BITS (0’S AND 1’S) | CONVERTING TO 0’S AND 1’S |

**NETWORKING PROTOCOLS**

Protocols - set of rules for two computers to communicate with each other.

**1. TCP/IP**

**2. UDP**

**3. DNS**

**4. DHCP**

TCP/IP - TRANSMISSION CONTROL PROTOCOL / INTERNET PROTOCOL

UDP - USER DATAGRAM PROTOCOL

Normally, computer communication happens in packets. All these packets are like

courier packets with a from and to address.

These two protocols are responsible for two computer to communicate with each

other.

| **TCP** | **UDP** |
| --- | --- |
| Will always check if the recipient is  available or not. | Will not check |
| Will always expect an acknowledgement  from the recipient | Will not expect |
| Will be slow | Will be fast |
| No data loss | Data loss will occur |
| It is called heavy weighted protocol | It is called lightweight protocol |
| Ex : normal browser communication | Ex: Whatsapp, voip calls |

**TCP FLAGS**

RST - RESET

ACK - ACKNOWLEDGE

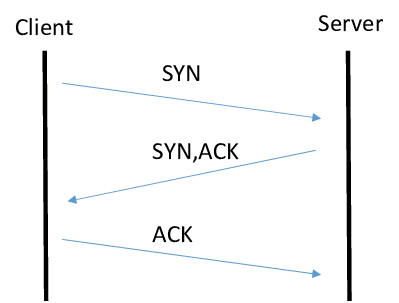
SYN - SYNCHRONIZE

FIN - FINISH

URG - URGENT

PSH - PUSH

**TCP 3 WAY HANDSHAKE:**



**TCP PORTS**

Every protocol will have a port number assigned to it.

Range = 0 - 65535

HTTP : 80

**PORT NUMBERS WILL HAVE A PORT STATUS - OPEN OR CLOSED**

In case the port is open, it will allow traffic. If not it will not allow traffic.

**TCP HEADER**

Source Port no

Destination Port No

SEQ NO

ACK NO

FLAG STATUS - RST | FIN | URG

Data

**TODO 1**

**COLLECT A LIST OF COMMONLY USED PROTOCOL WITH PORT NUMBERS** **(30)**

**EG: HTTP - 80**

**FTP - 20**

**IP ADDRESS - IPV4:**

**IP - INTERNET PROTOCOL**

**CONTENTS:**

1. IP RANGE

2. DECIMAL TO BINARY CONVERSIONS

3. WHY IP IS 32 BIT

4. WHY RANGE IS 2555. CLASSES OF IP

6. SUBNET MASK

7. NID & BID

8. PRIVATE IP RANGE

9. DEFAULT SUBNET MASK

10.CALCULATION OF NO OF N/W AND HOST PORTIONS

**IP RANGE**

IP Range is from 0 to 255

An IP looks something like 192.168.1.23

IP range starts from

0.0.0.0

0.0.0.1

0.0.0.2

……

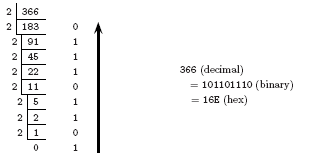
……

……

255.255.255.255

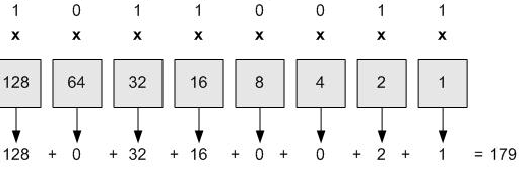
**DECIMAL TO BINARY CONVERSIONS**

366 is a decimal number which has to be converted to binary.



**BINARY TO DECIMAL CONVERSION**

10110011 is the binary number which has to be converted into decimal



**WHY IP IS 32 BIT?**

0.0.0.0

00000000.00000000.00000000.00000000

……

……

……

255.255.255.255

-

11111111.11111111.11111111.11111111

8 BITS

8 BITS = 32 BITS

8 BITS = 1 OCTET, TOTAL 4 OCTETS WHICH IS 32 BITS. THIS IS WHY IP IS 32

BITS.

**WHY IP RANGE IS 255?**

Can we extend the range to 455, 855, 955

The maximum IP address which we can obtain using IPV4 is 4.2 billion

0.0.0.0

0,0,0,1

0.0.0.2

……

……

……

4.2 billion ip

Calculation - 2 power n

When 2 power 8 = 256

00000000

00000001

00000010

00000100

……

……

……

We take from 0 so range is 0-255

**CLASSES OF IP**

**CLASS** **RANGE**

A 0 - 127

B 128 - 191

C 192 - 223

D 224 - 239 MILITARY & RESERVED PURPOSE

E 240 -254 Reserved for Future uses and also R&D Process

CLASS A

0.0.0.0

0.0.0.1

……

127.255.255.255

CLASS B

128.0.0.0

128.0.0.1

…….

…….

191.255.255.255

CLASS C

192.0.0.0

192.0.0.1.

……

……

223.255.255.255

Ex :

100.0.0.1 - A

132.10.0.2 - B

192.168.1.3 - C

**SUBNET MASK**

**CLASS A** Larger MNC **N.H.H.H**

**CLASS B** Mid-level comp **N.N.H.H**

**CLASS C** Small Comp & Home Users **N.N.N.H**

**Network and Host portion**

**\_ . \_ . \_ .\_**

Network portion means / related to network **N**

Host refers to computers **H**

**DEFAULT SUBNET MASK**

We have to assign the following

N = 255

H = 0

To get the default subnet mask for each class

**CLASS A N.H.H.H 255.0.0.0**

**CLASS B N.N.H.H 255.255.0.0**

**CLASS C N.N.N.H 255.255.255.0**

**NID, DG & BID :**

**Network ID**

Its like your department name

Ex: Computer Science Department - It represents all the students studying in that

Department. It's the collective representation of all computers in your network or LAN - usually in IP

To find NID

1. Find class

2. Get number of network and host portions

3. Make the host portions zero.

192.168.1.10

Class - C

SM - N.N.N.H

NID - 192.168.1.0 **FIRST IP ADDRESS**

DG - 192.168.1.1 **SECOND IP ADDRESS**

BID - 192.168.1.255 **LAST IP ADDRESS**

100.10.10.5

Class - A

SM - N.H.H.H

NID - 100.0.0.0

DG - 100.0.0.1

BID - 100.255.255.255

128.15.10.10

Class - B

SM - N.N.H.H

NID - 128.15.0.0

DG - 128.15.0.1

BID - 128.15.255.255

**Broadcast ID**

When we need to send a single message to all the computers in our LAN. Then ill use

broadcast ID

EX: 192.168.1.10 is my computer IP, then we can identify the following

192.168.1.0 - the first IP will be my NID

192.168.1.1 - the second IP will be my Default gateway IP / Modem IP / Router IP

192.168.1.255

- the last IP will be my BID

**IMPORTANT**

We cannot use/assign the above 3 IP addresses to any computer.

**PRIVATE IP ADDRESS vs PUBLIC IP ADDRESS:**

Is the IP address unique? ?

**Private IP**

Used only inside a LAN

When this IP goes out of LAN, it becomes invalid and it changes to public IP

Ex: India being our LAN, We use INR only inside INdia, when go abroad, we convert

INR to USD.

We can view, edit, change

It is assigned by user or admin

**Public IP**

Used only outside a LAN

When this IP comes inside LAN, it becomes invalid and it changes to private IP

Ex: India being our LAN, We use INR only inside India, when go abroad, we convert

INR to USD.

We can view but cannot edit, change

It is assigned by ISP (internet service provider)

**CLASS Public IP Range Private IP**

A 0.0.0.0 - 127.255.255.255 10.0.0.0 - 10.255.255.255

B 128.0.0.0 - 191.255.255.255 172.16.0.0 - 172.31.255.255

C 192.0.0.0 - 223.255.255.255 192.168.0.0- 192.168.255.255

Public IP is unique everywhere.

Private IP is unique inside a LAN but not between LAN.

**CALCULATION OF NUMBER OF NETWORK AND HOST FOR EACH**

**CLASS**

EX: CLASS A uses more computers. - How Much?

CLASS priority bit (p)

A N.H.H.H 1

B N.N.H.H 2

C N,N,N,H 3

To find no of n/w = 2 power n-p

To find no of hosts = 2 power h and -2

**CLASS A**

No of n/w = 2 power 8-1 = 127 n/w

No f host = 2 power 24 and -2 = 16777216 hosts

B Network 16384 Host 65536

C Network 2097152 Host 256

No of host = 2 power 8 and -2 = 254 hosts

**SUBNETTING**

1. IMPORTANCE OF SUBNET MASK

2. USES OF SUBNETTING

3. HOW SUBNETTING WORKS

4. SCENARIO 1, 2, 3

**IMPORTANCE OF SUBNET MASK**

192.168.1.2 - our computer

CLASS C

NID : 192.168.1.0 - A

DG : 192.168.1.1

PING - PACKET INTERNET GROPER

We are trying to ping another ip from our computer

PING 192.168.1.3

SWITCH - PERFORMS BOOLEAN AND ’ING OPERATION .

DEST IP

192.168.1.3

11000000.10100000.00000001.00000011

SUB MASK

255.255.255.0

11111111.11111111.11111111.00000000

BOOLEAN AND

11000000.10100000.00000001.00000000

RESULT

192.168.1.0 - BA=B, SWITCH DECIDES THAT PACKET BELONGS INSIDE LAN AND WILL NOT SEND

IT TO ROUTER

A NOT EQUAL TO B, SWITCH DECIDES PACKET BELONGS TO ANOTHER LAN, SO IT

WILL FORWARD IT TO THE ROUTER.

**USES OF SUBNETTING:**

- TO MINIMIZE COST

- TO MINIMIZE IP WASTAGE

COMPANY - SALES, HR, DEVELOPERS, SUPPORT - 100, 200, 300, 400

HOME - DESKTOP,LAPTOP - 2 COMPUTER.

CLASS C = 254 -2 = 252 HOSTS WASTED.

THIS CAN BE PREVENTED BY SUBNETTING.

EX : 255.255.255.0 - 11111111.11111111.11111111.000000**00** - 2 COMPUTERS

111111 - CONVERTING TO N/W

11111111.11111111.11111111.11111100

255.255.255.248 - CUSTOM SUBNET MASK(CSM)

**HOW SUBNETTING WORKS?**

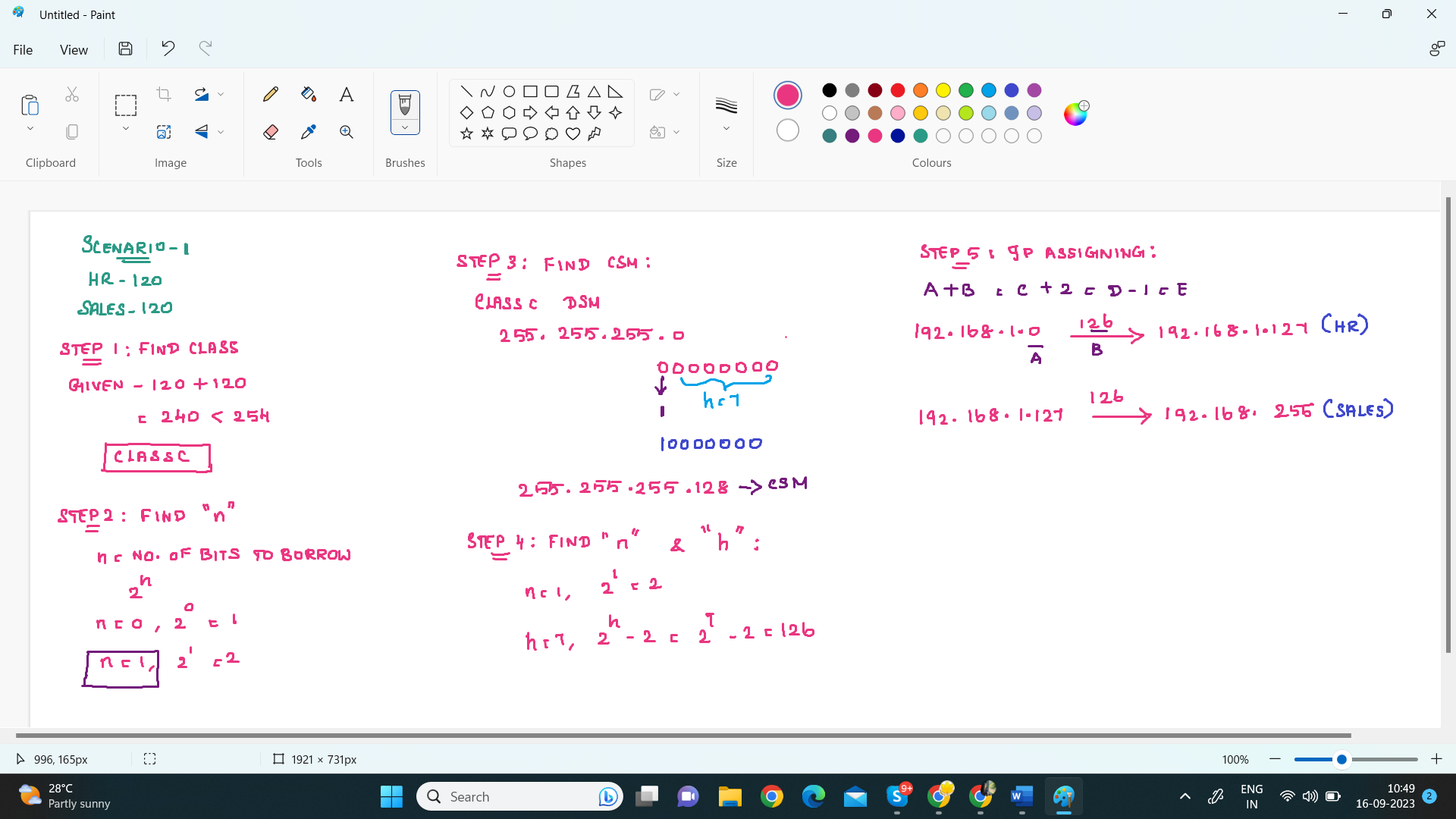
IT IS THE PROCESS OF CALCULATING WASTED HOST BITS AND

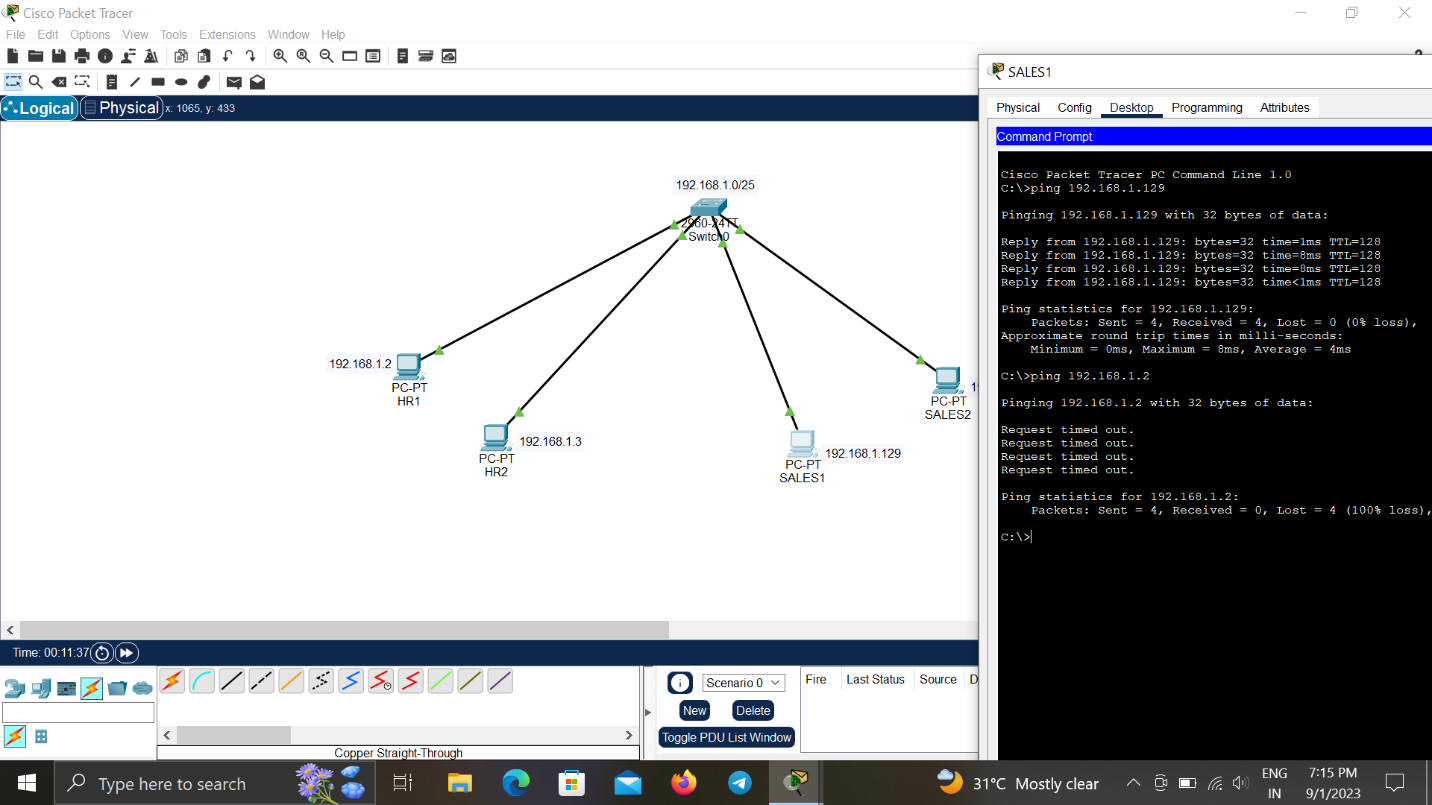
CONVERTING THE WASTED HOST BIT TO NETWORK BITS.

**SCENARIO 1**

SALES - 120

HR - 120



****

**VERIFY:**

PING HR -SALES-YOU WILL NOT GET ANY REPLY

PING HR-HR- YOU WILL GET REPLY

**TODO:**

**SCENARIO 2**

LAB 1 - 30

LAB 2 - 30

LAB 3 - 30

LAB 4 - 30

LAB 5 - 30

SCENARIO 1 & 2

- SAME COMPANY

- SAME NO OF HOSTS

WE FOUND ‘n’ - NO OF N/W TO BE BORROWED

**SCENARIO 3**

- Different company

- Different no of hosts

- We need to find ‘h’

SBI - 120

HDFC - 30

ICICI - 60

HSBC - 30

**Soln:**

SBI - 120

FIND CLASS

FIND ‘h’

2 power h and -2 >= Req no of host

FIND CSM

CALC NO OF N/W AND HOST

You will or you should get 2 networks and 126 hosts each

IP ASSIGNING

ICICI - 60

FIND CLASS

FIND ‘h’

FIND CSM

You will not take the default subnet mask, you will take the previous custom subnet

mask and use the host bits and convert the remaining to network bits.

CALC NO OF N/W AND HOST

You will or you should get 2 networks and 62/60 hosts each

IP ASSIGNING

HSBC - 30

FIND CLASS

FIND ‘h’

FIND CSM

You will not take the default subnet mask, you will take the previous custom subnet

mask and use the host bits and convert the remaining to network bits.

CALC NO OF N/W AND HOST

You will get 2 networks with 30 hosts each. You will use one 30 host for HSBC and

other 30 host for hdfc

IP ASSIGNING

**ROUTER**

A. INTRODUCTION

B. ROUTER PORTS

C. ROUTER RULES

D. ROUTER MODES

E. ROUTER BASIC CONFIGURATION

**INTRODUCTION**

THE MAIN FUNCTION OF A ROUTER IS TO FIND THE BEST PATH.WHAT DIFFERENCE DOES IT MAKE TO HAVE A ROUTER?

Bandwidth utilization - We use router to use maximum of our bandwidth without

any loss. If our internet speed is 10 mbps, we can use the maximum of that with

router, and in case if we use a modem we will have loss.

In case if we don’t have a router, our ISP will take care of routing needs.

**ROUTER PORTS**

**INTERFACE** - used to connect a router with other devices (router, Switch)

Ex:

-Ethernet interface

- Old and Slow

- Et

-Fast ethernet interface

- Fast and new

- Fe

-Gigabit ethernet interface

- Very fast and advanced - Ge

All the above 3 will look the same. (RJ45 port), but differs in speed -

-Serial Interface

Used to connect two routers.

**LINE** - used to configure a router

Types of line

- Console port (CON)

used for direct configuration

- Auxiliary port (AUX)

used for remote configuration

**C. ROUTER RULES**

Rule 1 - All interfaces of a router should be in different network | should have

different NID

Rule 2 - A serial interface connecting two routers should be in same network |

should have the same NID.

**D. ROUTER MODES**

Router Modes - User Mode, Privilege Mode, Global Configuration Mode

1.User Mode

**Router >**

It's just a login mode, we cannot configure anything in this mode.

To enter into next mode,Router > enable

or

Router > en

2.Privilege mode

**Router #**

This mode we cannot configure anything in router, but we can see what is already

configured in router using SHOW command

We use this mode for Troubleshooting

In order to go to the next mode

Router # show ?

? is for help, it will display what possible commands

can come after show

Router # show version

Router # show clock

Router# show vlan

To go to next mode

Router# configure terminal

Router# conf t

3.Global Configuration Mode

**Router(config) #**

All router configurations can be made in this mode.

**TO DO**

1. Assign password for USER MODE

2. Command to rename the NAME OF ROUTER

3. TELNET configuration for router

4. Router Basic Configuration

4. Basic Configuration

Router> enable

Router# configure terminal

Router(config)# Interface fastethernet 0/0

Int fasttab

Tab tab is to complete the command

Router(config-if)# ip address 192.168.1.1 255.255.255.0

Router(config-if)# no shutdown

**VERIFY:**

PC 192.168.1.2

CMD

ping 192.168.1.1

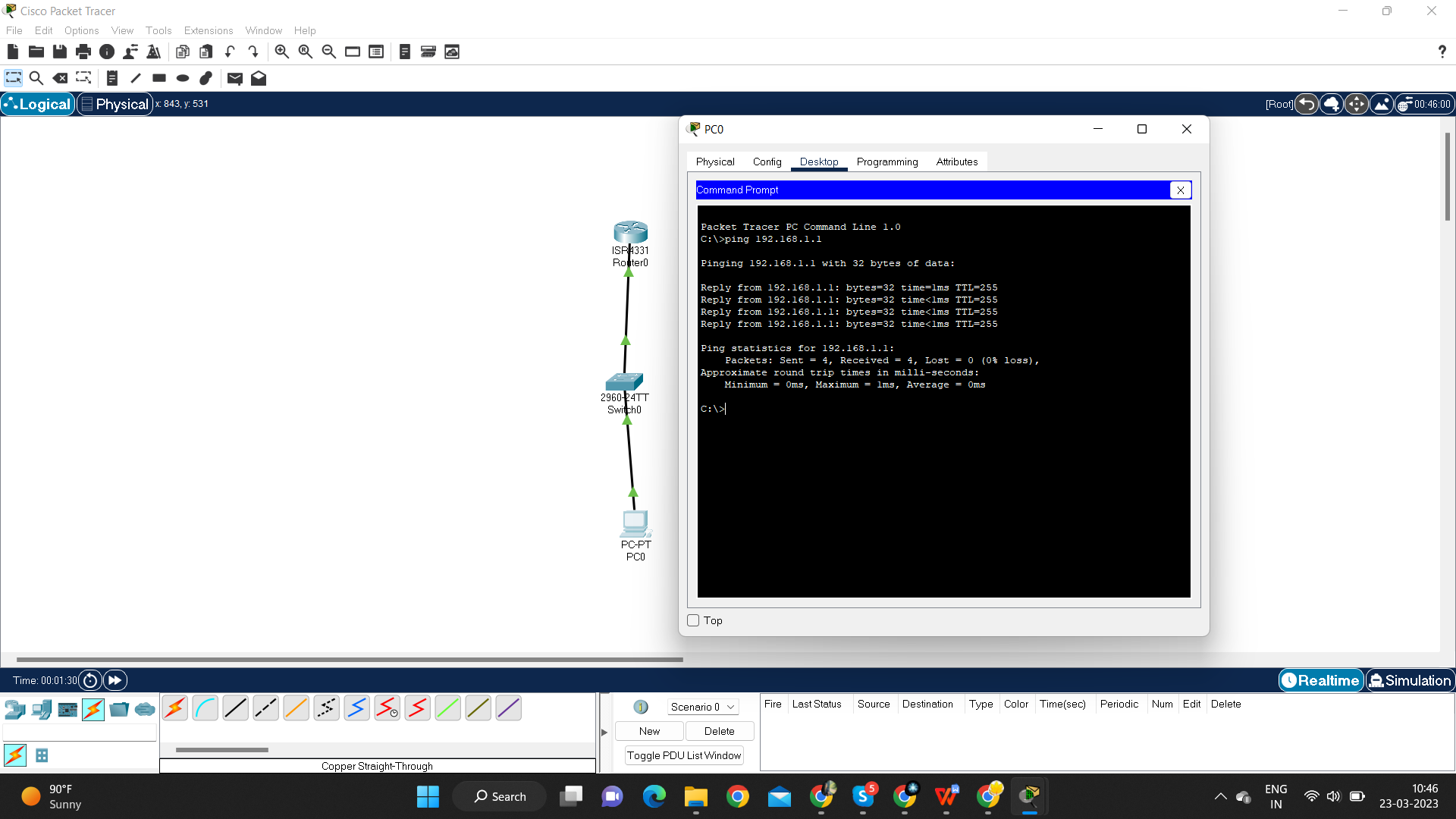
reply from 192.168.1.1

/ Configuration is right

Request timed out

Destination host unreachable

/ Error in configuration



**ROUTING**

It is a process of making two routers communicate with each other.

Or

Process of filling IP tables either manually or automatically.

**TO DO**

1. Create Template in Packet tracer with 3 routers

2. Identify Master and Slave end of Serial cable in packet tracer

3. Set Clock rate as "64000" for master end and "not set" for slave end

**TYPES OF ROUTING**

A. STATIC ROUTING

-Process of filling ip tables with UNKNOWN NID / NETWORKS.

-Configured for smaller networks

B. DYNAMIC ROUTING

-Process of filling ip tables with KNOWN NID / NETWORKS.

-Configured for larger networks

**STATIC ROUTING**

We need to enter Unknown network ids

When we configure static routing in router, we get the following options

Network

- Network ID

Mask

- Subnet Mask

Next Hop

- IP address

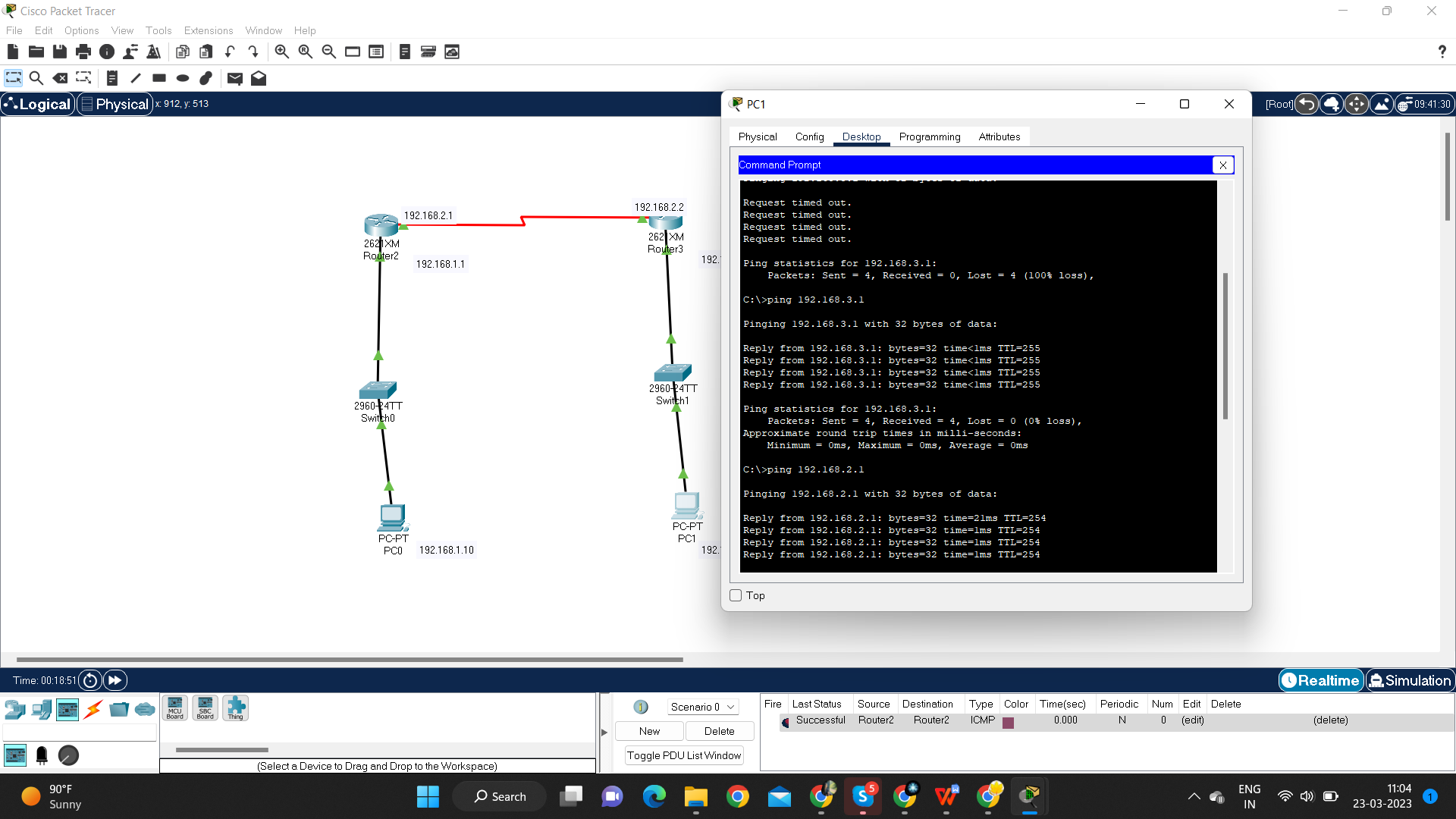
**TODO**

1. Open template in packet tracer

2. Configure Static routing

3. Verify configuration

4. Save As - Static routing



**VERIFY:**

TRY TO PING PC TO PC AND PC TO ROUTERS

**DYNAMIC ROUTING**

In dynamic we configure router with KNOWN NETWORK ID's

TYPES OF DYNAMIC ROUTING PROTOCOLS

A. DISTANCE VECTOR PROTOCOL

- RIP (Routing Information Protocol)

B. LINK STATE PROTOCOL

- OSPF (Open Shortest Path First)

C. ADVANCED DISTANCE VECTOR PROTOCOL

- EIGRP (Enhanced Interior Gateway Protocol)

-All the above routing protocols will identify the best path differently.

-This is based on METRIC (based on what criteria best path is identified)

-Based on the purpose, we use any one of routing protocol

**METRICS OF PROTOCOLS**

**RIP (Routing Information Protocol)**

Metric

- Hop Count

Best Path

- Minimum Hop Count will be considered as the best path.

It's an old protocol and not commonly used nowadays due to false positives.

**OSPF (Open Shortest Path First)**

Metric

- Bandwidth

Bandwidth is the channel width, (Like roadsize, bigger the road size faster we can

travel) more the bandwidth, speed of internet will be more.

Best Path

- Maximum Bandwidth is considered as best path

Used commonly for router configuration

**EIGRP (Enhanced Interior Gateway Protocol)**

Metric

- Bandwidth & Delay

Delay is the time taken for the packet to reach the destination and come back.

Best Path

- Maximum Bandwidth & Minimum delay is best path

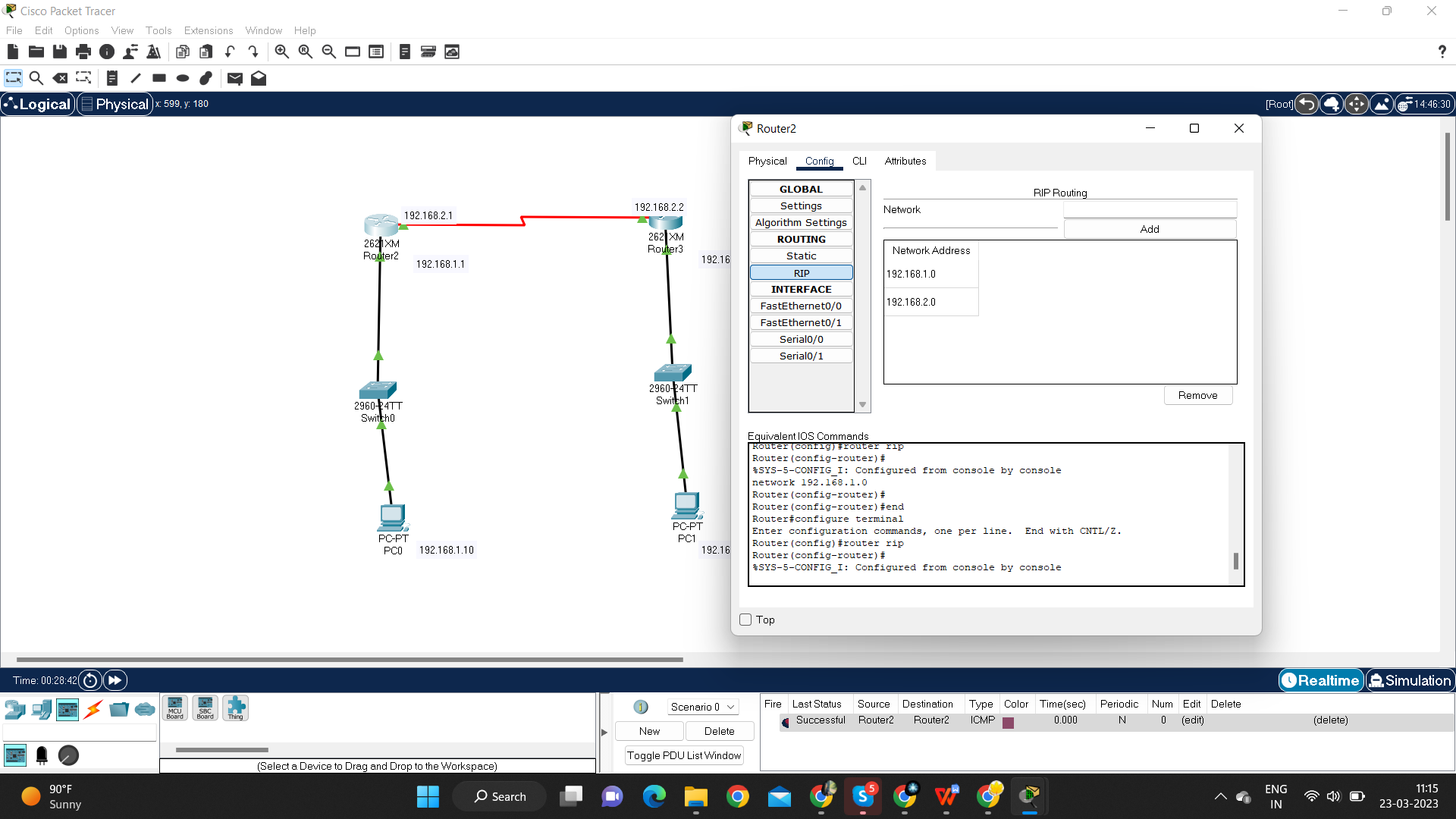
Most commonly used routing protocol.

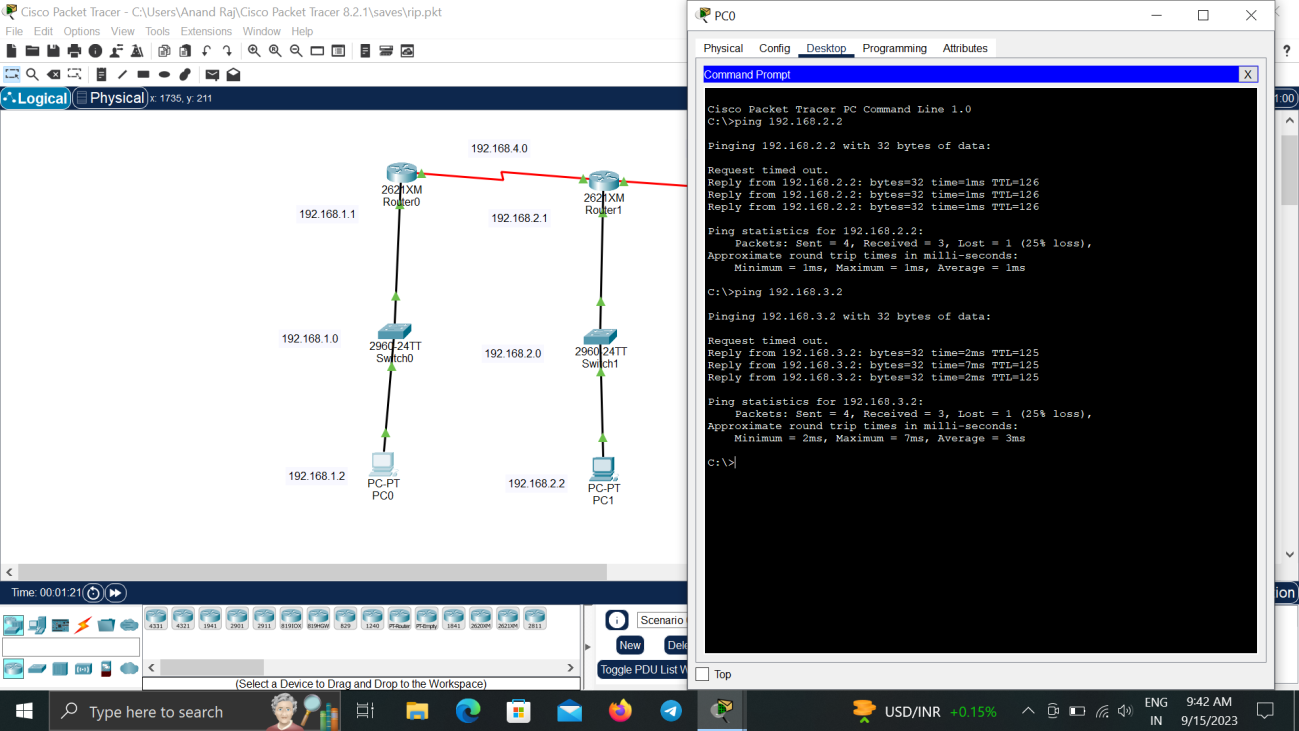
**CONFIGURATION COMMANDS**

**RIP**

#ROUTER RIP

#NETWORK (NETWORK ID)

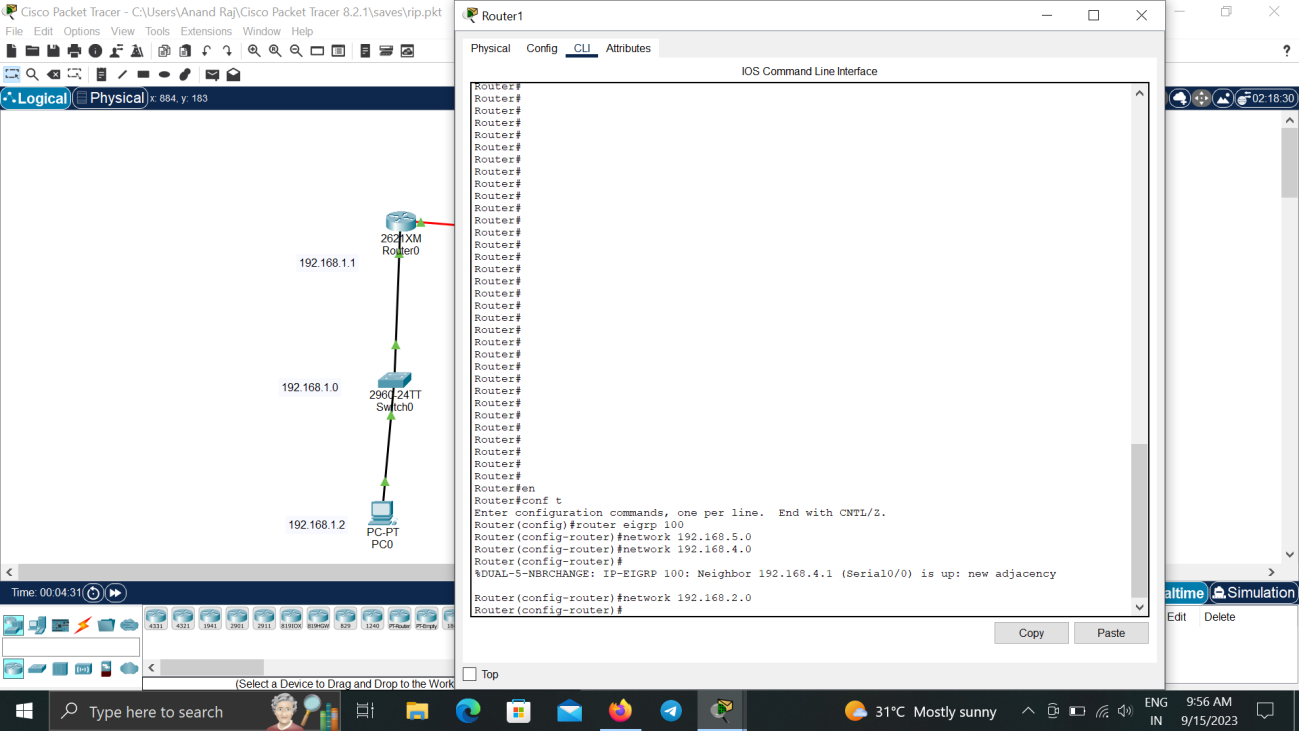




**EIGRP**

#ROUTER EIGRP (AUTONOMOUS NUMBER)

#NETWORK (NETWORK ID)



**OSPF**

ROUTER A

#ROUTER OSPF **PROCESS ID(600)**

#NETWORK 192.168.1.0 **WILDCARD MASK AREA 100**

#NETWORK 192.168.2.0 0.0.0.255 AREA 100

ROUTER B

#ROUTER OSPF 700

#NETWORK 192.168.2.0 0.0.0.255 AREA 100

#NETWORK 192.168.3.0 0.0.0.255 AREA 100

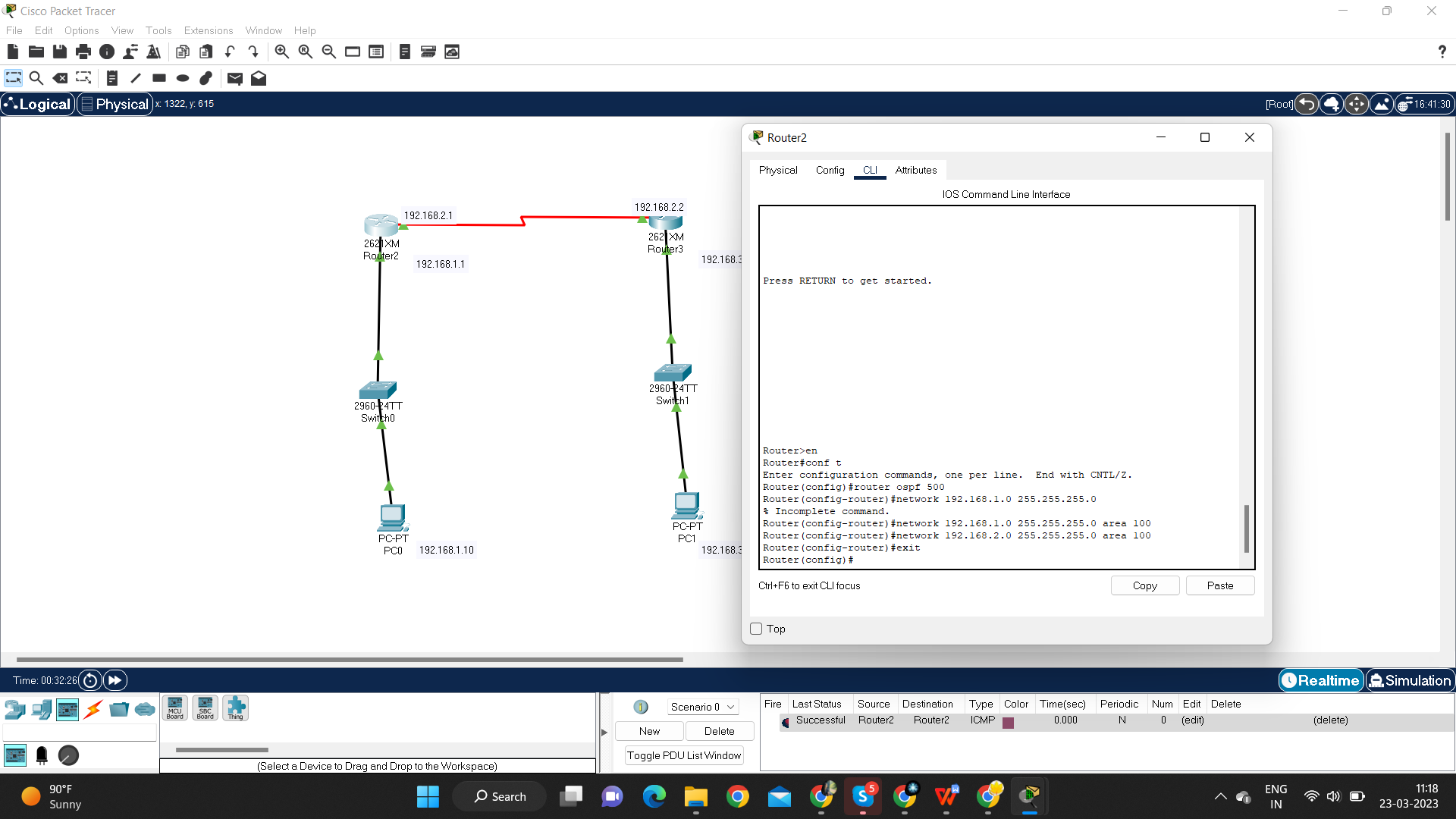
#NETWORK 192.168.4.0 0.0.0.255 AREA 100

ROUTER C

#ROUTER OSPF 800

#NETWORK 192.168.4.0 0.0.0.255 AREA 100

#NETWORK 192.168.5.0 0.0.0.255 AREA 100



**VERIFY:**

**TRY TO PING PC TO PC AND PC TO ROUTERS**

**SWITCH-SWITCHING**

-SWITCH PORTS

-SWITCH RULES

-SWITCH MODES

-BASIC CONFIG

**SWITCH PORTS**

-BASED ON FUNCTIONALITY

1. ACCESS PORT

-used for connecting a switch with another device(comp,router)

2. TRUNK PORT

-used to connect two switches

**SWITCH RULES**

- When you are trying to connect a switch to a router, you will connect in 0/1

to the router's 0/0 port.

- When you are trying to connect a switch with another switch, you will

connect in 0/24 to another switch 0/1

**SWITCH MODES**

- Similar to router modes

- We have 24 port switch

- We have to assign the ports manually.

**BASIC CONFIGURATION**

#INTERFACE FASTETHERNET 0/2

#SWITCHPORT MODE ACCESS

#EXIT

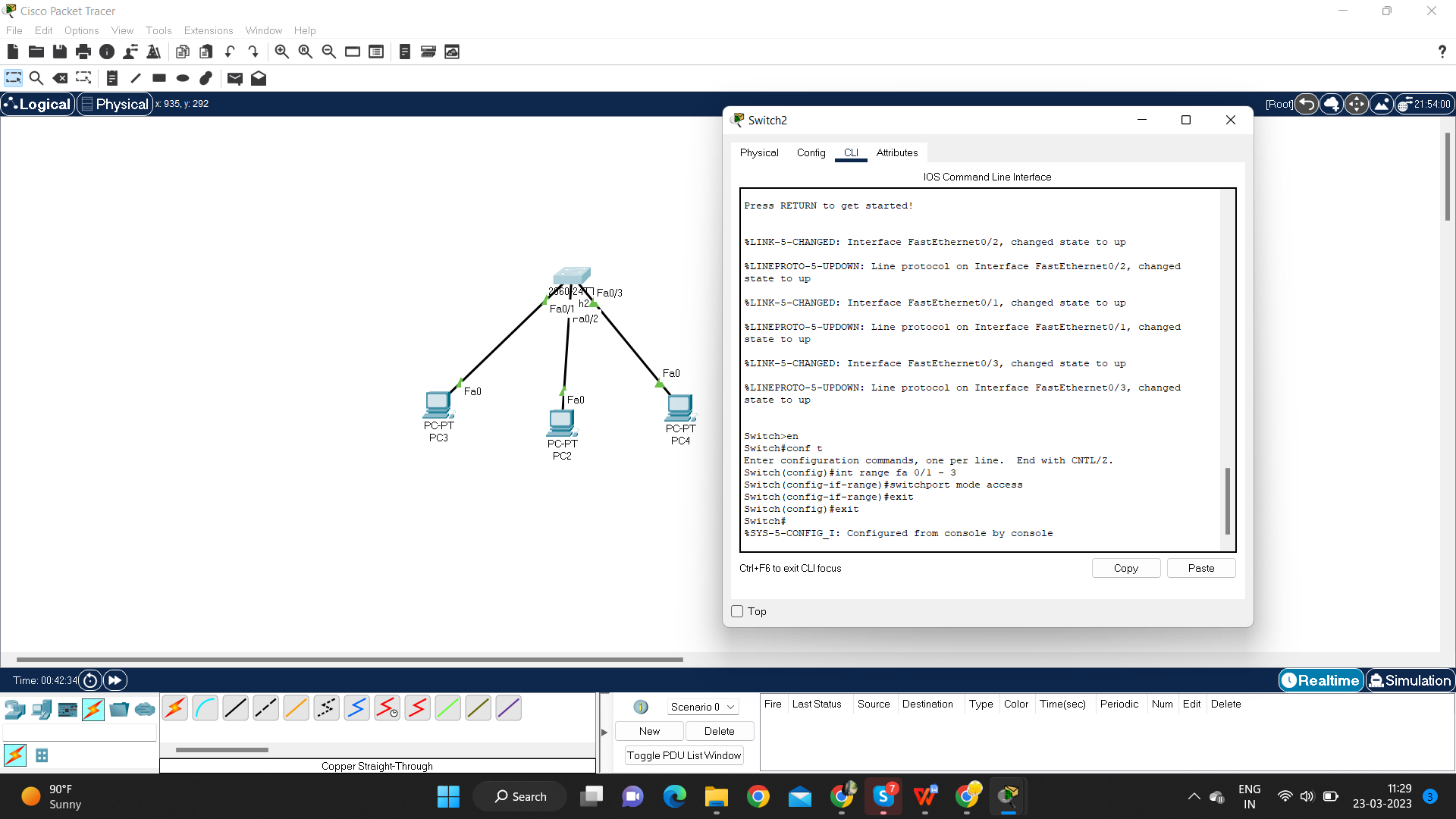
If you have many ports that has to be assigned as access mode, then you can use

the RANGE command

#INTERFACE RANGE FA0/1 - 20

#SWITCHPORT MODE ACCESS

#EXIT



**VERIFY:**

TRY TO PING PC TO PC - YOU SHOULD GET REPLY

**VLAN**

- Subnetting depends on two factors - IP RANGE & CUSTOM SUBNET MASK

- Vlan does not depend on both of these, because we configure the ports of a switch

and not computers.

**Steps to create VLAN**

1. Create vlan name and number

2. Configure switch port - Access port / Trunk port

3. VLAN membership - link the port with created vlan

PACKET TRACER

Create two VLANs

SALES 100 & HR 200

SWITCH>EN

#SHOW VLAN

#CONF T

#VLAN 100 //STEP1

#NAME SALES //STEP1

#EXIT

#EXIT

#SHOW VLAN

#CONF T

#INTERFACE FA0/2 //STEP 2

#SWITCHPORT MODE ACCESS //STEP 2

#SWITCHPORT ACCESS VLAN 100 //STEP 3#EXIT

#SHOW VLAN

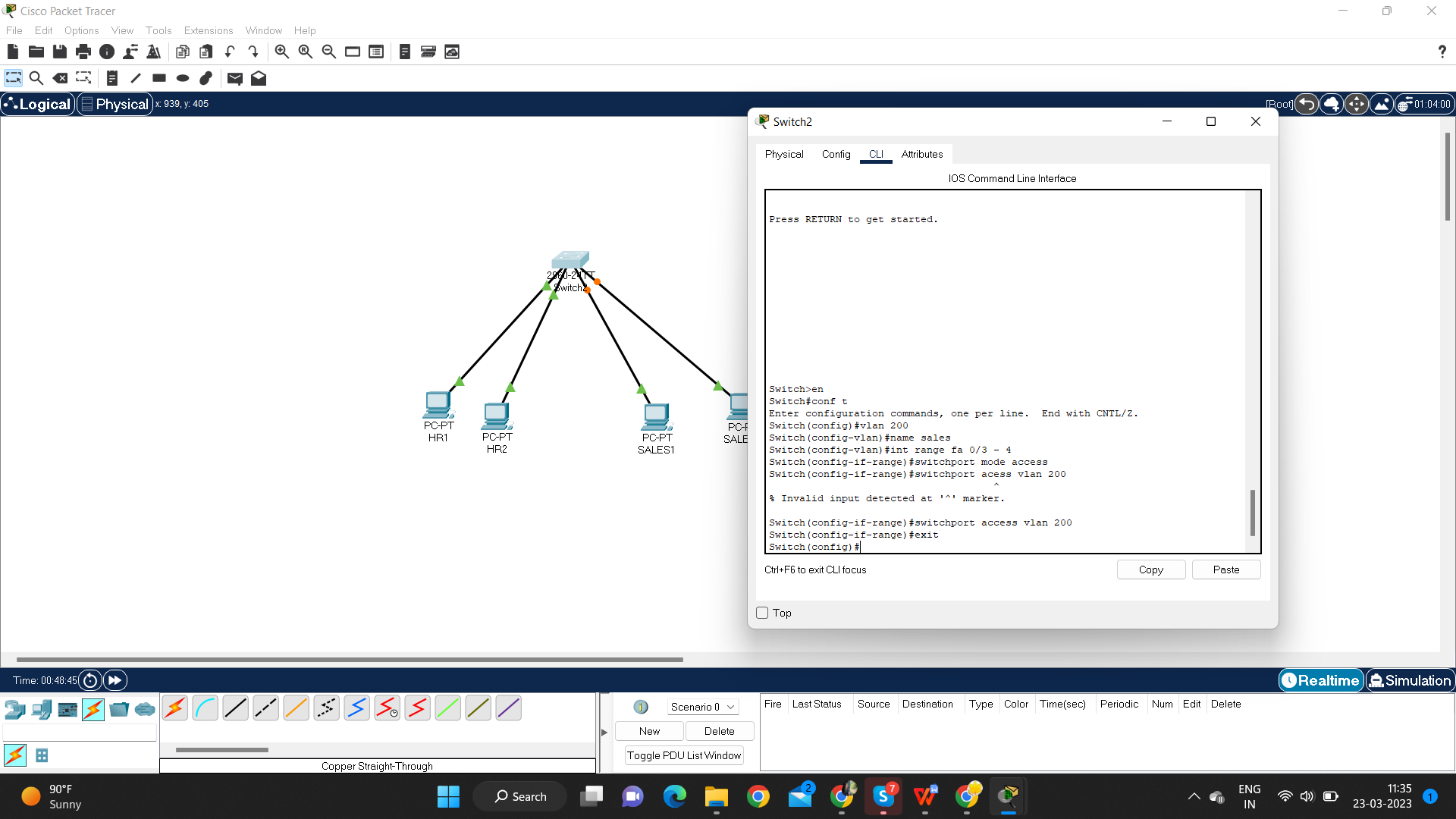
Repeat the same for HR 200

**Verify:**

PING

192.168.1.2 -- 192.168.1.3

No reply



**VERIFY:**

PING HR - HR - GET REPLY

SALES - HR - NO REPLY

**PORT SECURITY**

Disadvantages of VLAN

When attacker computer from outside our LAN tries to connect to sales vlan 100 of

switch 1, what will happen?

He will be able to connect and he can access all the documents of sales vlan, this is

a security risk and port security is used to stop this.

- Port security assigns a particular mac address to a particular port.

- Only a computer with that mac address can access that port.

- If a computer with different mac address tries to access, the port will be either

blocked or shut down

**Steps to configure PORT SECURITY**

1. CHOOSE PORT/INTERFACE OF SWITCH

2. CONFIGURE PORT - ACCESS PORT / TRUNK PORT

3. ENTER PORT SECURITY CONFIGURATION

4. CHOOSE MAXIMUM NO OF COMPUTERS THAT CAN ACCESS THE PORT

5. ASSIGNING MAC ADDRESS - AUTOMATIC(STICKY) OR MANUAL

6. CONFIGURING VIOLATION RULE - RESTRICT,SHUTDOWN

RESTRICT - PACKET TRACER WILL KEEP THE PORT ON - GREEN, BUT ATTACKER

WON'T BE ABLE TO ACCESS ANYTHING FROM SALES VLAN

SHUTDOWN - PORT WILL BE DOWN, PACKET TRACER - RED

PACKET TRACER 1

#INT FA0/2

#SWITCHPORT MODE ACCESS

#SWITCHPORT PORT SECURITY

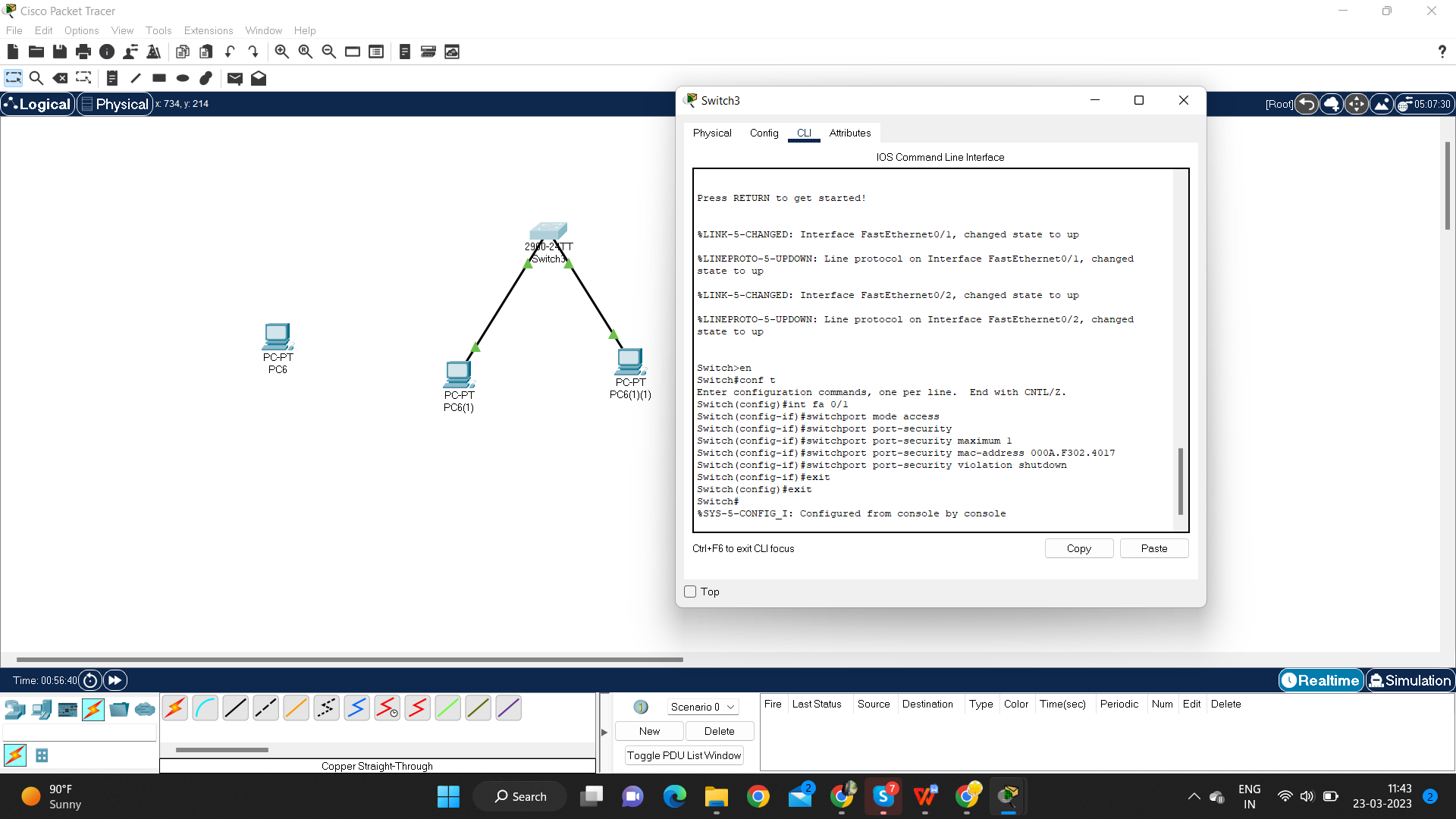
#SWITCHPORT PORT-SECURITY MAXIMUM 1#SWITCHPORT PORT-SECURITY MAC ADDRESS STICKY

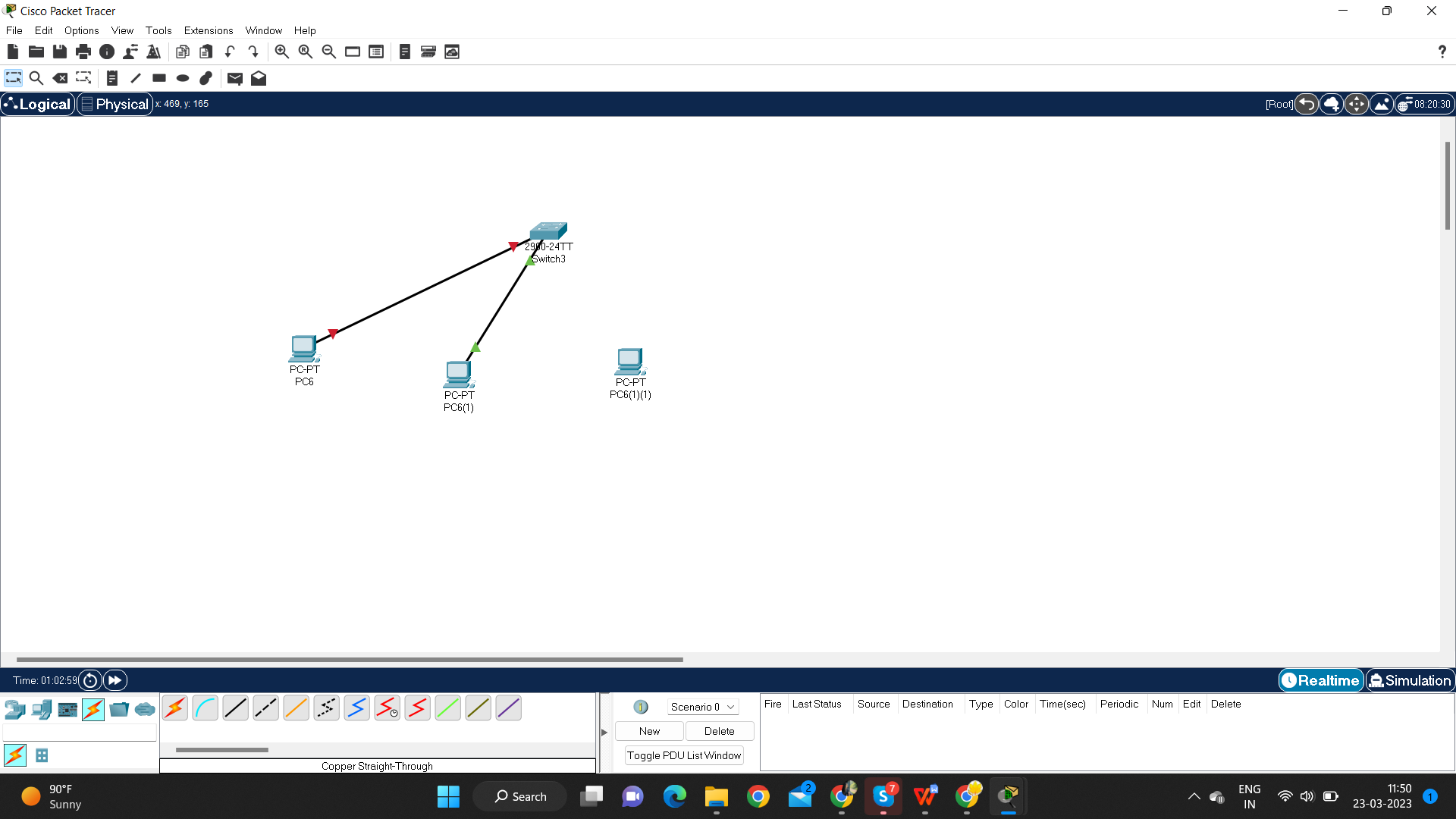
#SWITCHPORT PORT-SECURITY VIOLATION SHUTDOWN

VERIFY

REMOVE THE CONNECTION FROM 0/2, CONNECT A NEW COMPUTER TO 0/2,

PORT WILL TURN RED





**VERIFY:**

CONNECT UNKNOWN PC TO THE INT 0/2 PC

SHUTDOWN - PORT WILL INTO RED

RESTRICT - PING PC TO PC - REQ TIMED OUT.

**ACL - ACCESS CONTROL LIST**

It's a configuration done at router

It is used to control traffic of all computers in our lan

It permits / denies traffic based on the rules which we create.

**TYPES OF ACL**

A. STANDARD ACL

B. EXTENDED ACL

**A. STANDARD ACL**

- Its old and used in smaller networks

- It is permits / denies traffic based on "SOURCE IP ADDRESS"

- Configured close to "DESTINATION"

- Number Range 0 - 99

**B. EXTENDED ACL**

- Its new and used in larger networks

- It is permits / denies traffic based on

"SOURCE IP ADDRESS"

"DESTINATION IP ADDRESS"

"PROTOCOL"

"PORT NUMBER"

- Configured close to "SOURCE"

- Number Range 100 - 199

**STEPS TO CONFIGURE STD ACL**

1. ACL CREATION

2. SELECT AN INTERFACE

3. IMPLEMENTATION OF ACL

4. VERIFICATION OF ACL STANDARD ACL CONFIGURATION

1.ACL CREATION

#ACCESS-LIST <NO>PERMIT/DENY <SOURCE IP><SOURCE WILDCARD MASK>

2.IMPLEMENTATION OF ACL

#INTERFACE<TYPE><NO>

#IP ACCESS-GROUP<NO> IN/OUT

3.VERIFICATION OF ACL

#SHOW IP ACCESS-LIST

4.VERIFICATION-IMPLEMENTATION OF ACL

#SHOW IP INTERFACE <TYPE><NO>

router A,

#access-list 10 deny 192.168.3.2 0.0.0.0

#interface fast ethernet 0/0

ip access-group 10 in

verify

3.2 - > 1.2 ping

**NOTE** :

WILDCARD MASK FOR ACL WILL HAVE THE FOLLOWING CRITERIA

NORMAL WILDCARD MASK WILL BE THE INVERSE OF UR SUBNET MASK

BUT HERE WE HAVE TWO SCENARIOS

SCENARIO 1 - WHEN WE CONFIGURE FOR A SINGLE HOST / IP

i.e 192.168.1.2, then Wildcard mask will be all zeros 0.0.0.0

SCENARIO 2 - WHEN WE CONFIGURE FOR A ENTIRE NETWORK

i.e 192.168.1.0, then Wildcard mask will be 0.0.0.255

WHEN IMPLEMENTING ACL , WE HAVE TWO OPTIONS

IN & OUT

IN blocks the incoming traffic

OUT block the outgoing traffic

**VERIFY:**

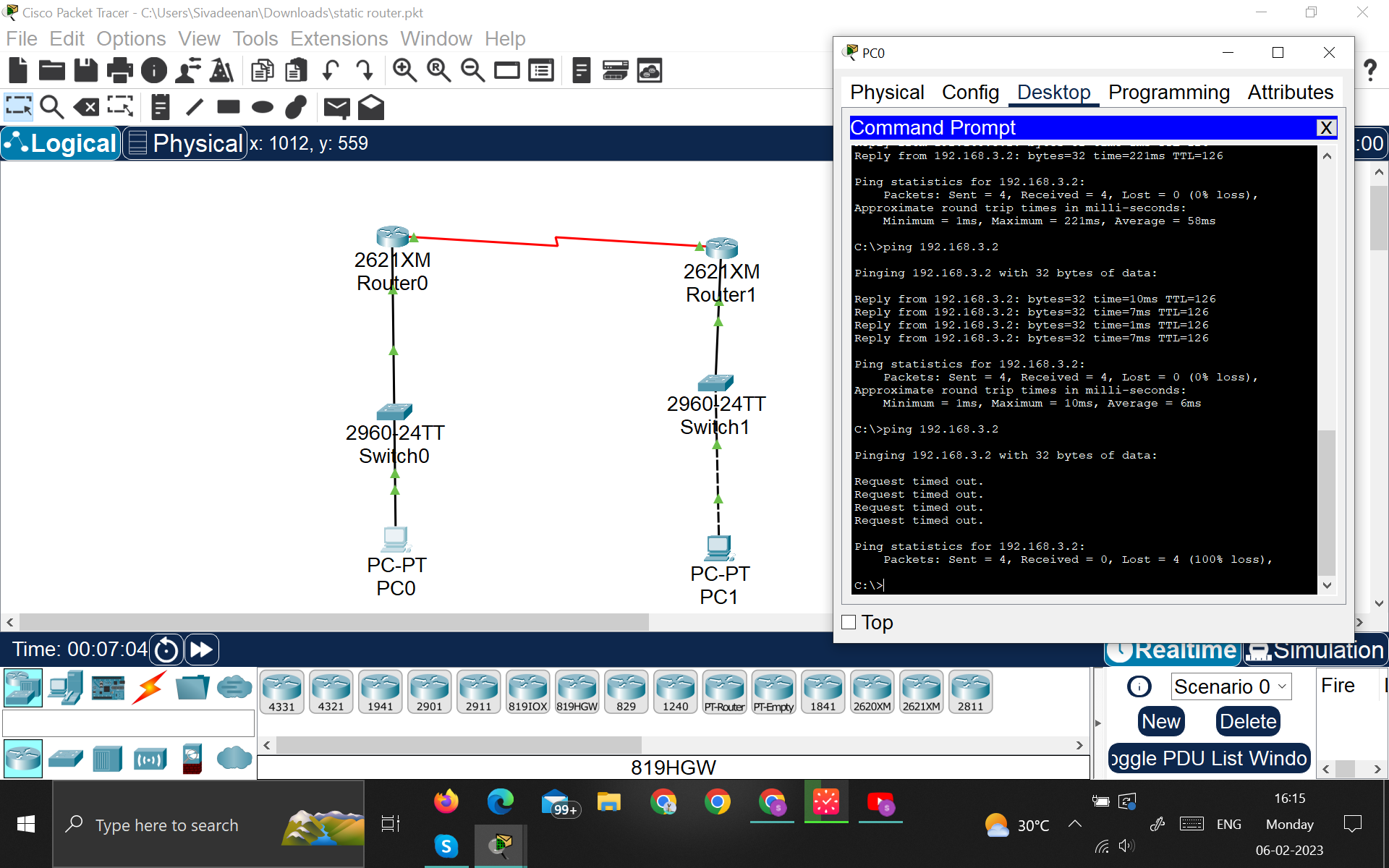
THE OUTPUT VARIES LIKE BELOW WHEN WE PING

IN

:REQUEST TIMEOUT

OUT

:DESTINATION HOST UNREACHABLE



**EXTENDED ACL**

ACL CREATION:

#ACCESS-LIST <NO>PERMIT/DENY<PROTOCOL><SOURCE IP><SOURCE

WILDCARD MASK><DESTINATION IP><DESTINATION WILDCARD

MASK><OPERATOR><PORT NO>

IMPLEMENTATION OF ACL

#INT <TYPE><NO>

#IP ACCESS-GROUP <NO>IN/OUT

Note:

1. More specific statements should be at top

2. More generic statements should be at bottom

access-list 110 permit 192.168.1.2 ..........

(1)

access-list 110 deny 192.168.1.0 .......

(2)

The above statement will permit only 1.2 and deny all other computers

access-list 110 deny 192.168.1.0 .......

(2)

access-list 110 permit 192.168.1.2 ..........

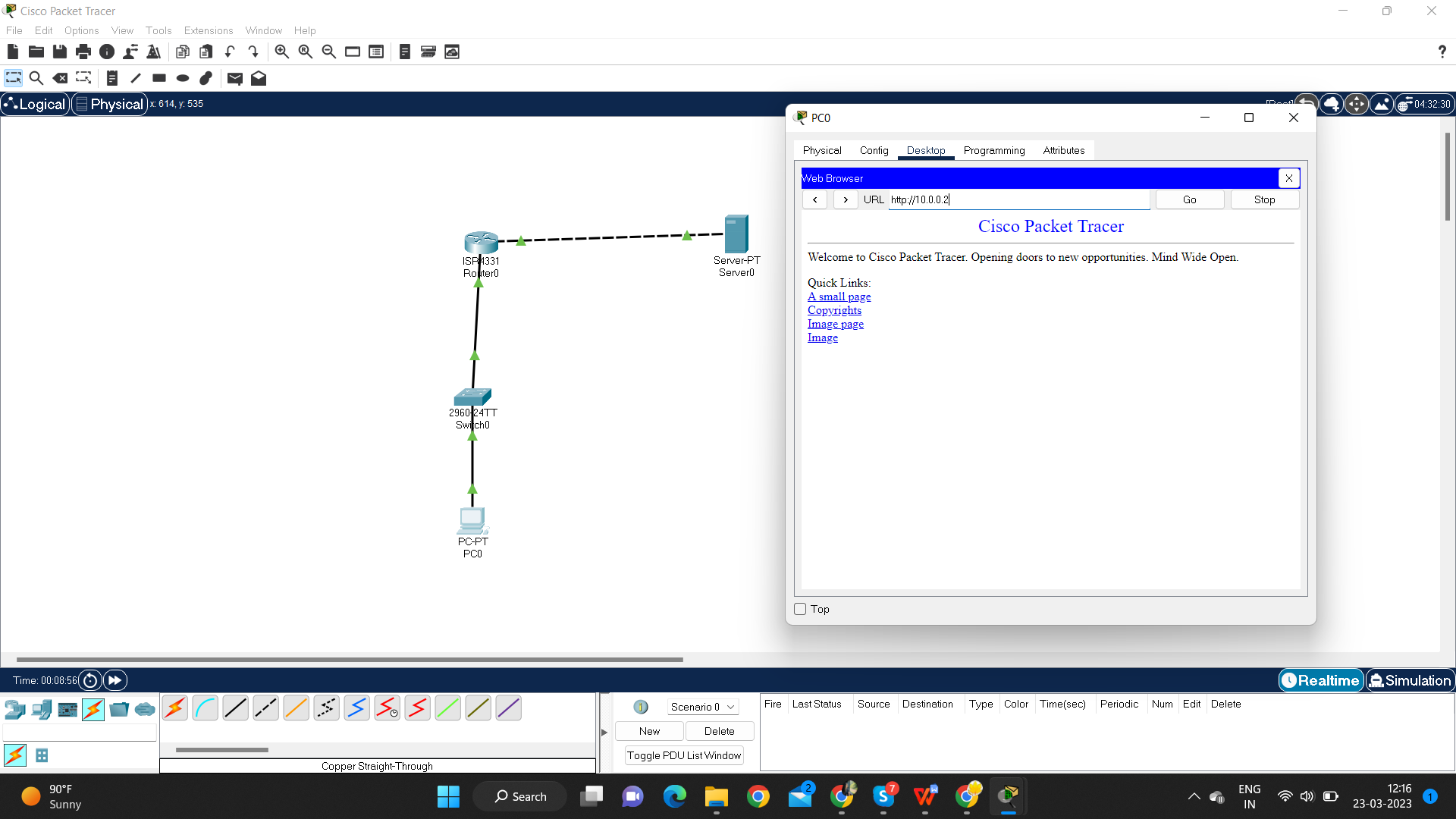
(1)

The above statement will deny all computers including 1.2,

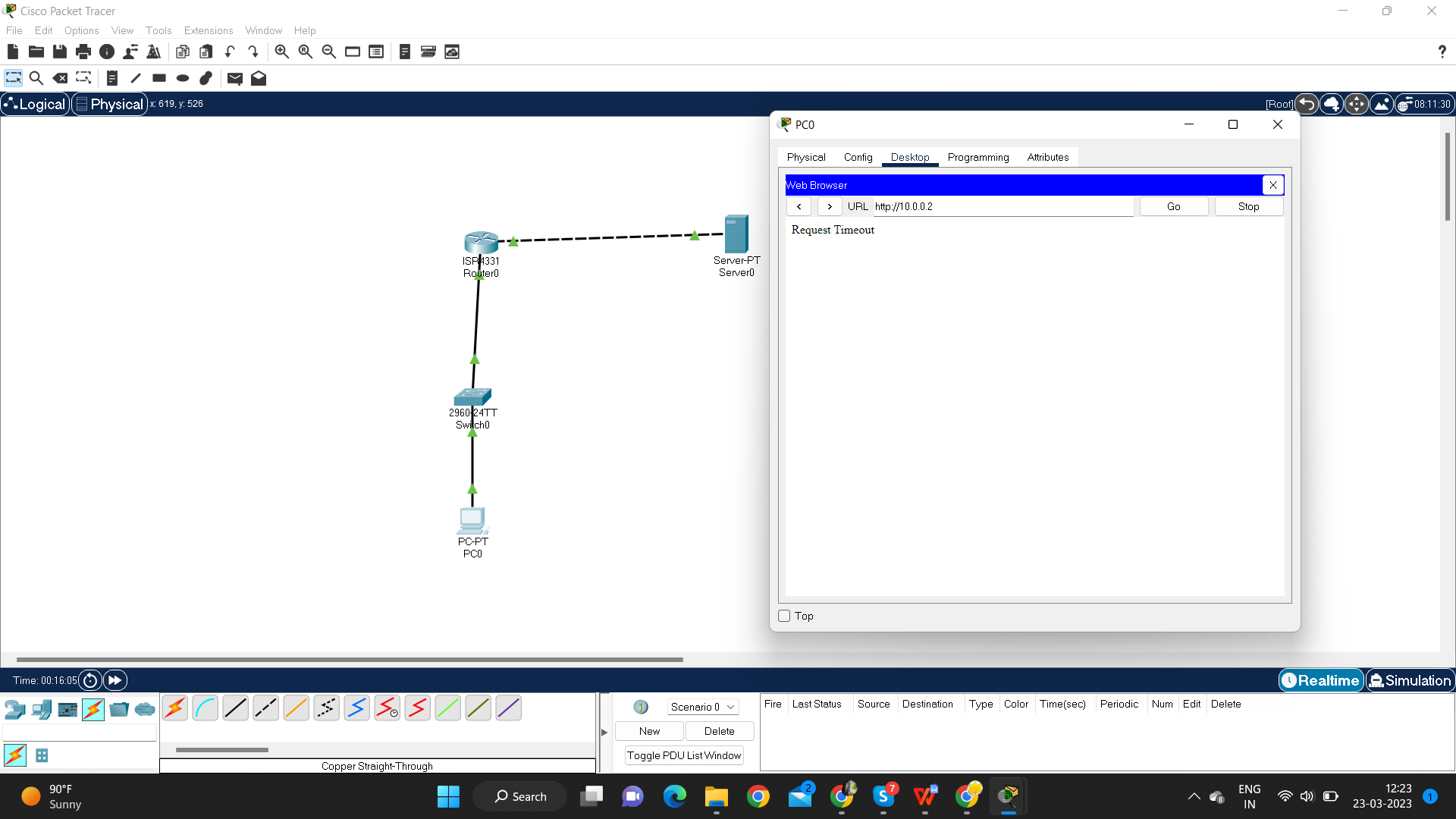
so statement number (2) will not work.

**VERIFY:**

**BEFORE EXT ACL CONFIG:**



**AFTER EXT ACL CONFIG:**



**BGP - BORDER GATEWAY PROTOCOL:**

THIS COMES UNDER EGP - EXTERIOR GATEWAY PROTOCOL

IN CCNA WE SAW IGP - INTERIOR GATEWAY PROTOCOL, AND THAT'S THE REASON WHEN WE CONFIGURED 3 ROUTERS, THE AUTONOMOUS NUMBER FOR THE THREE ROUTERS WERE SAME, BECAUSE IGP WILL ONLY CONFIGURE ROUTERS IN SAME AREA. WHEREAS BGP CAN PROVIDE ROUTING TO ROUTERS WITH DIFFERENT AUTONOMOUS NUMBER.

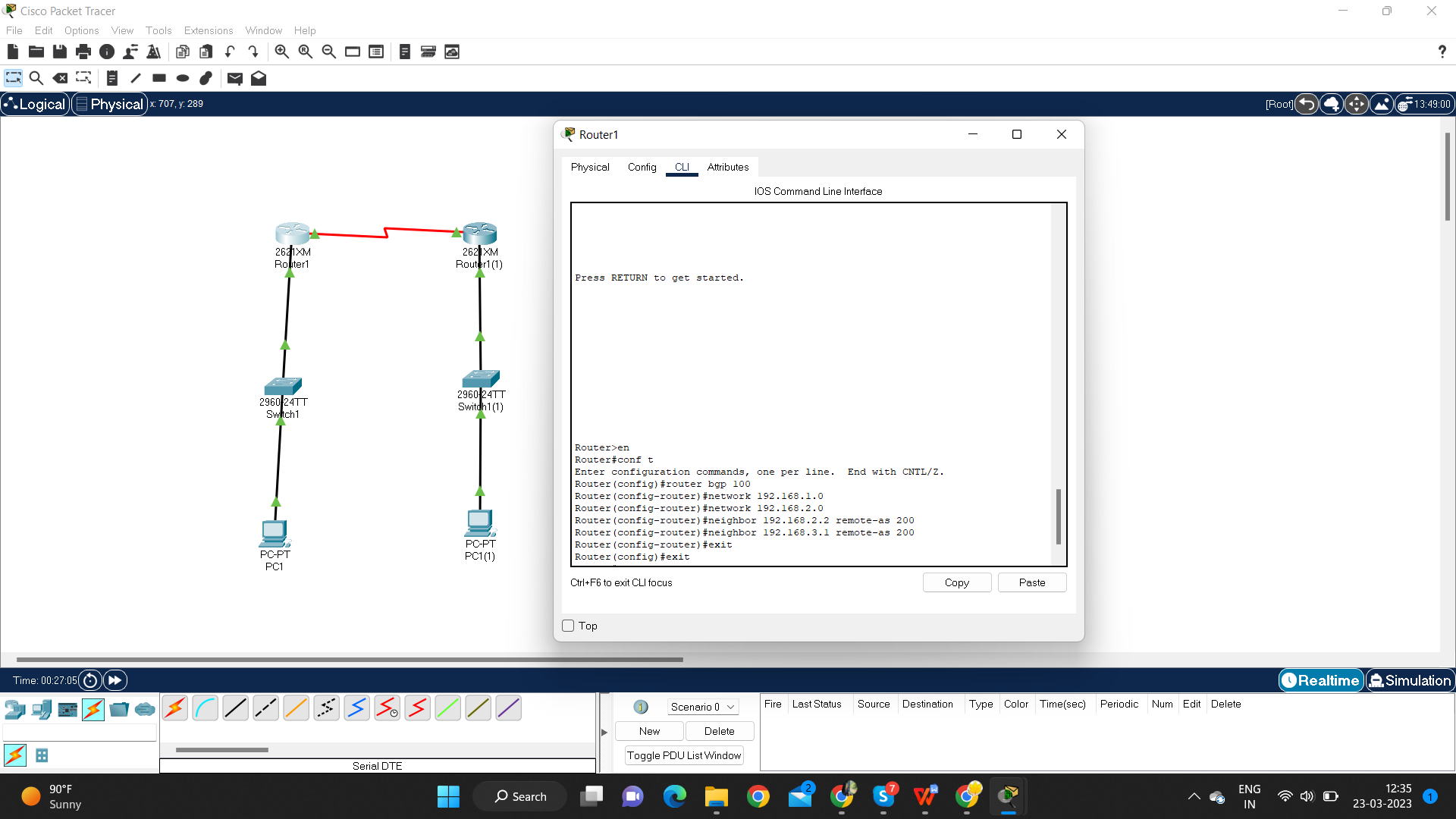
**CONFIGURATION**

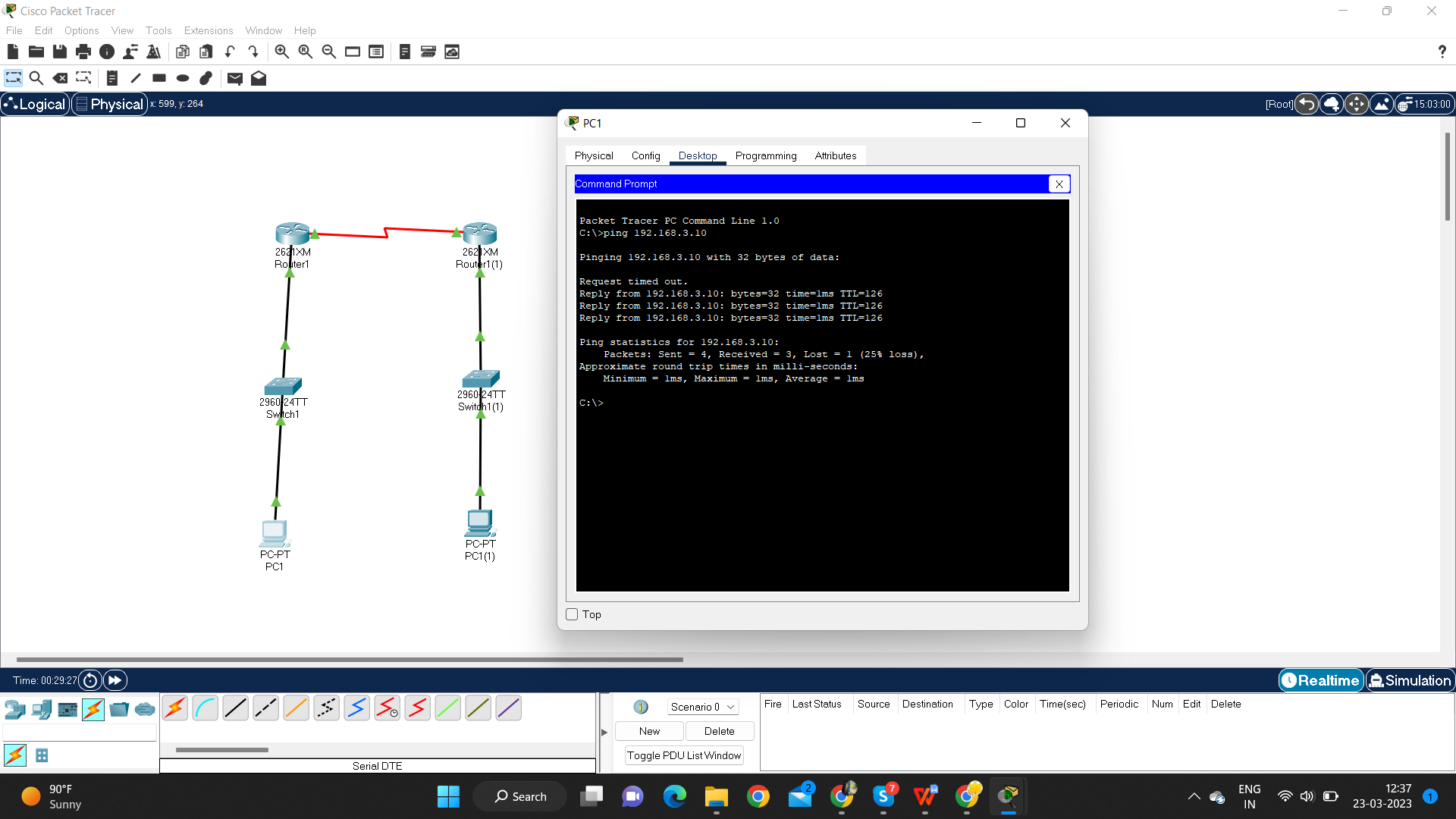
ROUTER A

#ROUTER BGP (AUT NO- A)

#NETWORK (NID)

#NEIGHBOR (NEXT HOP IP ADDRESS) REMOTE-AS (REMOTE ROUTER AUT NO- B)





**VERIFY:**

PING PC TO PC - GET REPLY

**NAT:**

**NETWORK ADDRESS TRANSLATION**

- Its a default occurrence in our LAN (Private ip to public ip)

- Also configured for security reasons - to mask or hide or server ip

NAT is also configured for LOAD BALANCING

load balancing is done for any company which has a larger number of servers. A load Balancer can split the traffic uniformly among available servers, so that server

overload can be prevented

Example of Load Balancer is F5 Load balancer

The main objective of configuring NAT is - When someone pings our server, our

server should not directly reply to them instead, a different ip address should reply.

Ex: When we ping google.com, we get a reply from google.co.in

**Config Steps:**

1.Router A & B - static routing

2.Verify - 192.168.1.2 --> 10.0.0.2

reply from 10.0.0.2

3.Configure NAT

4. Repeat Step 2

Reply from 200.1.1.2

Steps to configure NAT

#IP NAT INSIDE SOURCE STATIC (ACTUAL IP) (CONVERTED IP)

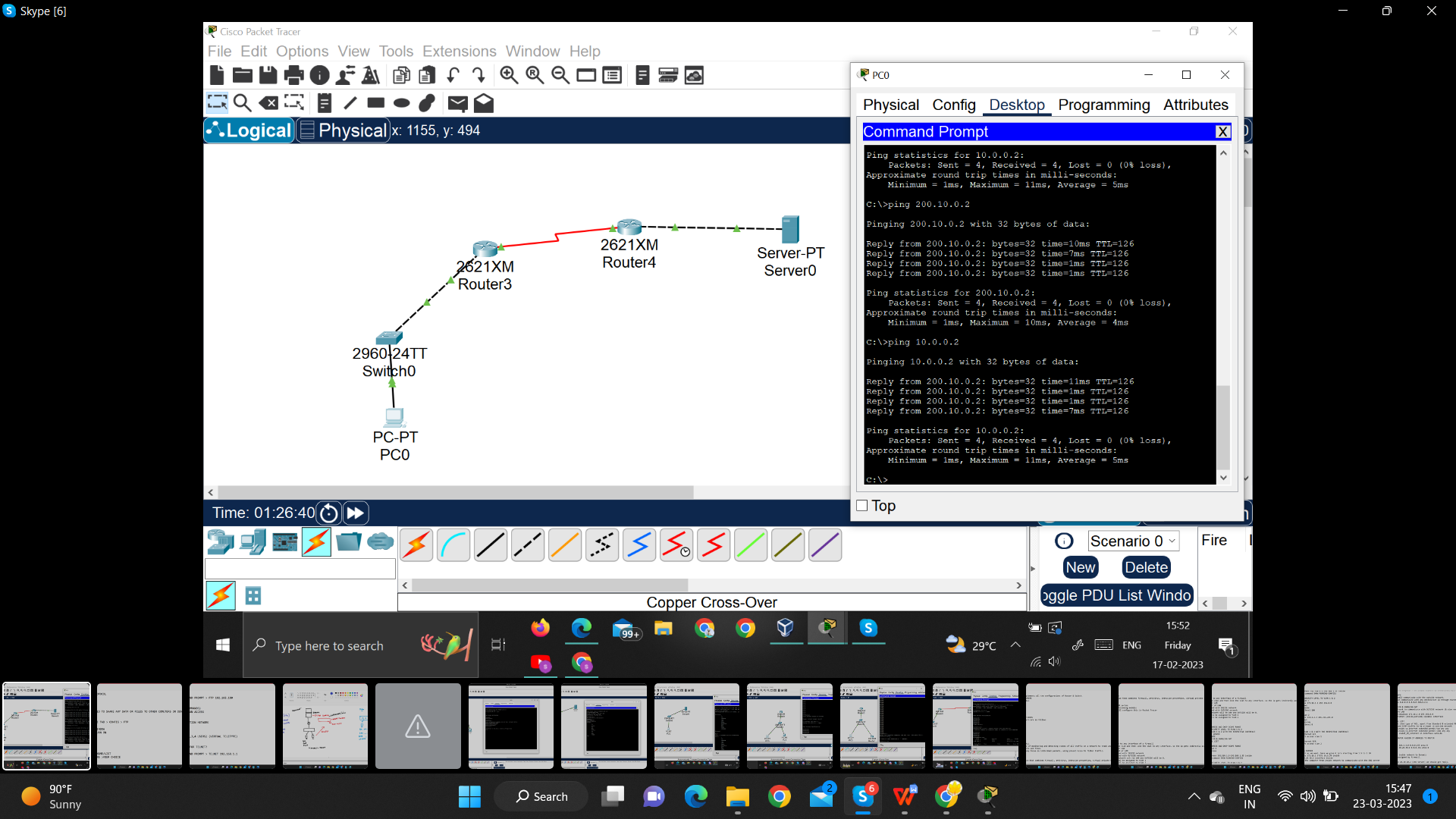
#INTERFACE FAST ETHERNET (NUMBER)

#IP NAT INSIDE

#INTERFACE SERIAL (NUMBER)

#IP NAT OUTSIDE

#EXIT



**VERIFY:**

PING SERVER - REPLY COMES FROM PROXY IP

**PAT - PORT ADDRESS TRANSLATION**

* COMMONLY KNOWN AS "NAT OVERLOAD"
* IT IS MAPPING MANY INTERNAL LAN COMPUTERS PRIVATE IP TO A SINGLE IP ADDRESS,
* BUT USING DIFFERENT PORT NUMBERS.
* IT IS ONE WAY OF IMPLEMENTING NAT

**3 WAYS OF IMPLEMENTING NAT**

* PAT
* POOLED NAT
* STATIC NAT
* EACH INTERNAL LAN COMPUTER (PRIVATE IP) WILL HAVE A SINGLE IP ADDRESS (PUBLIC IP)
* MAPPED BUT USES DIFF PORTS TO DIFFERENTIATE EACH COMPUTER
* NAT CONFIGURATION DEFINES WHICH IP SHOULD RESPOND WHEN SOMEONE PINGS TO A SERVER

(EX: WHEN WE PING GOOGLE.COM,GOOGLE.CO.IN RESPONDS)

* PAT CONFIGURATION DEFINES WHICH IP SHOULD BE SHOWN WHEN WE PING TO ANY COMPUTER OR
* SERVER  (EX: WHEN WE PING GOOGLE.COM, PRIVATE IP WILL BE MASKED AND
* PUBLIC IP WILL BE DISPLAYED TO GOOGLE SERVER) CONFIGURATION

**STEPS TO CONFIGURE PAT:**

1.CONFIGURE IP TO ROUTERS & PC (A ROUTER CONNECTED TO LAN-1.1, A CONNECTED 20.0.0.1 20.0.0.2 , B CONNECTED TO SERVER 10.0.0.1 10.0.0.2)

2.CONFIGURE ROUTING (STATIC OR DYNAMIC)

3.CONFIGURE TELNET TO 2 ROUTERS

4.CONFIGURE GENERAL NAT IN ROUTER

5.CREATE NAT POOL

6.CREATE ACL

7.APPLY NAT RULE

8.VERIFICATION

STEP 3> CONFIGURE TELNET TO ROUTERS

ROUTER A & B

>EN

#CONF T

#LINE VTY 0 4              //CONFIGURING TELNET TO A AND B ROUTERS

VERIFY FROM PC

TELNET 192.168.1.1

ROUTER>

STEP 4:CONFIG GENERAL NAT IN ROUTER

ROUTER A

#INT FA 0/1

#IP NAT INSIDE

#EXIT

#INT SE 0/0/0

#IP NAT OUTSIDE

#EXIT

STEP 5:CREATE NAT POOL

#IP NAT POOL TEST 20.0.0.1 20.0.0.1 NETMASK 255.0.0.0

TEST IS THE NAME OF NAT POOL AND SINCE WE HAVE ONLY ONE ROUTER, OUT NAT POOL

RANGE WILL BE 20.0.0.1 TO 20.0.0.1

STEP 6:CREATE ACL (STANDARD)

#ACCESS-LIST 10 PERMIT 10.0.0.0 0.255.255.255       //PERMITTING TO ACCESS WHOLE SERVER

STEP 7:APPLY NAT RULE

#IP NAT INSIDE SOURCE LIST 10 POOL TEST OVERLOAD         //ENABLING NAT OVERLOAD(PAT)

**VERIFY:**

FROM COMPUTER PING 10.0.0.2 - check reply

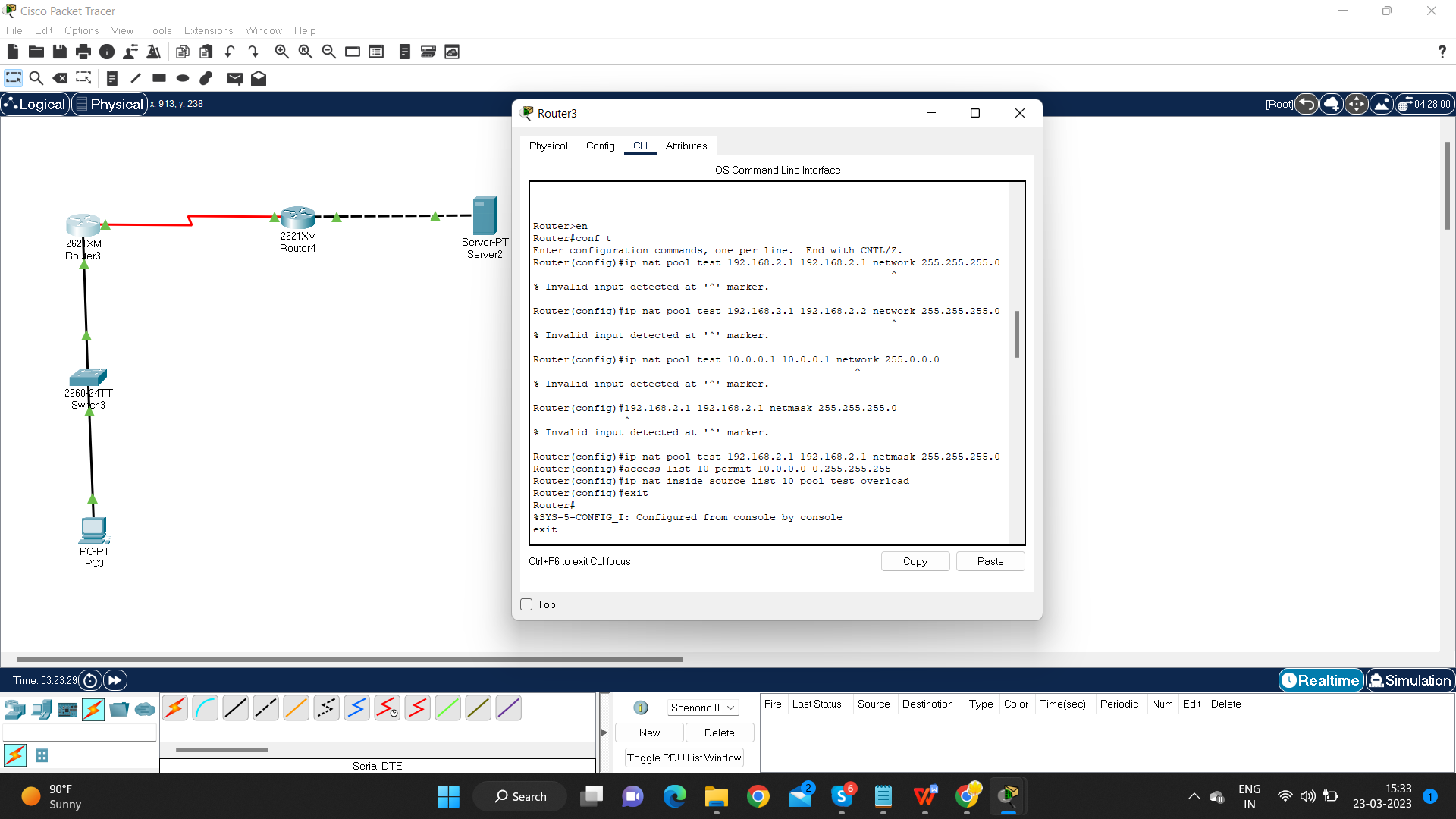
TELNET 20.0.0.2     //IT WILL LOGIN TO ROUTER B

>EN

#SHOW USER         //IT WILL NOT DISPLAY 10.0.0.2 IP

GO TO ROUTER A

#SHOW IP NAT TRANSLATIONS



**FTP-FILE TRANSFER PROTOCOL**

PORT NO: 20,21

20 > DATA PORT

21 > COMMAND PORT

FTP IS A PROTOCOL USED FOR FILES TRANSFERRING. IT IS A PROTOCOL USED TO SHARE ANY DATA OR FILES TO COMPUTER AND OTHER DEVICES.

**TODO:**

PT SETUP AND IP ASSIGNING

CONFIGURATION STEPS:

OPEN SERVER > SERVICE TAB > CONFIG > FTP

SELECT FTP PORT AND TURN ON

RIGHT SIDE > NEW PANEL OPENS

USERNAME: ADMIN

PASSWORD: ADMIN@123

PERMISSION:

READ/WRITE/DELETE/LIST/RENAME

SELECT ANY PERMISSIONS

ADD > CLICK

**VERIFY:**

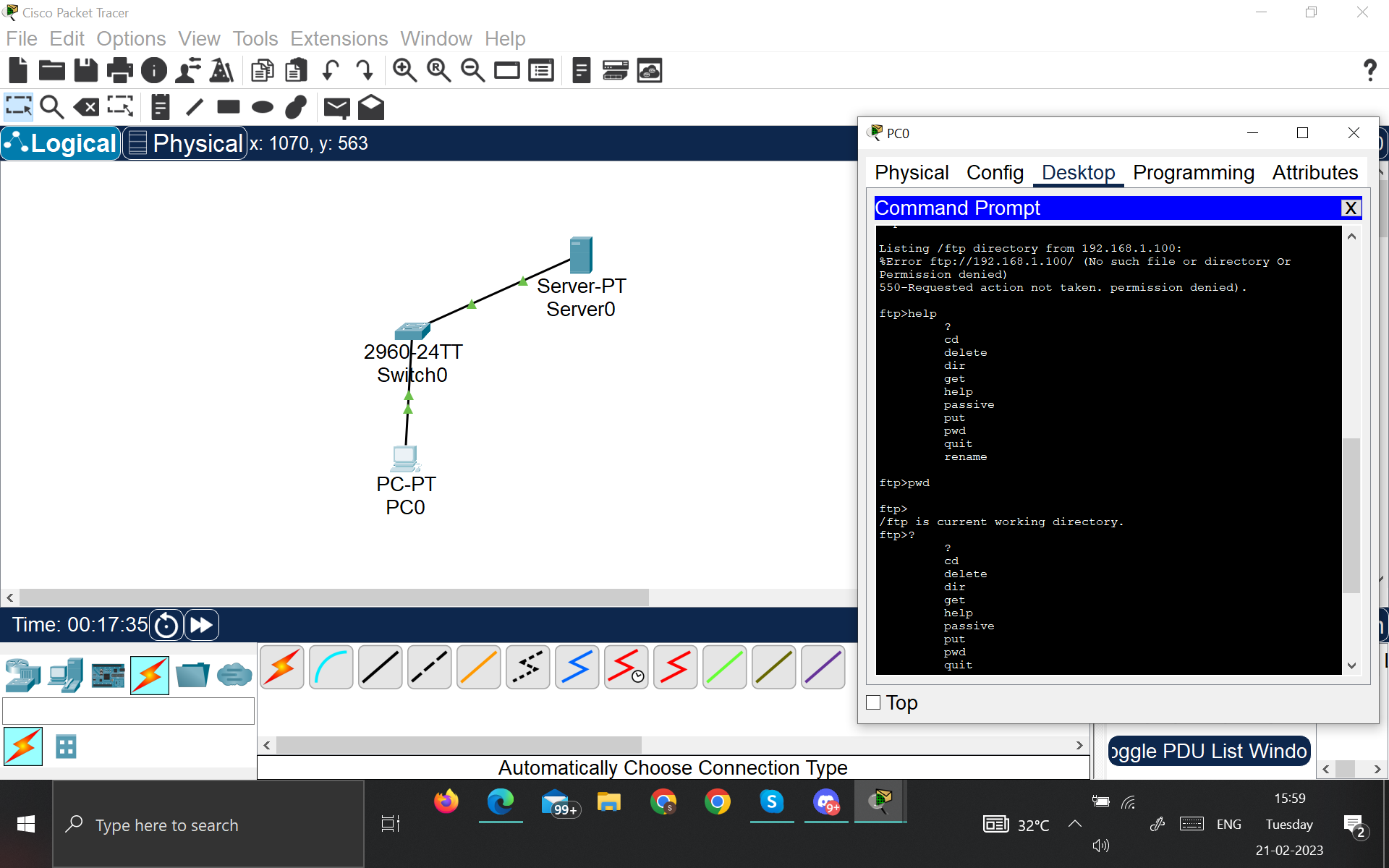
OPEN PC > DESKTOP > COMMAND PROMPT > FTP 192.168.1.100

FTP>

USERNAME:

PASSWORD:

FTP > HELP (LIST OF COMMANDS WILL BE DISPLAYED)



**SMTP-SIMPLE MAIL TRANSFER PROTOCOL**

SMTP IS A PROTOCOL USED TO SEND AND RECEIVE REPLY MAIL FROM THE SENDER AND RECEIVER.

**TODO:**

PACKET TRACER SETUP-SWITCH,2 PC'S (SENDER AND RECEIVER),SERVER(SMTP)

STEP 1:

OPEN SERVER > SERVICE TAB > SMTP SERVICE > TURN ON THE PORT

DOMAIN NAME: GMAIL.COM

USERNAME: ADMIN10 (SENDER)

PASSWORD: 1234

ADD > CLICK

USERNAME: USER12 (RECEIVER)

PASSWORD: 0011

ADD > CLICK

MAIL SERVER > DESKTOP > IP CONFIG 192.168.1.2 SM 255.255.255.0

STEP 2: OPEN SENDER PC

DESKTOP > EMAIL

USER INFO:

NAME: ADMIN10

GMAIL: ADMIN10@GMAIL.COM

SERVER INFO:

INCOMING: 192.168.1.2

OUTGOING: 192.168.1.2

LOG ON INFO:

USERNAME: ADMIN10

PASSWORD: 1234

STEP 3: REPEAT FOR RECEIVER PC

STEP 4: IP ASSIGNING FOR SENDER AND RECEIVER PC

**VERIFY:**

SENDER PC > EMAIL > COMPOSE > TO:

                                                     FROM:

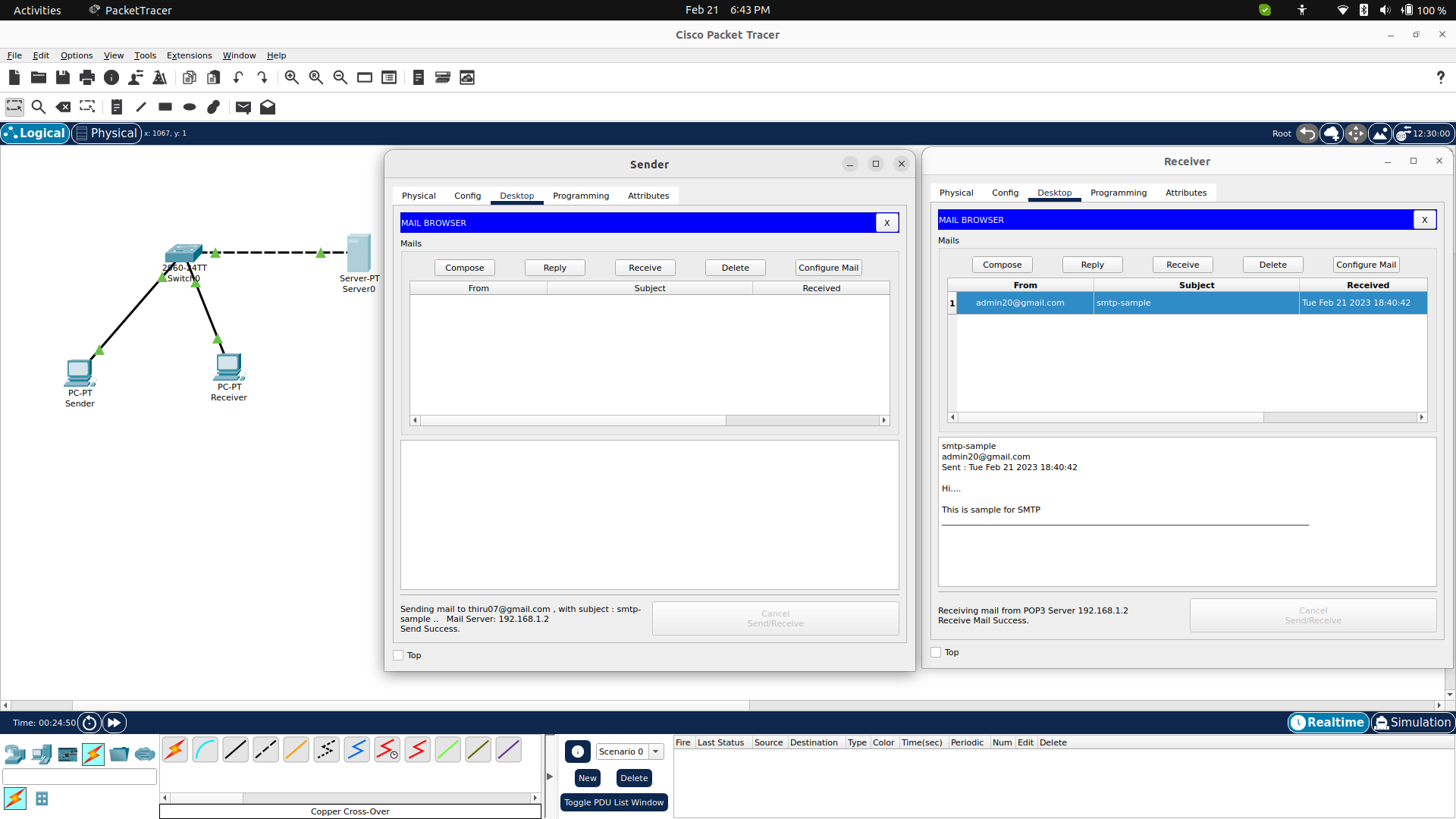
                               SUB:

COMPOSE AN EMAIL

SEND > CLICK

DIALOG BOX SHOWS MAIL HAS BEEN SENT SUCCESSFULLY !

OPEN RECEIVER PC > MAIL > MAIL RECEIVED WITH FROM, TO ,SUB



**SSH-SECURE SHELL**

* IT IS A PROTOCOL
* TO REMOTE LOGIN SECURELY
* IT IS A METHOD FOR SECURE REMOTE LOGIN FROM ONE COMPUTER TO ANOTHER COMPUTER, ROUTER
* IT PROVIDES STRONG AUTHENTICATION (username,password)
* IT ENCRYPTS THE COMMUNICATION WITH STRONG ENCRYPTION
* IN ADDITION, IT CREATES A SECURE CHANNEL BETWEEN LOCAL AND REMOTE COMPUTER
* SSH IS USED TO MANAGE ROUTERS,SERVERS,VIRTUAL PLATFORMS AND FILE TRANSFER APPLICATIONS

**TODO**

PT SETUP:

CONFIG STEPS:

OPEN ROUTER (1) > OPEN

CLI > EN

#CONF T

STEP 1:

#HOSTNAME ROUTER1

#INT GI/FA 0/0

#IP ADDRESS 192.168.1.1 255.255.255.0

#NO SHUTDOWN

#EXIT

STEP 2:

#IP DOMAIN NAME ABCD        //DOMAIN NAME HAS TO CREATED FOR IDENTIFICATION PURPOSE OF LAN

#CRYPTO KEY GENERATE RSA          // FOR STRONG AUTHENTICATION PURPOSE

BITS: 1024

STEP 3:

#IP SSH TIME-OUT 10                 //IF USER LOGINS REMOTELY, PASSWORD MUST BE ENTERED WITHIN 10 SECS

#IP SSH AUTHENTICATION-RETRIES 3     //USER CAN TRY TO REMOTE LOGIN (3 ATTEMPTS)-MAXIMUM 5 ATTEMPTS

#LINE VTY 0 4

#LOGIN LOCAL

#PRIVILEGE LEVEL 15               // FULL ACCESS TO ALL CONFIGURATION COMMANDS

#TRANSPORT INPUT SSH              //AFTER SSH CONFIG, THE ROUTER1 GIVES ACCESS TO THE PC AND LOCAL ROUTERS

#EXIT

STEP 4:

#USERNAME ADMIN PRIVILEGE 15 PASSWORD ADMIN@123     //USERNAME AND PASSWORD HAS TO BE CREATED FOR SECURITY PURPOSE

#END

#WR

STEP 5:

PC > DESKTOP > IP CONFIG

IP: 192.168.1.10

SM: 255.255.255.0

DG: 192.168.1.1

STEP 6:

OPEN ROUTER (2)

CONFIG > GI/FA 0/0 > ON

IP: 192.168.1.2

SM: 255.255.255.0

**VERIFY:**

1.PC > COMMAND PROMPT > SSH -L ADMIN 192.168.1.1

USERNAME:

PASSWORD:

ROUTER1 > EN

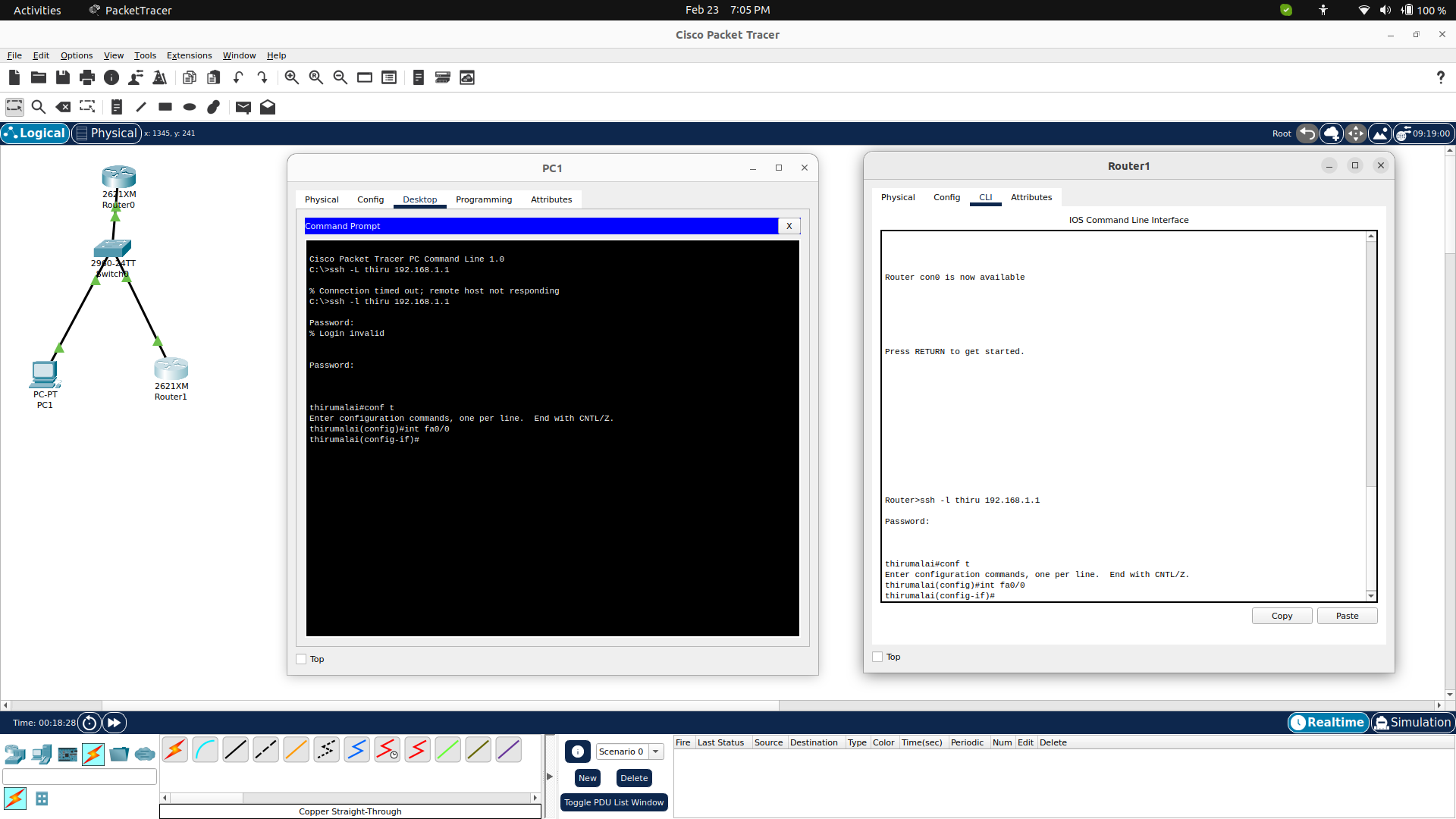
2.ROUTER (2) OPEN

CLI > SSH -L ADMIN 192.168.1.1

USERNAME:

PASSWORD:

ROUTER1 > EN



**SNMP-SIMPLE NETWORK MANAGEMENT PROTOCOL**

SNMP IS A PROTOCOL WHICH IS USED TO MONITOR THE NETWORK, WE CAN GET INFORMATION LIKE NAME,INTERFACES OF NETWORK DEVICES ETC..,

AND ALSO YOU CAN SET THE INFORMATION USING THE GET AND SET REQUEST WITH USING MIB (MANAGEMENT INFORMATION BASE)

1)ADD A NEW NETWORK TO ROUTER

2)ADD ADDITIONAL SLOTS TO THE ROUTER IF NECESSARY

3)ASSIGN THE IP ADDRESS TO THE PORTS OF ROUTER.

4)GET THE INFORMATION OF THE REMOTE SYSTEM USING GETREQ,ATTRIBUTE FOR THE SAME IS NEW HOST NAME

BEFORE GOING TO GET/SET INFORMATION, WE NEED TO CONFIGURE ROUTER WITH SNMP COMMUNITY

SNMP MANAGER: WHO MONITORS THE NETWORK DEVICES (LAPTOP)

SNMP AGENT: WHO PROVIDE YOU THE NETWORK (ROUTERS,SWITCHES,SERVERS)

**CONFIG STEPS:**

OPEN ROUTER> CLI

>EN

#CONF T

#SNMP-SERVER COMMUNITY ADMIN RO

#SNMP-SERVER COMMUNITY ADMIN RW

#EXIT

SELECT MIB BROWSER FROM ANY ONE OF THE SNMP MANAGER FOR GETTING/SETTING INFORMATION OF HOSTNAME OF ROUTER.

OPEN MIB IN PC

TYPE IP ADDRESS OF ROUTER - 192.168.2.1

PASSWORD: ADMIN

SNMP: V1

MIB TREE > CLICK > SYSTEM NAME > GET > GO

WE GOT INFO OF HOSTNAME AS ROUTER WITH THE OCTET STRING

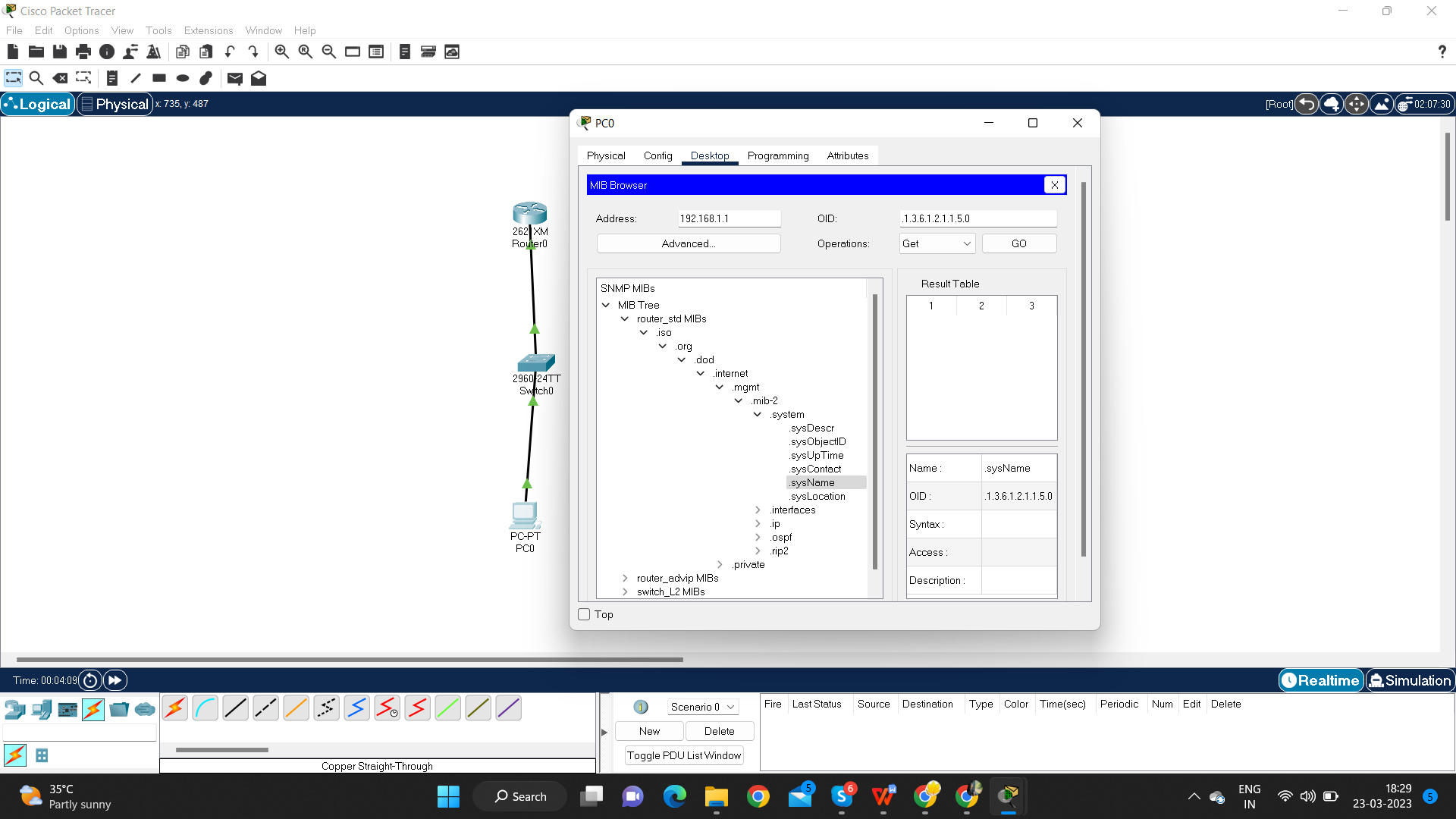
NEXT, SET ROUTER NAME AS ADMIN ROUTER

CHOOSE AS SET,CHOOSE OCTET STRING

VALUE: ADMIN ROUTER > CLICK OK

**VERIFY:**

LOGIN TO ROUTER> YOU CAN SEE THE HOSTNAME HAS BEEN CHANGED



**FIREWALL**

Security Device - Both Hardware & Software

Implements all the configurations of Router & Switch.

1. HARDWARE FIREWALL MANUFACTURERS

2. STATEFUL & STATELESS FIREWALL

3. CISCO ASA FIREWALL

4. CISCO ASA MODELS

5. FIREWALL RULES

6. KEY POINTS OF CISCO ASA

7. CONFIGURATION STEPS

**1. HARDWARE FIREWALLS MANUFACTURERS**

Different Firewall manufacturers are as follows

-Check Point.

-FortiGate.

-Palo Alto Networks.

-WatchGuard.

-Seqrite Firewall.

-Cisco Asa Firepower.

-Cisco PIX.

-Mcafee Firewall.

**2. STATEFUL & STATELESS FIREWALL**

Stateful firewalls are capable of monitoring and detecting states of all traffic on a network to track and defend based on traffic patterns and flows.

Stateless firewalls, however, only focus on individual packets, using preset rules to filter traffic.

**3.CISCO ASA FIREWALL**

ASA - Adaptive Security Appliance

-Cisco ASA is a security device that combines firewall, antivirus, intrusion

prevention, virtual private network (VPN) & SSL capabilities.

**4.CISCO ASA MODELS**

ASA models are all in the 5500 series

The ASA 5500 series has the following models:

Cisco ASA 5505 // We will configure this in Packet Tracer

Cisco ASA 5510

Cisco ASA 5520

Cisco ASA 5525-X

Cisco ASA 5540

Cisco ASA 5550

Cisco ASA 5580-20

Cisco ASA 5580-40

**5.FIREWALL RULES**

- Inbound Rules

- Outbound Rules

**6.KEY POINTS OF CISCO ASA**

1. We can't assign ip directly to any interface of a firewall

2. we have to assign ip to the vlan and then link the vlan to any interface.

so the ip gets indirectly assigned to the interface

3. INSIDE network is inside ur LAN

4. OUTSIDE network will be out of LAN

5. VLAN 1 will always be linked with INSIDE network

6. VLAN 2 will always be linked with OUTSIDE network

7. Security level of the INSIDE network will be 100 and OUTSIDE will be 0

8. Ethernet 0/1 of firewall will be assigned to VLAN 1

9. Ethernet 0/0 of firewall will be assigned to VLAN 2

**7. CONFIGURATION STEPS**

STEPS TO CONFIGURE FIREWALL

STEP 1 - REMOVE DEFAULT IP ADDRESS AND DHCP SCOPE RANGE

STEP 2 - ASSIGN IP,NAME AND SECURITY LEVEL TO VLAN 1 & 2

STEP 3 - LINK CORRESPONDING VLAN 1 & 2 WITH THE RESPECTIVE INTERFACE

STEP 4 - CONFIGURE DHCP & DNS SERVER

STEP 5 - CONFIGURE DEFAULT ROUTE

STEP 6 - OBJECT NETWORK CREATION & ENABLING NAT

STEP 7 - CREATE ACCESS CONTROL LIST

---------------------------------------------------------

STEP 1 - REMOVE DEFAULT IP ADDRESS AND DHCP SCOPE RANGE

ciscoasa(config)#interface vlan 1

ciscoasa(config-if)#no ip address

ciscoasa(config-if)#exit

ciscoasa(config)#no dhcpd address 192.168.1.5-192.168.1.35 inside

(We can find this using SHOW command

SHOW RUNNING-CONFIG)

------------------------------------------------------------

STEP 2 - ASSIGN IP,NAME AND SECURITY LEVEL TO VLAN 1 & 2

ciscoasa(config)#interface vlan 1

ciscoasa(config-if)#ip address 172.16.1.1 255.255.0.0

ciscoasa(config-if)#no shutdown

ciscoasa(config-if)#nameif inside

ciscoasa(config-if)#security-level 100

ciscoasa(config-if)#exit

ciscoasa(config)#interface vlan 2

ciscoasa(config-if)#ip address 210.2.2.2 255.255.255.0

ciscoasa(config-if)#no shutdown

ciscoasa(config-if)#nameif outside

ciscoasa(config-if)#security-level 0

ciscoasa(config-if)#exit

----------------------------------------------------------------

STEP 3 - LINK CORRESPONDING VLAN 1 & 2 WITH THE RESPECTIVE INTERFACE

ciscoasa(config)#interface ethernet 0/1

ciscoasa(config-if)#switchport access vlan 1

ciscoasa(config-if)#exit

ciscoasa(config)#interface ethernet 0/0

ciscoasa(config-if)#switchport access vlan 2

ciscoasa(config-if)#exit

----------------------------------------------------------------

STEP 4 - CONFIGURE DHCP & DNS SERVER

we can give dhcp range as much as we want, here we give 6 ip's

starting from 1.5 to 1.10

ciscoasa(config)#dhcpd address **172.16.1**.3-**172.16.1**.30 inside

ciscoasa(config)#dhcpd dns 20.20.20.2 interface inside

The above command allows all the computer from inside network to communicate with the DNS server

----------------------------------------------------------------

STEP 5 - CONFIGURE DEFAULT ROUTE

The command will let the firewall communicate with the outside network. 0.0.0.0

means any source ip can communicate with any destination ip through router ip

210.2.2.1

ciscoasa(config)#route outside 0.0.0.0 0.0.0.0 210.2.2.1

----------------------------------------------------------------

STEP 6 - OBJECT NETWORK CREATION & ENABLING NAT

This will allow the INSIDE network to communicate with OUTSIDE network (& vice

versa) with the public ip address

ciscoasa(config)#object network LAN

ciscoasa(config-network-object)#subnet 172.16.1.0 255.255.0.0

ciscoasa(config-network-object)#nat (inside,outside) dynamic interface

----------------------------------------------------------------

STEP 7 - CREATE ACCESS CONTROL LISTThis is the EXTENDED NAMED ACL (3rd type of ACL, apart from Standard &

extended ACL) where we use Alphabets instead of Number.

This ACL will allow both TCP and ICMP traffic to be allowed in outside network

ciscoasa(config)#access-list inside\_to\_internet extended permit tcp any any

ciscoasa(config)#access-list inside\_to\_internet extended permit icmp any any

ciscoasa(config)#access-group inside\_to\_internet in interface outside

----------------------------------------------------------------

STEP 8 - STEPS TO CONFIGURE ROUTER

ASSIGN IP ADDRESS TO ROUTER

Configure OSPF for ISP Router

Router(config)#router ospf 1

Router(config-router)#network 210.2.2.0 0.0.0.255 area 0

Router(config-router)#network 20.20.20.0 0.0.0.255 area 0

----------------------------------------------------------------

**VERIFY**

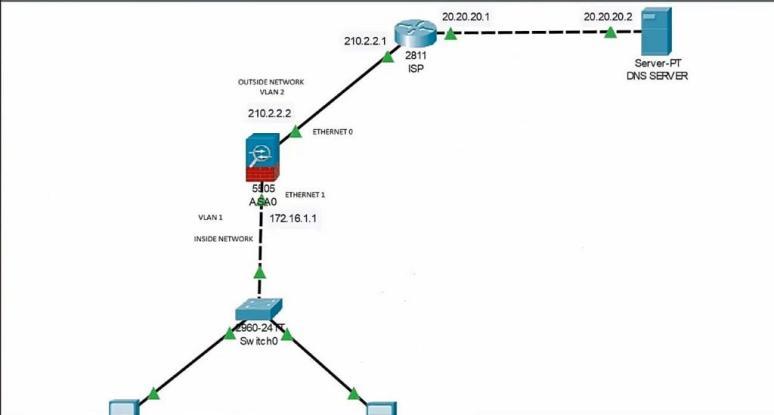
1.Change ip of computers from inside network to Dynamic

2.Ip should be automatically assigned by firewall.

Ex: 172.16.1.5

3. Now ping from 172.16.1.5 to 20.20.20.2 (DNS Server)

we should get a reply.



**DOMAIN NAME SERVER/SYSTEM**

ABC.COM-3.2.6.7

FB.COM-8.7.9.10

Domain Name System (DNS) is an Internet service that translates domain names (e.g., its.umich.edu)

into IP addresses. Dynamic Host Configuration Protocol (DHCP) is a protocol for automatically assigning

IP addresses and other configurations to devices when they connect to a network.

DNS CACHE STORED IN C: /WIN/SYS32/DRIVERS/ETC/HOSTS-OPEN WITH NOTEPAD.

**DHCP-DYNAMIC HOST CONFIGURATION PROTOCOL**

DHCP USED FOR MANAGING IP USAGE & CLIENT IP ALLOCATION

DORA PROCESS-DISCOVER,OFFER,REQUEST,ACKNOWLEDGEMENT

**KEY TERMS:**

1.DHCP SCOPE RANGE **>** IP RANGE - 192.168.1.2 TO 192.168.1.202

2.LEAST TIME **>** NO.OF HOURS.

This is the length of time that the client can use the IP address it has been assigned. The duration of the lease time can be changed according to your specific requirement.

WIRED-8 DAYS

WIRELESS-24 HOURS

3.CLIENT TABLE

STORES IP ADDRESS,MAC ADDRESS,CLIENT NAME,LEAST TIME

**DNS CONFIGURATION TODO:**

TO DO THIS, CLICK ON THE SERVER, THEN CLICK ON SERVICES TAB, CLICK ON DNS SERVER FROM THE MENU. FIRST TURN ON THE

DNS SERVICE, THEN DEFINE NAMES OF THE HOSTS AND THEIR CORRESPONDING IP ADDRESS.

FOR EG: TO SPECIFY THE DNS ENTRY FOR PC0:

IN THE NAME AND ADDRESS FIELDS TYPE:

NAME: PC0

ADDRESS: 192.168.1.3

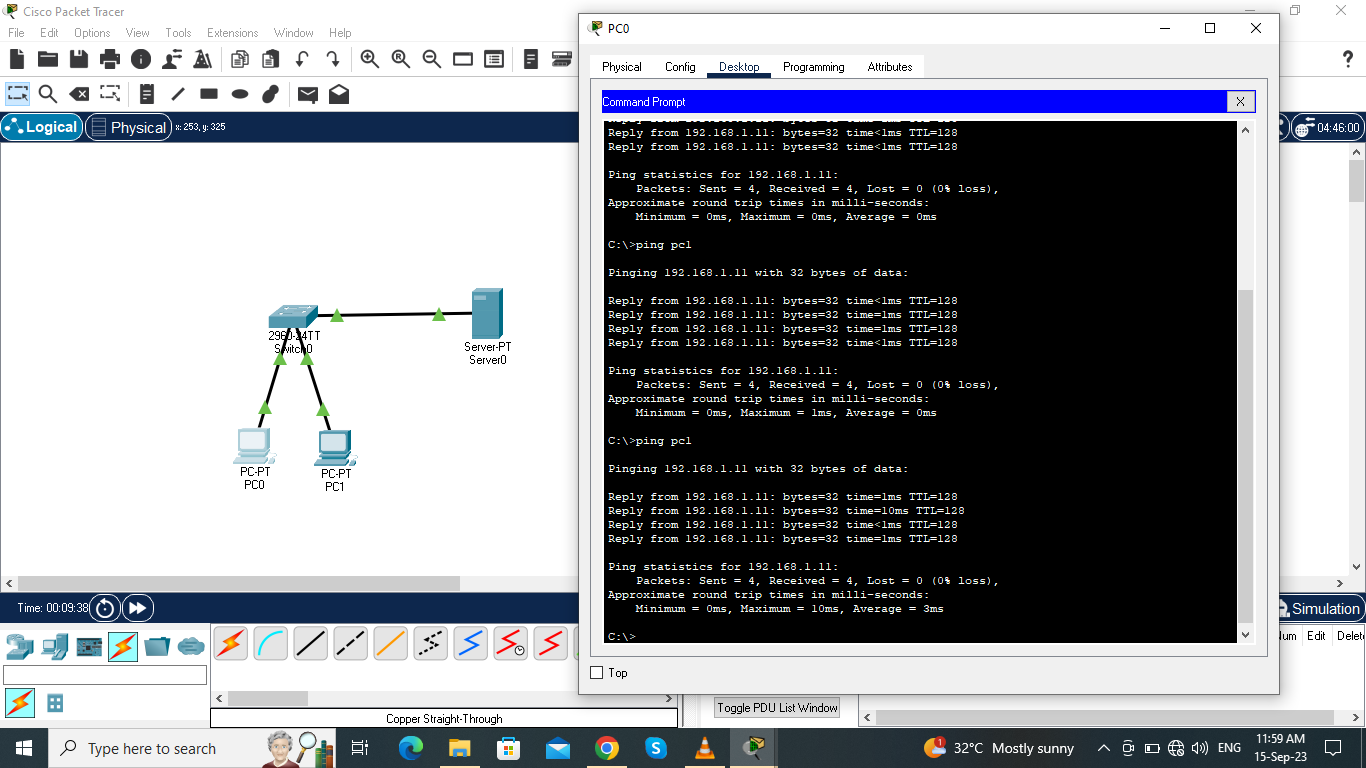
CLICK ON ADD THEN SAVE, REPEAT THIS FOR THE PC1 AND THE SERVER

ONCE YOUR DONE, YOUR DNS ENTRIES WILL LOOK LIKE THIS:

FINALLY, TEST DOMAIN NAME-IP RESOLUTION, PING THE HOSTS FROM ONE ANOTHER USING THEIR NAMES INSTEAD OF THEIR IP ADDRESS, IF THE DNS SERVICE IS TURNED ON AND ALL IP CONFIGURATIONS ARE OKAY, THEN PING SHOULD WORK.

**VERIFY:**

PING PC1 FROM PC0,PING SHOULD BE SUCCESSFUL.



**DNS RECORDS:**

The main job of DNS is to resolve domain names into IP addresses and the reason it has to do this is because pc’s don’t understand names, they understand numbers only. A domain name is just a text that you type in a web browser when you want to go to a certain website such as example.com, google.com and so on. So when you type a name as example.com, google.com in a browser, DNS will resolve that domain name into an IP address so you can retrieve the website.

Now in a DNS hierarchy there are three levels of servers. There are

**\*Root servers**

**\*Top level domain servers**

**\*Name servers**

But of these three DNS servers that are responsible for storing DNS records for resolving domain names to IP addresses. They know everything about domain name, including IP addresses and much more. But for your query to resolve example.com into an ip address, it needs to know which name server to ask?

Example.com goes to root server and will forward the query to the correct top level domain server. Top level domain server is responsible for info of top level domains, such as .com, .net, .org and so on. And once the query reaches the Name server, example.com will be resolved to the ip addresses so the website can be retrieved. So in a DNS database you have what’s called a DNS zone file. Zone file contains the DNS records. Now there are numerous DNS records.

**1. A RECORD:**

**TYPE NAME IP ADDRESS TTL**

**A EXAMPLE.COM 12.17.14.148 7200**

The “A” record resolves domain names into IPV4 addresses. IPV4 consists of 32 bits.

**2.AAAA RECORD:**

**TYPE NAME IP ADDRESS TTL**

**AAAA EXAMPLE.COM 2501:0:53b::3330:C2f4 7200**

The “AAAA” is just like the A record. So, both A and quad A records resolve domain names to ip addresses. But the difference is that quad A records resolve domain names to Ipv6 addresses (replaces ipv4 addresses).

**3.CNAME RECORD:**

**TYPE NAME ALIAS TO TTL**

**CNAME** [**WWW.EXAMPLE.COM**](http://www.example.com) **EXAMPLE.COM 7200**

The “CNAME” or canonical name resolves a domain or subdomain to another domain name. So basically, it’s an alias for another domain name. Computer reads domain name from right to left example.com. Domain name will have several parts: a root domain, a top level domain, second level, and a subdomain

**www .example .com .**

**subdomain second level top level root domain**

**4.MX RECORDS:**

**TYPE PRIORITY NAME HOST TTL**

**MX 10 EXAMPLE.COM MAIL1EXAMPLE.COM 7200**

**MX 20 EXAMPLE.COM MAIL2EXAMPLE.COM 7200**

The “MX” (Mail exchanger) simply points to the server where emails should be delivered for that domain. Your MTA (Mail Transfer Agent) will query the MX records for example.com because it’s looking for an email server. It will respond back telling the MTA which server to send the email to which in this case would be mail1.example.com because that is what the MX records points to.

MX records has two email servers along with priority numbers. The lower the priority number means that’s the primary email server. But if the primary mail server gets overwhelmed or goes down, then the secondary email server would be used.

**5.SOA RECORDS:**

**TYPE NAME RNAME SERIAL # RETRY TTL**

**SOA ns1.example.com admin.example 510025 60 7200**

**.com**

The “SOA” record stores administrative information about a DNS zone. A DNS zone is a section of domain name space that a certain administrator has been delegated control over. DNS zones allow a domain name-space such as example.com to be divided into a different section. So, if we look at the domain example.com. If this domain was broken down into three sections or subdomains such as shop.example.com, blog.example.com and support.example.com

Each domain has computers. The shop.example.com and blog.example.com has small no. of computers so therefore it is considered as DNS zone 1 and the support.example.com considered to be DNS zone 2. The head admin could create one zone of three two subdomains and assign their own DNS zone file which contains an SOA record. So here is an example of a SOA record.

**DNS QUERIES:**

**RECURSIVE QUERY AND ITERATIVE QUERY:**

The goal of DNS is to resolve a fully qualified domain name (FQDN) to an Ip address. The process is called Name Resolution.

The recursive query demands a name resolution or the answer would be: “it can’t be found”. The recursive query is between a DNS client and it’s local DNS server.On the other hand, the iterative query is between a local DNS server and other DNS servers.The iterative query does not demand a name resolution, which means other DNS servers may provide a name resolution if they know or simply respond with a referral. Suppose, I want to go to the google web server([www.google.com](http://www.google.com/))

Web browser will check two places. First to see if there is any previous name resolution record of this google machine. One is my computer’s cache memory. The other place is a simple text file called**: Hosts.** Suppose, there is no record in either of these two locations. My computer would ask my local DNS servers.

This initial query from my computer, a DNS client to my local DNS server is a recursive query. My computer demands a clear answer. To resolve a name is the responsibility of my local DNS server. Let us assume that my local DNS server is a brand new machine and it has no records of any IP address of www.google.com . It would say: “I’m sorry, I don’t know. But I will find it for you. It is my job”. Now the iterative query starts: During the iterative query, the other DNS servers can simply provide a referral if they do not know the requested Ip address. My local DNS server is looking for an Ip address of google web server.

First, my local server will go up to a root domain name server and ask: “what is the Ip address of [www.google.com](http://www.google.com/)?” The root domain servers are only responsible for top level domain (TLD) servers, such as .com, .edu, .org etc.., and thus the root server would reply: “I don’t know Ip of google.com but I know Ip address of .com address!”. Here the root domain server gives a referral. Then my local DNS server goes to the .com server asking the exact same question. The .com server would reply: “I do not know the IP address of this google web server, but I do know an Ip address of a google DNS server. It finds the google DNS server, and asks the same question again. At the same time my computer saves this IP address in its cache memory just in case it will use it again. So does my local DNS server. It saves this IP address in its memory. Next time when any other computer in the network asks the same question, it would give this Ip address directly from its memory without going through all those repetitive steps I mentioned above.

A DNS recursive query is between a DNS client and its local DNS server. The local DNS server is responsible for answering questions from its DNS clients. When this local DNS server could not resolve a new name from its own database, it would make an iterative query to another DNS server.

**REVERSE DNS:**

Reverse DNS (RDNS), also known as reverse domain name system, is a process that involves mapping ip addresses back to domain names. In contrast to the standard DNS, which translates domain names to IP addresses, reverse DNS helps identify the domain name associated with a given IP address.

Reverse DNS server multiple purposes including network. Most commonly used for network diagnostics , security checks, spam filtering.

A Reverse DNS lookup is a DNS query for the domain name associated with a given IP address. This accomplishes the opposite of which the DNS system is queried to return an IP address.

**How does reverse DNS work?**

Reverse DNS query DNS servers for a PTR (Pointer) record, if the server does not have a ptr record, it cannot resolve a reverse lookup. PTR records store IP addresses with their segments reversed, and they append “.in-addr.arpa” to that. For example, if a domain has an IP address of 192.0.2.1, the ptr record will store the domain's information under 1.2.0.192 in-addr.arpa.

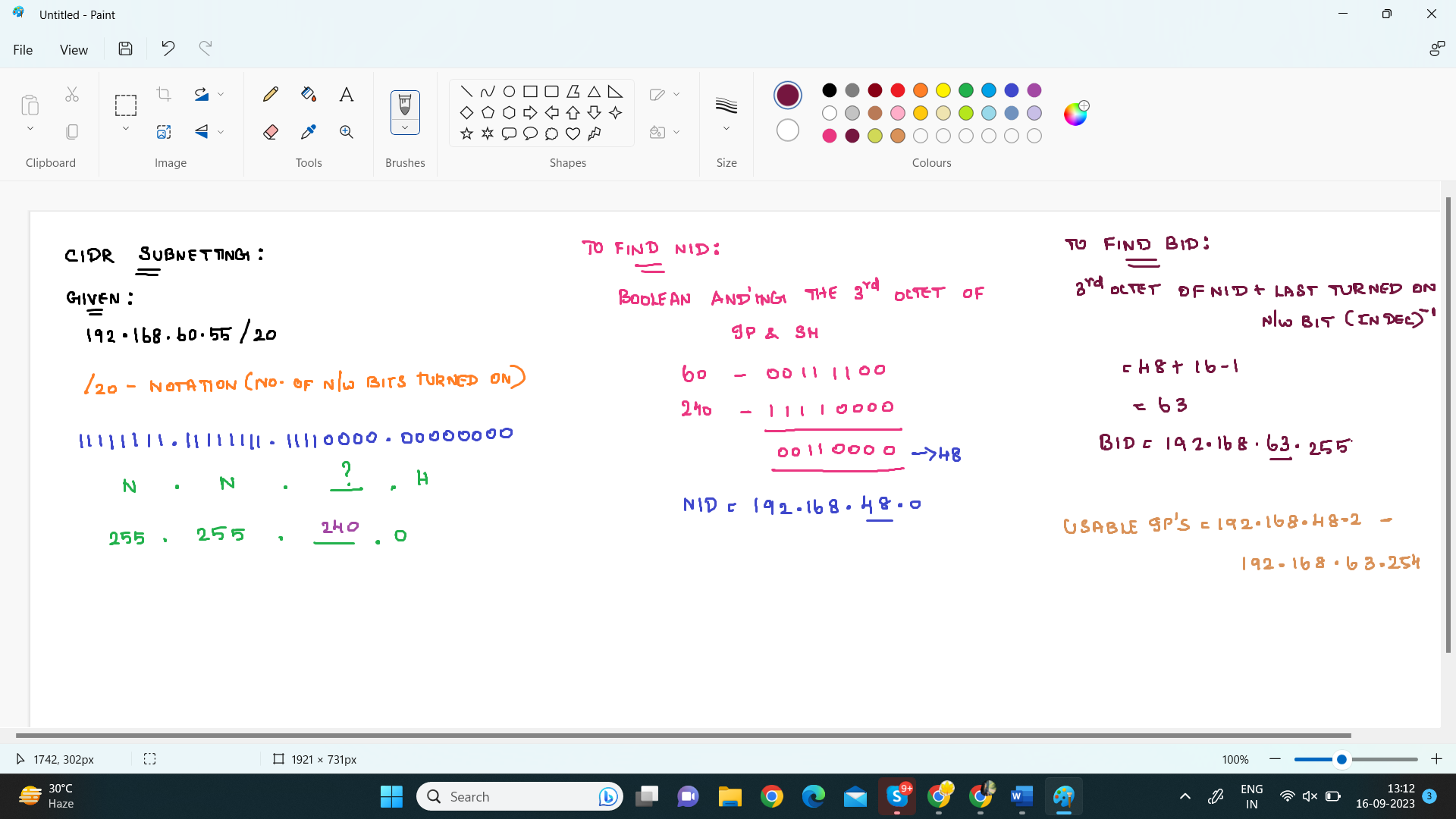
In IPV6, the latest version of the internet protocol, PTR records are stored within the “ipv6.arpa” domain instead of “.in-addr.arpa”.

**What are reverse DNS lookups used for?**

Reverse DNS used by email servers, email servers check and see if an email message came from a valid server before bringing it on their network. Many email servers will reject messages from any server that does not support reverse lookups or from a server that is highly unlikely to be legitimate, spammers often use IP addresses from hijacked machines, which means there will be no PTR record. Or they may use dynamically assigned IP addresses that lead to server domains with highly generic names.

Logging softwares also employs reverse lookups in order to provide users with human-readable domains in their log data as opposed to a bunch of numeric IP addresses.

**CIDR - CLASSLESS INTER DOMAIN ROUTING:**

****