MINI-PROJECT

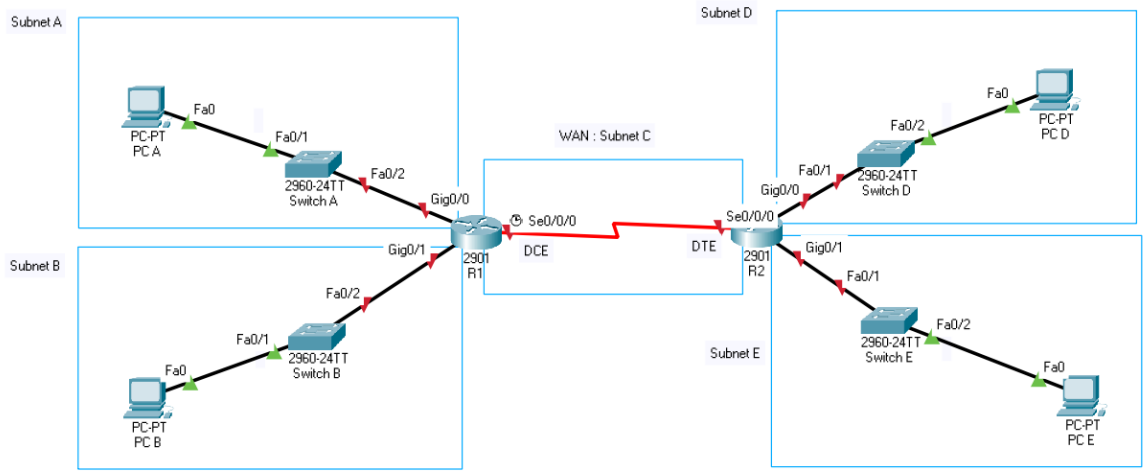
Name: Chinnu Raju Raju Ilamaran / Course: Electronics and computer engineering

Date:17/6/2024

Table of Contents

Introduction

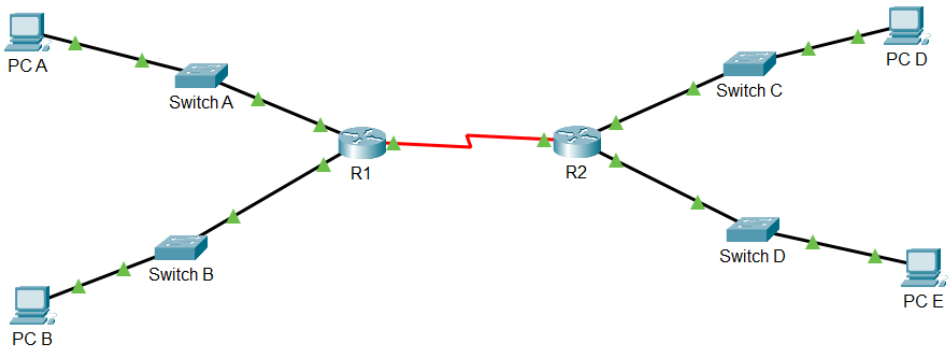
You are a Network Engineer in a small-medium sized enterprise company. Your company is implementing a wired network that can support growth over the next five years. Setup and configure the network using packet tracer to verify its connectivity. Your manager has given you the following topology and requirements for the company network.



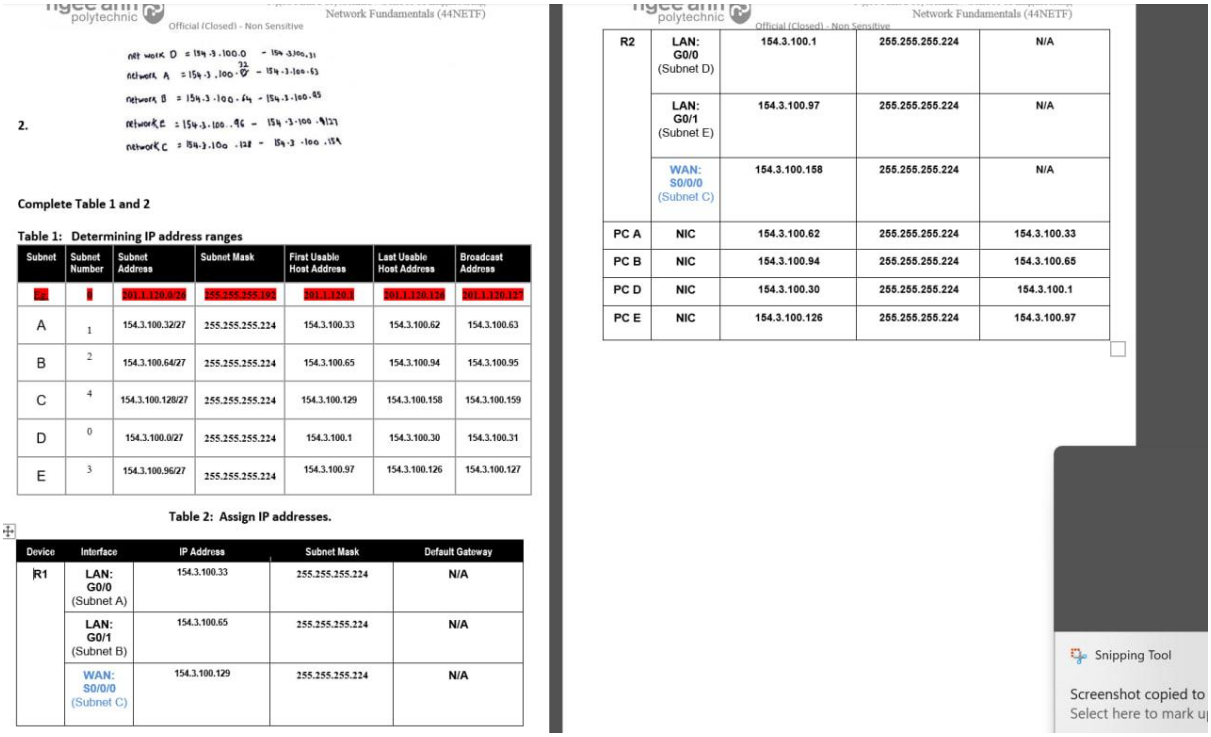
The company has the following requirements:

Subnet A (LAN)	11 IP addresses (usable)
Subnet B (LAN)	8 IP addresses (usable)
Subnet C (WAN connection)	2 IP addresses (usable)
Subnet D (LAN)	24 IP addresses (usable)

Network Design



The Fixed Length Subnet Mask (FLSM) subnetting approach, also known as traditional or classical subnetting, involves dividing an IP address space into subnets of equal size. Each subnet has the same number of addresses, and the subnet mask is the same for all subnets.



2.

Complete Table 1 and 2

Table 1: Determining IP address ranges

Subnet	Subnet Number	Subnet Address	Subnet Mask	First Usable Host Address	Last Usable Host Address	Broadcast Address
[illegible]	[illegible]	201.1.120.0/26	255.255.255.192	201.1.120.1	201.1.120.126	201.1.120.127
A	1	154.3.100.32/27	255.255.255.224	154.3.100.33	154.3.100.62	154.3.100.63
B	2	154.3.100.64/27	255.255.255.224	154.3.100.65	154.3.100.94	154.3.100.95
C	4	154.3.100.128/27	255.255.255.224	154.3.100.129	154.3.100.158	154.3.100.159
D	0	154.3.100.0/27	255.255.255.224	154.3.100.1	154.3.100.30	154.3.100.31
E	3	154.3.100.96/27	255.255.255.224	154.3.100.97	154.3.100.126	154.3.100.127

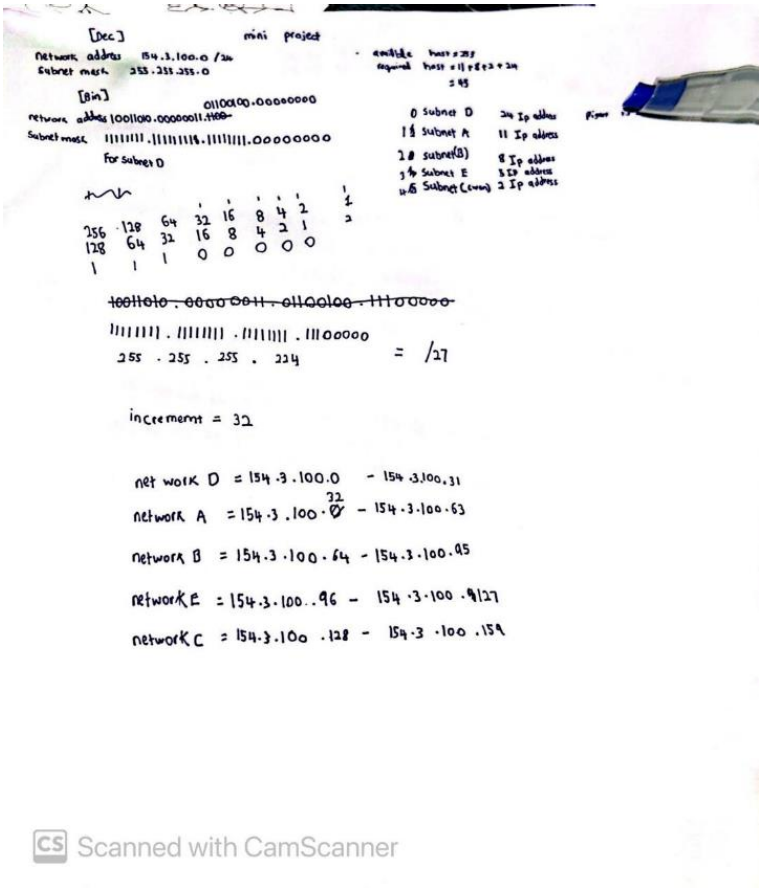
Table 2: Assign IP addresses.

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	LAN: G0/0 (Subnet A)	154.3.100.33	255.255.255.224	N/A
	LAN: G0/1 (Subnet B)	154.3.100.65	255.255.255.224	N/A
	WAN: S0/0/0 (Subnet C)	154.3.100.129	255.255.255.224	N/A
R2	LAN: G0/0 (Subnet D)	154.3.100.1	255.255.255.224	N/A
	LAN: G0/1 (Subnet E)	154.3.100.97	255.255.255.224	N/A
	WAN: S0/0/0 (Subnet C)	154.3.100.158	255.255.255.224	N/A
PC A	NIC	154.3.100.62	255.255.255.224	154.3.100.33
PC B	NIC	154.3.100.94	255.255.255.224	154.3.100.65
PC D	NIC	154.3.100.30	255.255.255.224	154.3.100.1
PC E	NIC	154.3.100.126	255.255.255.224	154.3.100.97

Snipping Tool

Screenshot copied to

Select here to mark u



Configuration

R1:	**R2:**
Router>enable	Router>enable
Router(config)#**hostname R1**	Router(config)#**hostname R2**
R1(config)#**no ip domain-lookup**	R2(config)#**no ip domain-lookup**
R1(config)#int g0/0	R2(config)#int g0/0
R1(config-if)#**ip address 154.3.100.33 255.255.255.224**	R2(config-if)#**ip address 154.3.100.1 255.255.255.224**
R1(config-if)#no shutdown	R2(config-if)#no shutdown
R1(config-if)#exit	R2(config-if)#exit

R1(config)#int g0/1	R2(config)#int g0/1
R1(config-if)#**ip address 154.3.100.65 255.255.255.224**	R2(config-if)#**ip address 154.3.100.97 255.255.255.224**
R1(config-if)#no shut	R2(config-if)#no shut
R1(config-if)#exit	R2(config-if)#exit
R1(config)#**int s0/0/0**	R2(config)#**int s0/0/0**
R1(config-if)#**ip address 154.3.100.129 255.255.255.224**	R2(config-if)#**ip address 154.3.100.158 255.255.255.224**
R1(config-if)#**clock rate 128000**	R2(config-if)#no shut
R1(config-if)#no shut	R2(config-if)#exit
R1(config-if)#exit	R2(config)# **ip route 154.3.100.32 255.255.255.224 154.3.100.129** R2(config)# **ip route 154.3.100.64 255.255.255.224 154.3.100.129**
R1(config)# **ip route 154.3.100.0 255.255.255.224 154.3.100.158** R1(config)# **ip route 154.3.100.96 255.255.255.224 154.3.100.158**	R2(config)#exit
R1(config)#exit	R2# copy running-config startup-config

R1# copy running-config startup-config

Testing and Analysis

Ping test

```
C:\>ping 154.3.100.62

Pinging 154.3.100.62 with 32 bytes of data:

Reply from 154.3.100.62: bytes=32 time=2ms TTL=128
Reply from 154.3.100.62: bytes=32 time=4ms TTL=128
Reply from 154.3.100.62: bytes=32 time=4ms TTL=128
Reply from 154.3.100.62: bytes=32 time=4ms TTL=128

Ping statistics for 154.3.100.62:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 4ms, Average = 3ms

C:\>ping 154.3.100.126

Pinging 154.3.100.126 with 32 bytes of data:

Reply from 154.3.100.126: bytes=32 time=44ms TTL=126
Reply from 154.3.100.126: bytes=32 time=46ms TTL=126
Reply from 154.3.100.126: bytes=32 time=45ms TTL=126
Reply from 154.3.100.126: bytes=32 time=37ms TTL=126

Ping statistics for 154.3.100.126:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 37ms, Maximum = 46ms, Average = 43ms

C:\>ping 154.3.100.30

Pinging 154.3.100.30 with 32 bytes of data:

Reply from 154.3.100.30: bytes=32 time=36ms TTL=126
Reply from 154.3.100.30: bytes=32 time=52ms TTL=126
Reply from 154.3.100.30: bytes=32 time=37ms TTL=126
Reply from 154.3.100.30: bytes=32 time=31ms TTL=126

Ping statistics for 154.3.100.30:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 31ms, Maximum = 52ms, Average = 39ms

C:\>ping 154.3.100.94

Pinging 154.3.100.94 with 32 bytes of data:

Reply from 154.3.100.94: bytes=32 time<1ms TTL=127
Reply from 154.3.100.94: bytes=32 time<1ms TTL=127
Reply from 154.3.100.94: bytes=32 time<1ms TTL=127
Reply from 154.3.100.94: bytes=32 time<1ms TTL=127

Ping statistics for 154.3.100.94:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Ip route

```
Gateway of last resort is not set

     154.3.0.0/16 is variably subnetted, 8 subnets, 2 masks
C       154.3.100.0/27 is directly connected, GigabitEthernet0/0
L       154.3.100.1/32 is directly connected, GigabitEthernet0/0
C       154.3.100.32/27 is directly connected, GigabitEthernet0/1
L       154.3.100.33/32 is directly connected, GigabitEthernet0/1
C       154.3.100.64/27 is directly connected, Serial0/0/0
L       154.3.100.65/32 is directly connected, Serial0/0/0
S       154.3.100.96/27 [1/0] via 154.3.100.94
S       154.3.100.128/27 [1/0] via 154.3.100.94

R1#
```

```
Gateway of last resort is not set

     154.3.0.0/16 is variably subnetted, 8 subnets, 2 masks
S       154.3.100.0/27 [1/0] via 154.3.100.65
S       154.3.100.32/27 [1/0] via 154.3.100.65
C       154.3.100.64/27 is directly connected, Serial0/0/0
L       154.3.100.94/32 is directly connected, Serial0/0/0
C       154.3.100.96/27 is directly connected, GigabitEthernet0/0
L       154.3.100.97/32 is directly connected, GigabitEthernet0/0
C       154.3.100.128/27 is directly connected, GigabitEthernet0/1
L       154.3.100.129/32 is directly connected, GigabitEthernet0/1

R2#
```

Ip int brief

```
R1#show ip int br
R1#show ip int brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     154.3.100.33    YES manual up                    up
GigabitEthernet0/1     154.3.100.65    YES manual up                    up
GigabitEthernet0/2     unassigned      YES unset  administratively down down
Serial0/0/0            154.3.100.129   YES manual up                    up
Serial0/0/1            unassigned      YES unset  administratively down down
Vlan1                  unassigned      YES unset  administratively down down
R1#
```

```
R2#show ip int br
R2#show ip int brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     154.3.100.1     YES manual up                    up
GigabitEthernet0/1     154.3.100.97    YES manual up                    up
GigabitEthernet0/2     unassigned      YES unset  administratively down down
Serial0/0/0            154.3.100.158   YES manual up                    up
Serial0/0/1            unassigned      YES unset  administratively down down
Vlan1                  unassigned      YES unset  administratively down down
R2#
```

Ip config

PC A

```
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::240:BFF:FE9A:388A
   IPv6 Address.....: ::
   IPv4 Address.....: 154.3.100.62
   Subnet Mask.....: 255.255.255.224
   Default Gateway.....: ::
                         154.3.100.33

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: ::
   IPv6 Address.....: ::
   IPv4 Address.....: 0.0.0.0
   Subnet Mask.....: 0.0.0.0
   Default Gateway.....: ::
                         0.0.0.0
```

PC B

Physical Config Desktop Programming Attributes

Command Prompt

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::202:16FF:FE12:73D9
   IPv6 Address.....: ::
   IPv4 Address.....: 154.3.100.94
   Subnet Mask.....: 255.255.255.224
   Default Gateway.....: ::
                         154.3.100.65

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: ::
   IPv6 Address.....: ::
   IPv4 Address.....: 0.0.0.0
   Subnet Mask.....: 0.0.0.0
   Default Gateway.....: ::
                         0.0.0.0

C:\>
```

PC D

Physical Config Desktop Programming Attributes

Command Prompt

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::20D:BDFF:FEE3:30EA
   IPv6 Address.....: ::
   IPv4 Address.....: 154.3.100.30
   Subnet Mask.....: 255.255.255.224
   Default Gateway.....: ::
                         154.3.100.1

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: ::
   IPv6 Address.....: ::
   IPv4 Address.....: 0.0.0.0
   Subnet Mask.....: 0.0.0.0
   Default Gateway.....: ::
                         0.0.0.0

C:\>
```

PC E

Physical Config Desktop Programming Attributes

Command Prompt

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ip config
Invalid Command.

C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::20C:CFFF:FEA5:E6BA
   IPv6 Address.....: ::
   IPv4 Address.....: 154.3.100.126
   Subnet Mask.....: 255.255.255.224
   Default Gateway.....: ::
                         154.3.100.97

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: ::
   IPv6 Address.....: ::
   IPv4 Address.....: 0.0.0.0
   Subnet Mask.....: 0.0.0.0
   Default Gateway.....: ::
                         0.0.0.0

C:\>
```

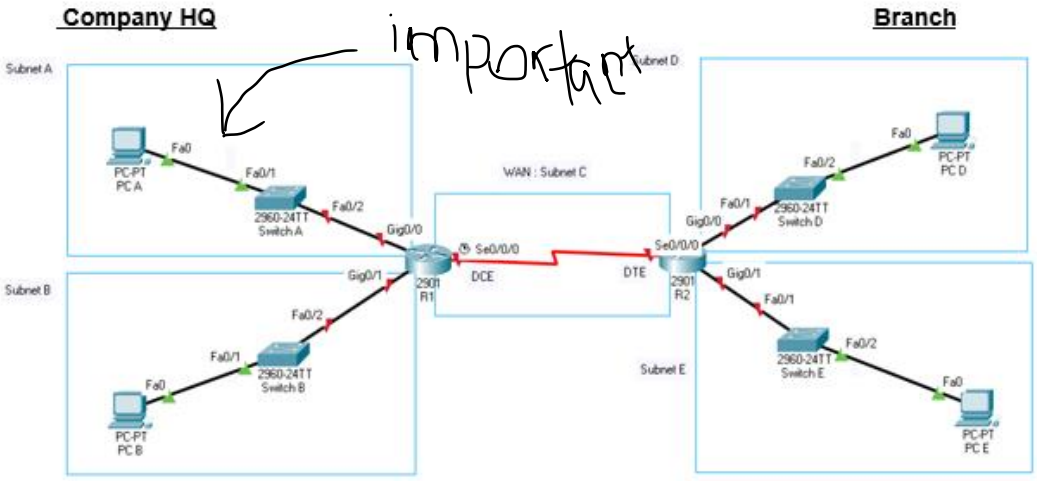
Tracert

```
C:\>tracert 154.3.100.1

Tracing route to 154.3.100.1 over a maximum of 30 hops:

  1    0 ms      0 ms      3 ms      154.3.100.33
  2    1 ms      0 ms      0 ms      154.3.100.1

Trace complete.

C:\>
```

Enhancements

Standard [ACL]Access control list

Access Control Lists (ACLs) are used to regulate network traffic and enhance security by defining rules that allow or deny traffic based on criteria such as IP addresses, protocols, and ports. This ensures that only authorized users and devices can access specific network resources, prevents unauthorized access, and helps manage and control the flow of data within the network, thereby protecting sensitive information and maintaining the integrity and efficiency of the network.. At the company headquarters, ACLs can be configured to ensure that only authorized PCs are permitted access, enhancing overall security. By establishing both allow and deny lists, the company can effectively monitor and restrict access, suspending devices if any suspicious activities are detected. This proactive approach helps safeguard sensitive information and maintain the integrity of the network by allowing only trusted devices to connect



```
R1>en
R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#acc
R1(config)#access-list 1
% Incomplete command.
R1(config)#acc
R1(config)#access-list 1?
<1-99>
R1(config)#access-list 1
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#access
R1(config)#access-list 1 per
R1(config)#access-list 1 permit 154.3.100.30 0.0.0.0
R1(config)#access
R1(config)#access-list 1 permit 154.3.100.126 0.0.0.0
R1(config)#access
R1(config)#access-list 1 permit 154.3.100.94  0.0.0.0
R1(config)#
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#show run
R1#show running-config
Building configuration...
```

```
R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#int g
R1(config)#int gigabitEthernet 0/0
R1(config-if)#ip acc
R1(config-if)#ip access-group 1 out
R1(config-if)#
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

Properties

1-99 is standard acl

100-199 onwards is extended acl

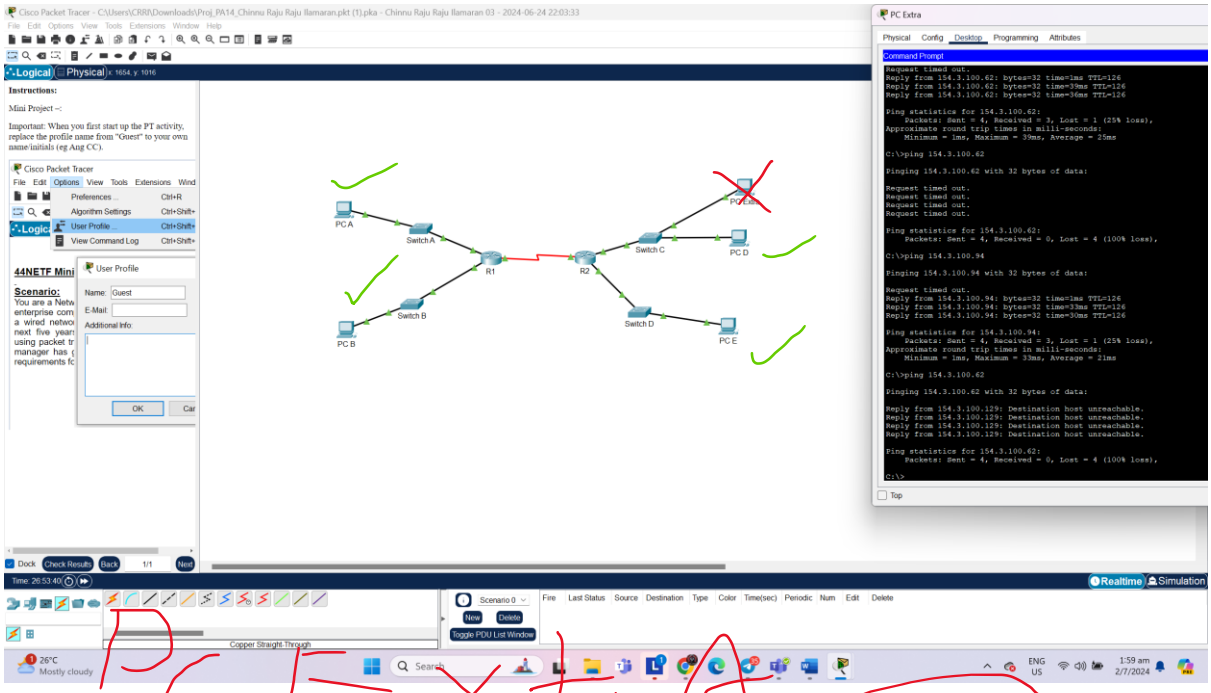
Denies or permits source ip address

Denies or permits source Ip add

Denies or permits destination Ip add

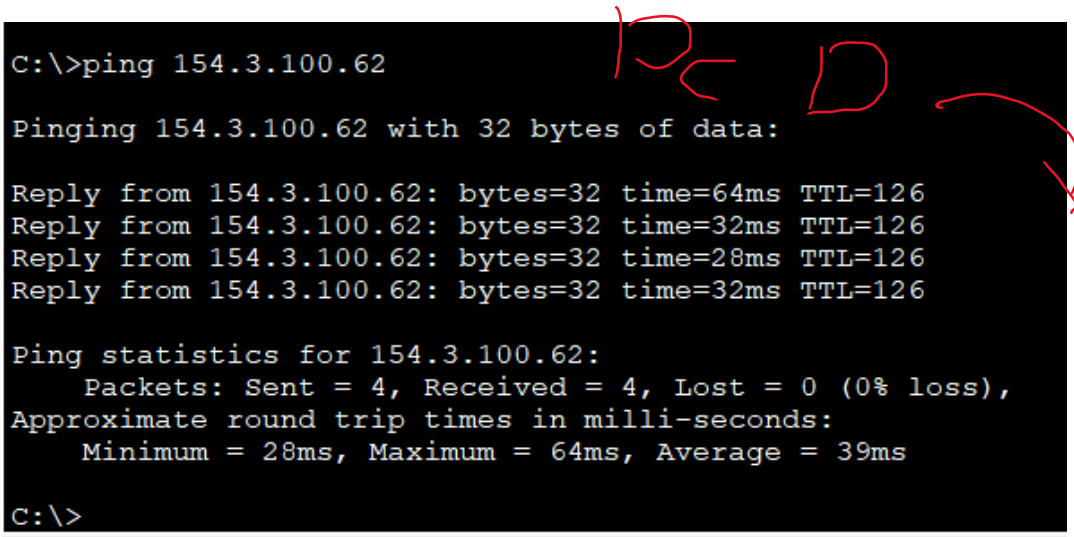
Denies or permits ports

```
!
!
interface GigabitEthernet0/0
 ip address 154.3.100.33 255.255.255.224
 ip access-group 1 out
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
```



```
C:\>ping 154.3.100.62

Pinging 154.3.100.62 with 32 bytes of data:

Reply from 154.3.100.129: Destination host unreachable.
Reply from 154.3.100.129: Destination host unreachable.
Reply from 154.3.100.129: Destination host unreachable.
Reply from 154.3.100.129: Destination host unreachable.

Ping statistics for 154.3.100.62:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Top



What each command does

access-list 1 permit/deny 154.3.100.1 0.0.0.0 or any
int g 0/0
ip access-group 1 out

Steps

1 Create access-list(extended or standard)

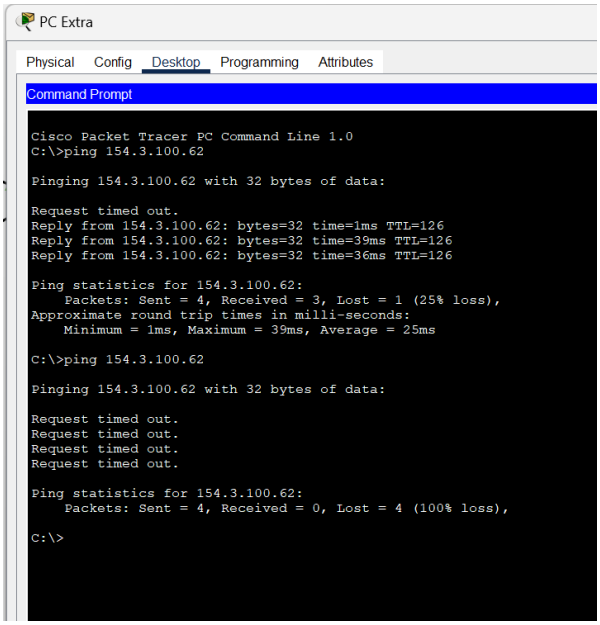
2 Apply the access-list to an interface (inbound outbound)

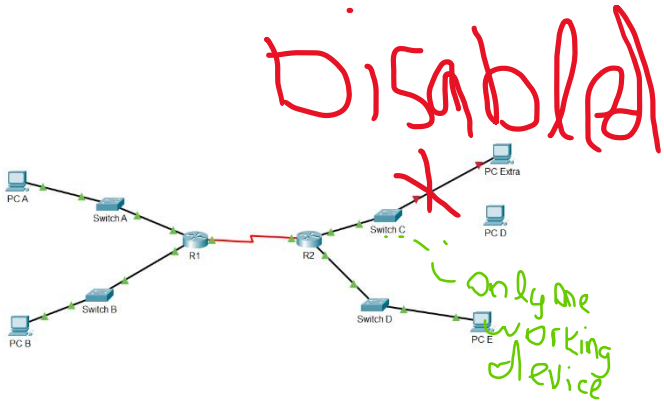
Port security

Port security ensures that employees at the company headquarters use only their assigned work PCs by restricting network access to specific MAC addresses. By configuring port security to recognize and allow only the MAC addresses of authorized work PCs, the network blocks any personal devices from connecting. This approach enhances security by ensuring that only approved hardware can access company resources, thereby reducing the risk of unauthorized access and maintaining a secure, efficient work environment.

```
Switch>enable
Switch#
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface FastEthernet0/1
Switch(config-if)#
Switch(config-if)#exit
Switch(config)#interface FastEthernet0/2
Switch(config-if)#
Switch(config-if)#exit
Switch(config)#interface FastEthernet0/1
Switch(config-if)#exit
Switch(config)#int fa0/2
Switch(config-if)#swit
Switch(config-if)#switchport mode acc
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port
Switch(config-if)#switchport port-security maxim
Switch(config-if)#switchport port-security maximum 1
Switch(config-if)#switchport port-security mac
Switch(config-if)#switchport port-security mac-address sti
Switch(config-if)#switchport port-security mac-address sticky
Switch(config-if)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console
```

```
spanning-tree extend system-id
!
interface FastEthernet0/1
!
interface FastEthernet0/2
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 000D.BDE3.30EA
!
interface FastEthernet0/3
!
```





What each command does

switchport mode access: Configures the port as an access port.
switchport port-security: Enables port security on the port.
switchport port-security maximum 1: Limits the port to learn and allow only 1 MAC address..
switchport port-security mac-address sticky : Enables the sticky MAC feature to automatically learn and retain MAC addresses. This makes it easier to manage authorized devices because the switch remembers the MAC addresses even after a reboot.

Conclusion

In conclusion, I managed to put in place a very solid and expandable infrastructure plan, which will be used to support growth for the next five years. Our network is made up of two routers, four switches, and four PCs that enable full connectivity within our organization. By adding standard ACLs, it was possible for me to enhance our network security by controlling access to essential resources and preventing potential risks. I also enabled port security on our switcher so as to prevent unauthorized access and other forms of security leaks. This diligent planning and designing in Packet Tracer shows its reliability, safe infrastructure setup that can allow future growth thus conforming with goals of the company in strategic IT architecture needs.

My Solution