

DEPARTMENT OF TELECOMMUNICATION ENGINEERING
MEHRAN UNIVERSITY OF ENGINEERING & TECHNOLOGY, JAMSHORO
COMPUTER COMMUNICATION & NETWORKING
(6th Term, 3th Year) LAB EXPERIMENT # 14/1

Name: _____ Roll No: _____

Score: _____ Signature of the Lab Tutor: _____ Date: _____

OBJECTIVES

#	Topic	#. Of Lectures	CLO	Taxonomy level
1	To apply the knowledge of standard and extended ACLs and configure it in router.	3	2	P3

OUTCOME(S)

a. An ability to apply knowledge of math, science, and engineering	PLO1: Engineering Knowledge:
k. an ability to use the techniques, skills, and modern engineering tools necessary for engineering practice.	PLO5: Modern Tool Usage

RUBRICS:

Performance Metric	Exceeds expectation (4-5)	Meets expectations (2-3)	Does not meet expectations (0-1)	Score
Knowledge and application [PLO1]	Applies the appropriate knowledge and concepts to the problem with accuracy and proficiency; shows precise understanding of these knowledge and concepts.	Applies the relevant knowledge and concept to the problem, possibly in a roundabout way; understands the major points of the knowledge, with possible misunderstanding or failure to recall minor points;	Fails to apply relevant knowledge and concepts to the problem; misunderstands or fails to recall critical points.	
Modern Tool Usage [PLO5]	Computer and software are extensively used in the course	Computer and software are somewhat utilized, effort was put into learning new software	Computer and software are not utilized, no attempt was made at learning new software	
Total Score				

EQUIPMENT

- Six PC
- Two Servers
- Two Routers with console
- Appropriate cables for connections

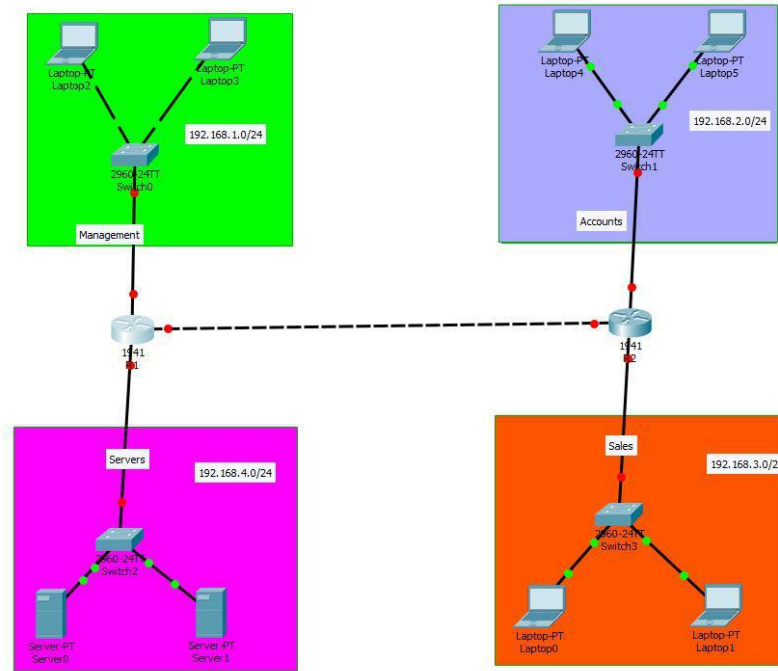
DISCUSSION & CONFIGURATION

ACL:

An access control list (ACL) is a table that tells a computer operating system which access rights each user has to a particular system object, such as a file directory or individual file. Each object has a security attribute that identifies its access control list. The list has an entry for each system user with access privileges. In simpler terms the ACL is like a authorization list to a security guard outside of a VIP hotel. Anyone trying to access the hotel will first have to get checked from the guard that whether this person is authorized to access the hotel or not, after verification the person is either permitted or denied the entry.

Step 1:

Design the network topology in to the packet tracer.



Step 2:

Do the basic configuration on both routers.

1) R1 configuration:

```
Router>en
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R1
R1(config)#int fa 0/0
R1(config-if)#ip add 192.168.1.1 255.255.255.0
R1(config-if)#no sh
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,
changed state to up
```

```
R1(config-if)#int fa0/1
R1(config-if)#ip add 192.168.4.1 255.255.255.0
R1(config-if)#no sh
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to up
```

```
int se0/0/0
R1(config-if)#ip add 192.168.5.1 255.255.255.0
R1(config-if)#clock rate 64000
R1(config-if)#no sh
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
```

On Router2

```
Router>en
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R2
R2(config)#int fa0/0
R2(config-if)#ip add 192.168.2.1 255.255.255.0
R2(config-if)#no sh
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on
Interface FastEthernet0/0, changed state to up

R2(config-if)#int fa 0/1
R2(config-if)#ip add 192.168.3.1 255.255.255.0
R2(config-if)#no sh
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on
Interface FastEthernet0/1, changed state to up

R2(config-if)#int se0/0/0
R2(config-if)#ip add 192.168.5.2 255.255.255.0
R2(config-if)#no sh
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed
state to up
```

2) Activate routing protocol on both routers

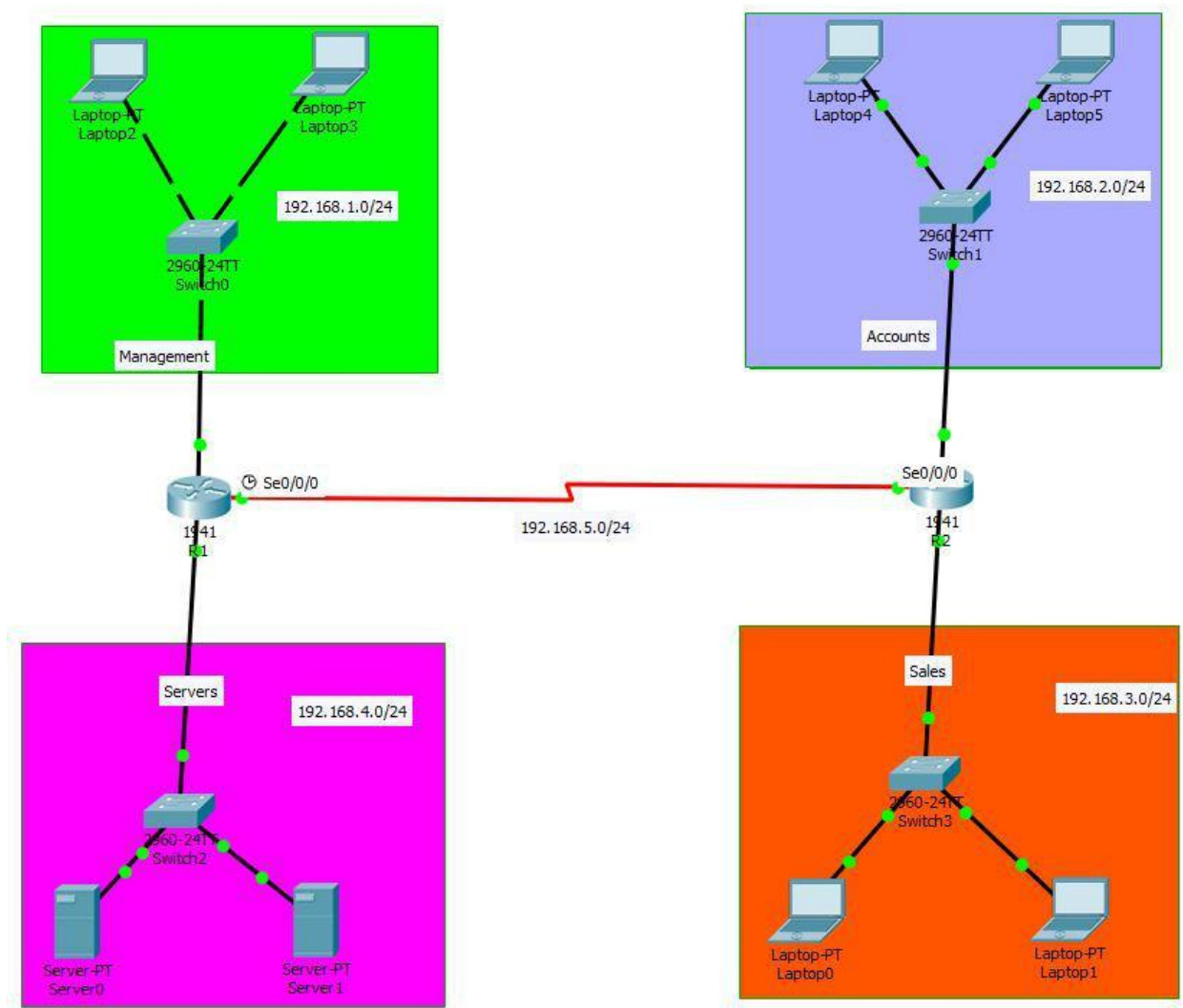
```
R1(config)# R1(config)#router rip
R1(config-router)#version 2

R1(config-router)#network 192.168.1.0
R1config-router)#network 192.168.4.0
```

```
R1(config-router)#network 192.168.5.0  
R1(config-router)#exit
```

```
R2(config)#router rip  
R2(config-router)#version 2  
R2(config-router)#network 192.168.2.0  
R2(config-router)#network 192.168.3.0  
R2(config-router)#network 192.168.5.0  
R2(config-router)#exit
```

After the basic configuration your topology should be up in all interfaces



- 3) Assign static ip's to PC's along with the gateway address according to the topology.
- 4) Check routing table at this point to confirm the routing entries are correct.

- 5) From Pc 0 of Management network try to ping other pc's and check the basic connectivity.

```
C:\>ping 192.168.3.5

Pinging 192.168.3.5 with 32 bytes of data:

Reply from 192.168.3.5: bytes=32 time=1ms TTL=126
Reply from 192.168.3.5: bytes=32 time=1ms TTL=126
Reply from 192.168.3.5: bytes=32 time=10ms TTL=126
Reply from 192.168.3.5: bytes=32 time=12ms TTL=126

Ping statistics for 192.168.3.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 12ms, Average = 6ms

C:\>ping 192.168.3.6

Pinging 192.168.3.6 with 32 bytes of data:

Request timed out.
Reply from 192.168.3.6: bytes=32 time=11ms TTL=126
Reply from 192.168.3.6: bytes=32 time=13ms TTL=126
Reply from 192.168.3.6: bytes=32 time=10ms TTL=126

Ping statistics for 192.168.3.6:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 10ms, Maximum = 13ms, Average = 11ms

C:\>ping 192.168.4.5

Pinging 192.168.4.5 with 32 bytes of data:

Request timed out.
Reply from 192.168.4.5: bytes=32 time=1ms TTL=127
Reply from 192.168.4.5: bytes=32 time<1ms TTL=127
Reply from 192.168.4.5: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.4.5:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
```

Name based ACL Commands:

- a) Router(Config)#ip access-list standard <ACL_no/Name>
For standard ACL number is from <1-99>
 - b) Router(Config-std-nacl)# <deny/permit> <matching
parameters> Applying ACL to an interface
 - c) Router(Config)#interface <type/slot>
 - d) Router(Config-if)#ip access-group <ACL_no./Name> <in/out>
- 6) Configuring Standard ACL:
- Task 1: Accounts department and management department employees should not be able to access company's server except managers of accounts and sales. The

respective ip's of managers of both departments are 192.168.2.5 and 192.168.3.5, they should be able to access the servers without interruption.

Task 2: Sales department should not be able to reach or access management.

In Task 1 we have to restrict the accounts and sales department so that restriction has to be placed on Router 1 further away from source.

```
R1(config)#access-list 1 permit host 192.168.2.5
```

```
R1(config)# access-list 1 permit host 192.168.3.5
```

```
R1(config)#deny 192.168.2.0 0.0.0.255
```

```
R1(config)#deny 192.168.3.0 0.0.0.255
```

```
R1(config)#Permit any
```

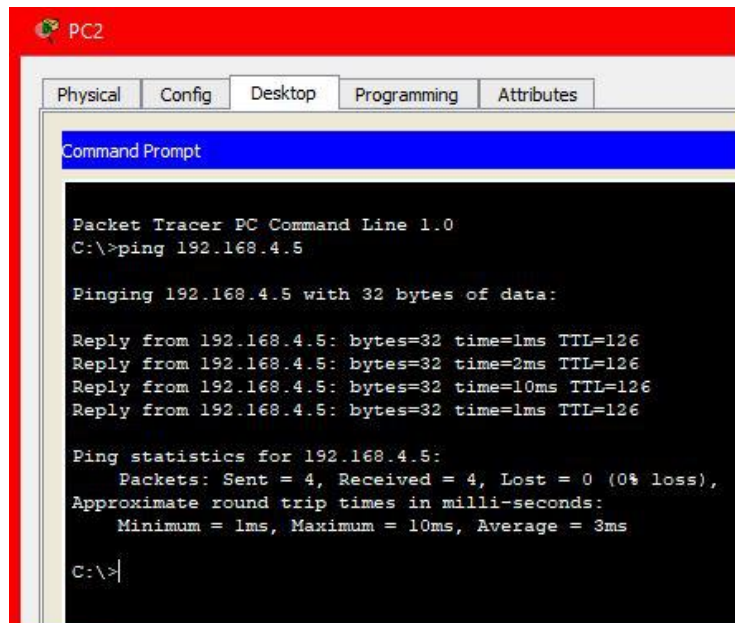
```
R1(config)#exit
```

```
R1(config)#int fa0/1
```

```
R1(config-if)#ip access-group 1 out
```

Now check the connectivity of the sales and accounts network.

- a) Check the connectivity of manager's pc's in both networks trying to reach server.



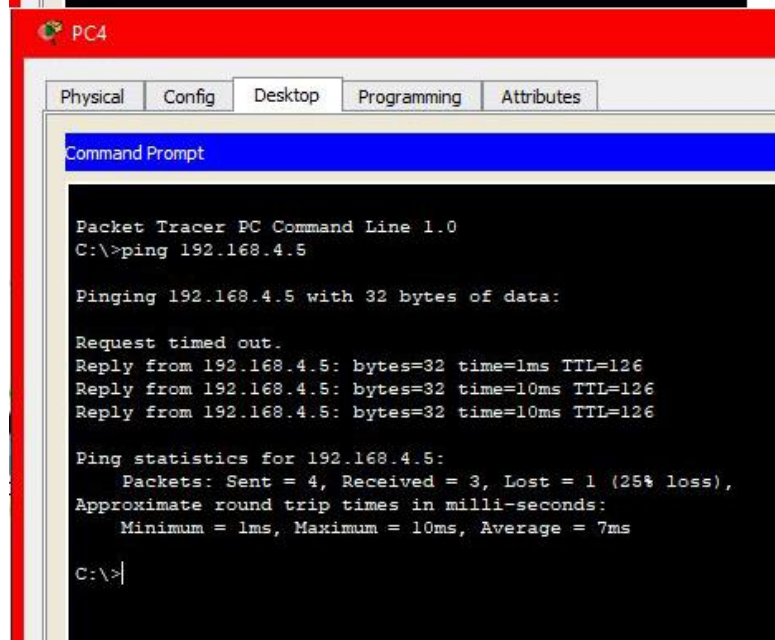
```
PC2
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.4.5

Pinging 192.168.4.5 with 32 bytes of data:

Reply from 192.168.4.5: bytes=32 time=1ms TTL=126
Reply from 192.168.4.5: bytes=32 time=2ms TTL=126
Reply from 192.168.4.5: bytes=32 time=10ms TTL=126
Reply from 192.168.4.5: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.4.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 10ms, Average = 3ms

C:\>
```



```
PC4
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.4.5

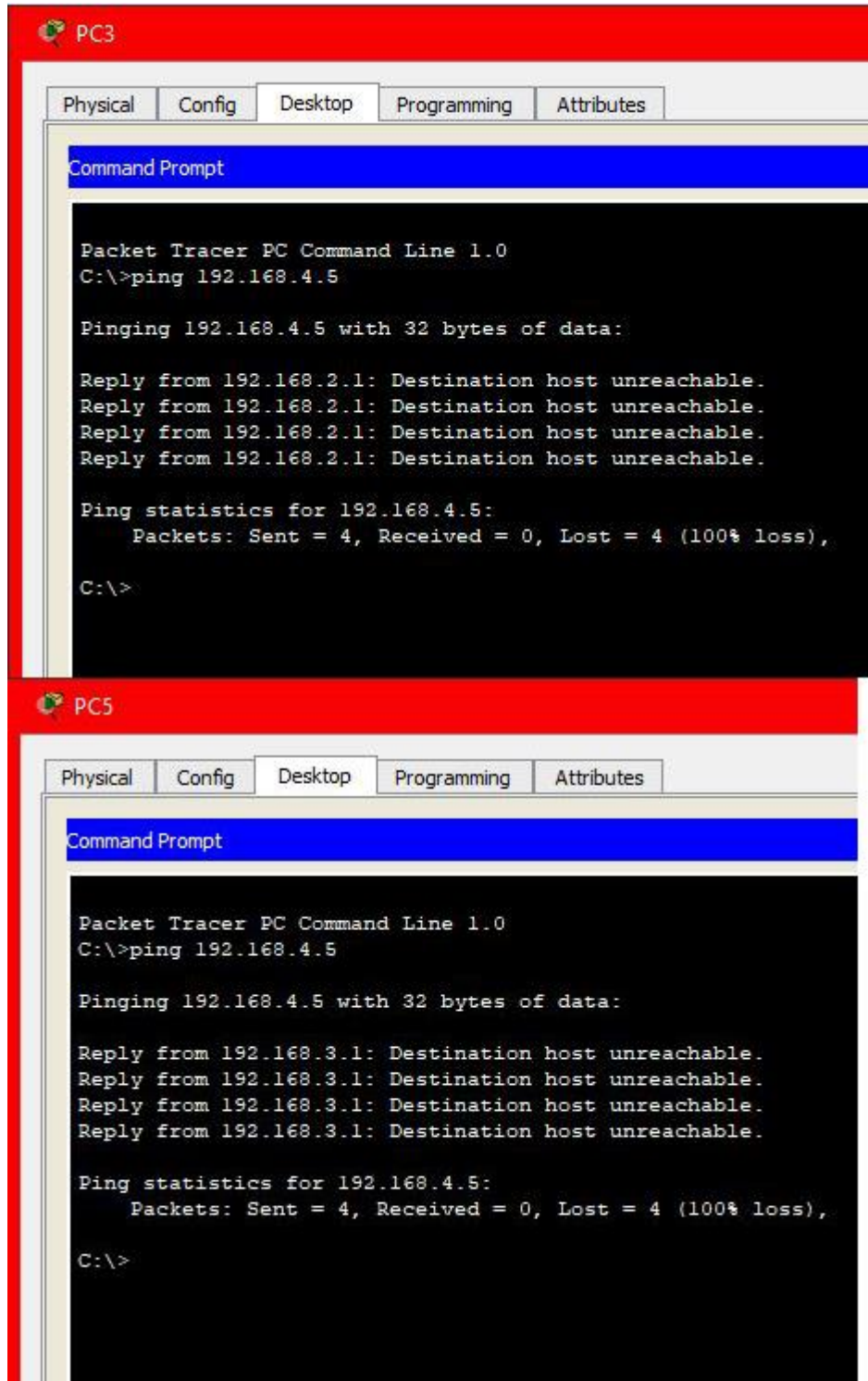
Pinging 192.168.4.5 with 32 bytes of data:

Request timed out.
Reply from 192.168.4.5: bytes=32 time=1ms TTL=126
Reply from 192.168.4.5: bytes=32 time=10ms TTL=126
Reply from 192.168.4.5: bytes=32 time=10ms TTL=126

Ping statistics for 192.168.4.5:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 10ms, Average = 7ms

C:\>
```


As we can see both manager's PC's are able to reach servers, now let's try other PC's



As we can see the rest of the network is restricted and unreachable.

Task 2:

Sales should not be able to access management department.

This will be done using name based standard ACL on Router 1.

```
R1(config)#ip access-list standard restrict_sales
```

```
R1(config-std-nacl)#permit host 192.168.3.5
```

```
R1(config-std-nacl)#deny 192.168.3.0 0.0.0.255
```

```
R1(config-std-nacl)#permit any
```

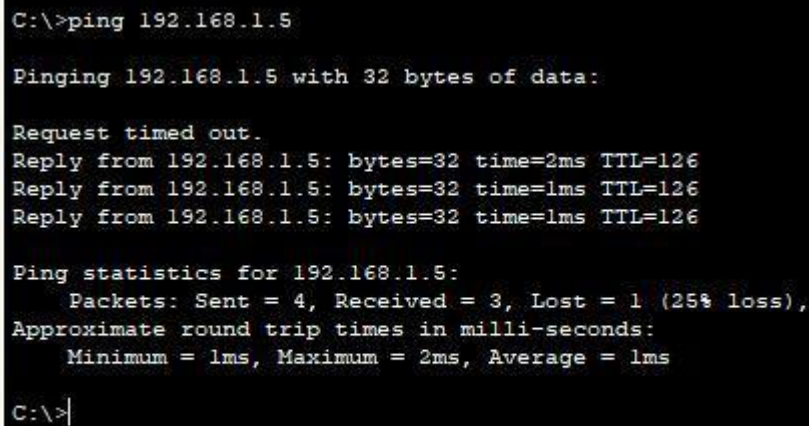
```
R1(config-std-nacl)#exit
```

```
R1(config)#int fa0/0
```

```
R1(config-if)#ip access-group restrict_sales out
```

```
R1(config-if)#exit
```

Now check the status can apart from the manager, rest of the network access the management network?



```
C:\>ping 192.168.1.5

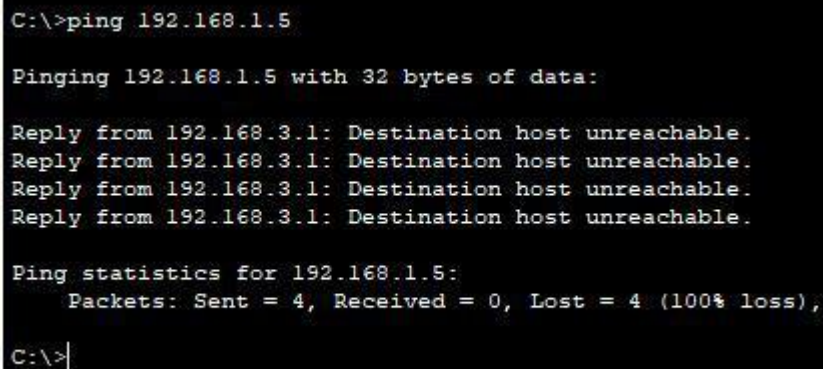
Pinging 192.168.1.5 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.5: bytes=32 time=2ms TTL=126
Reply from 192.168.1.5: bytes=32 time=1ms TTL=126
Reply from 192.168.1.5: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.1.5:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\>|
```

As we can see above manager's pc can access the management network



```
C:\>ping 192.168.1.5

Pinging 192.168.1.5 with 32 bytes of data:

Reply from 192.168.3.1: Destination host unreachable.
Reply from 192.168.3.1: Destination host unreachable.
Reply from 192.168.3.1: Destination host unreachable.
Reply from 192.168.3.1: Destination host unreachable.

Ping statistics for 192.168.1.5:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>|
```

In above figure it's evident that rest of the network of sales cannot reach management network

7) Configuring Extended ACL

Task 1: Account department users are allowed to access web service of server but manager of accounts 192.168.2.5 is not allowed to use web service.

Task2: Accounts department users are not allowed to use FTP server but manager of accounts 192.168.2.5 is allowed to access FTP server.

To achieve Task1 ACL is applied on Router 2 near to the source.syntax of extended ACL. The ip address of server is 192.168.4.200

R2(config)#access-list <100-199> <permit/deny> <protocol> <source-add> <destination-add> eq <port-number>

Task1:

We can also configure name-based ACL

R2(config)#ip access-list 101

R2(config)#deny tcp host 192.168.2.5 192.168.4.200 0.0.0.0 eq 80

R2(config)#permit tcp 192.168.2.0 0.0.0.255 192.168.4.200 0.0.0.0 eq 80

Task2: R2(config)#permit tcp host 192.168.2.5 192.168.4.200 0.0.0.0 eq 21

R2(config)#deny tcp 192.168.2.0 0.0.0.255 192.168.4.200 0.0.0.0 eq 21

Now we will apply this acl on R2 interface fa0/0 closest to the source network.

R2(config)#int fa0/0

R2(config-if)#ip access-group 101 out

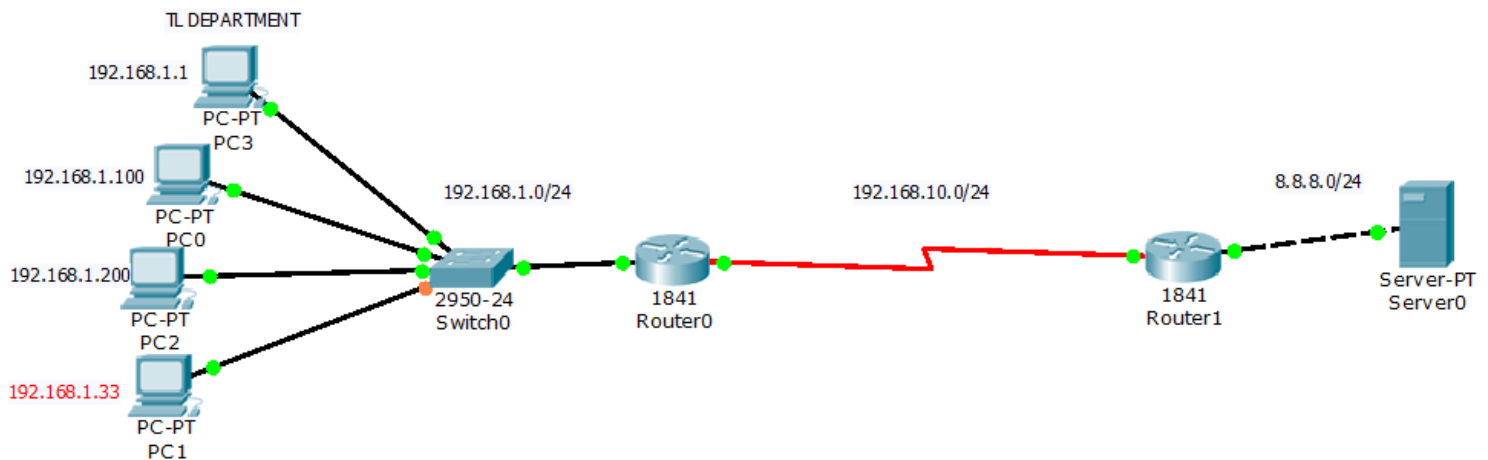
R2(config-if)#exit

NOTE: after destination address we will give wildcard mask to show network

NOW if manager tries to access Web service it will be denied and only allowed FTP service. On the other hand, any user from account can use Web service but FTP service is blocked.

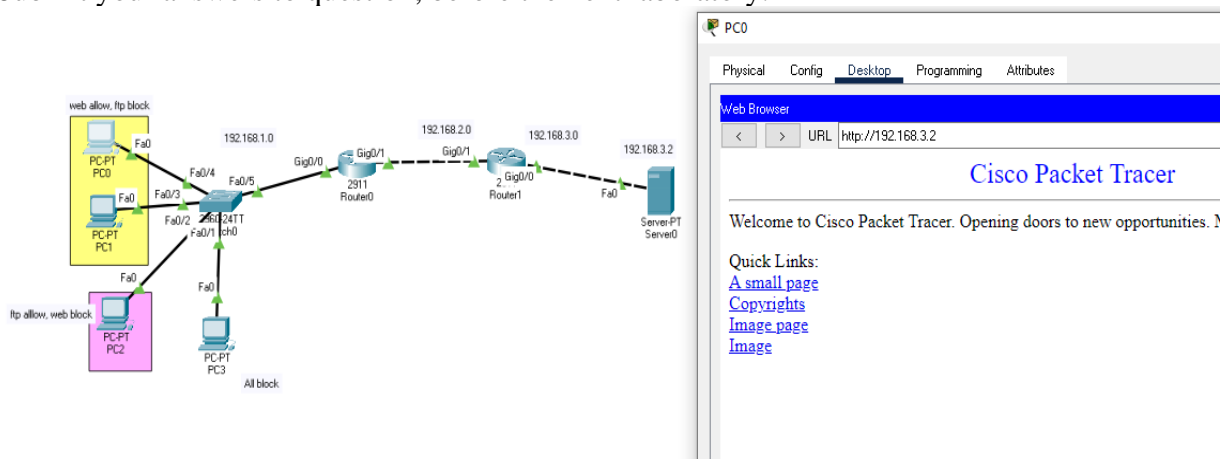
Task: Design the topology shown below

- 1) Allow Web service to user having ip address 192.168.1.100 and 192.168.1.200 but block their FTP service of the server.
- 2) Block Web service to user having ip address 192.168.1.1 but allow FTP service to this user.
- 3) Block all services for user 192.168.1.33 to the server.



FINAL CHECK LIST

1. Return all equipment and materials to their proper storage area.
2. Submit your answers to question, before the next laboratory.



DEPARTMENT OF TELECOMMUNICATION ENGINEERING
MEHRAN UNIVERSITY OF ENGINEERING & TECHNOLOGY, JAMSHORO
COMPUTER COMMUNICATION & NETWORKING
(6th Term, 3th Year) LAB EXPERIMENT # 14/12

