

# CSE 3502

## INFORMATION SECURITY MANAGEMENT



### Lab Assessment – ACL

L19+L20 | SJT516  
Dr. Lavanya K

WINTER SEMESTER 2021-22

by

**SHARADINDU ADHIKARI**

**19BCE2105**

### Exp. Standard Access List

Standard access lists are the oldest type of access lists, dating back as early as Cisco IOS Software Release 8.3. Standard access lists control traffic by comparing the source address of packets to the addresses configured in the access list.

In all software releases, the access list number for the standard IP access lists can be anything from 1 to 99. In Cisco IOS Software Release 12.0.1, standard IP access lists began using additional numbers from 1300 to 1999. These additional numbers are sometimes referred to as the *expanded range*. In addition to using numbers to identify access lists, Cisco IOS Software Release 11.2 and later added the ability to use names to define standard IP access lists. We will learn how to configure both numbered and named access lists as we proceed in this chapter.

**Table:** Access List Types and Corresponding Numbers

Access List Type	Number Range
IP Standard Access Lists	1-99
IP Standard Access Lists (expanded range)	1300-1999
IP Extended Access Lists	100-199
IP Extended Access Lists (expanded range)	2000-2699

We can differentiate between standard and extended access lists in the numbered format simply by looking at the access list number. Based on the number used when access list is created, the router also knows which type of syntax to expect as the list is entered. By using numbers 1 – 99 or 1300 – 1999, we are essentially telling the router that we want to create a standard IP access list. Thus the router will expect the standard IP access list syntax specifying only the source IP address in access list entries.

#### Components for Std. ACL:

Device	Interface	IP Address	Subnet Mask	Default Gateway
Router R1	G0/0	192.168.1.1	255.255.255.0	N/A
	G0/1	10.0.0.1	255.255.255.0	N/A
	G0/2	11.0.0.1	255.255.255.0	N/A
PC0	Fa0	10.0.1.2	255.255.255.0	10.0.0.1
PC1	Fa0	11.0.0.2	255.255.255.0	11.0.0.1
Server	Fa0	8.8.8.8	255.255.255.0	8.8.8.1

#### Commands:

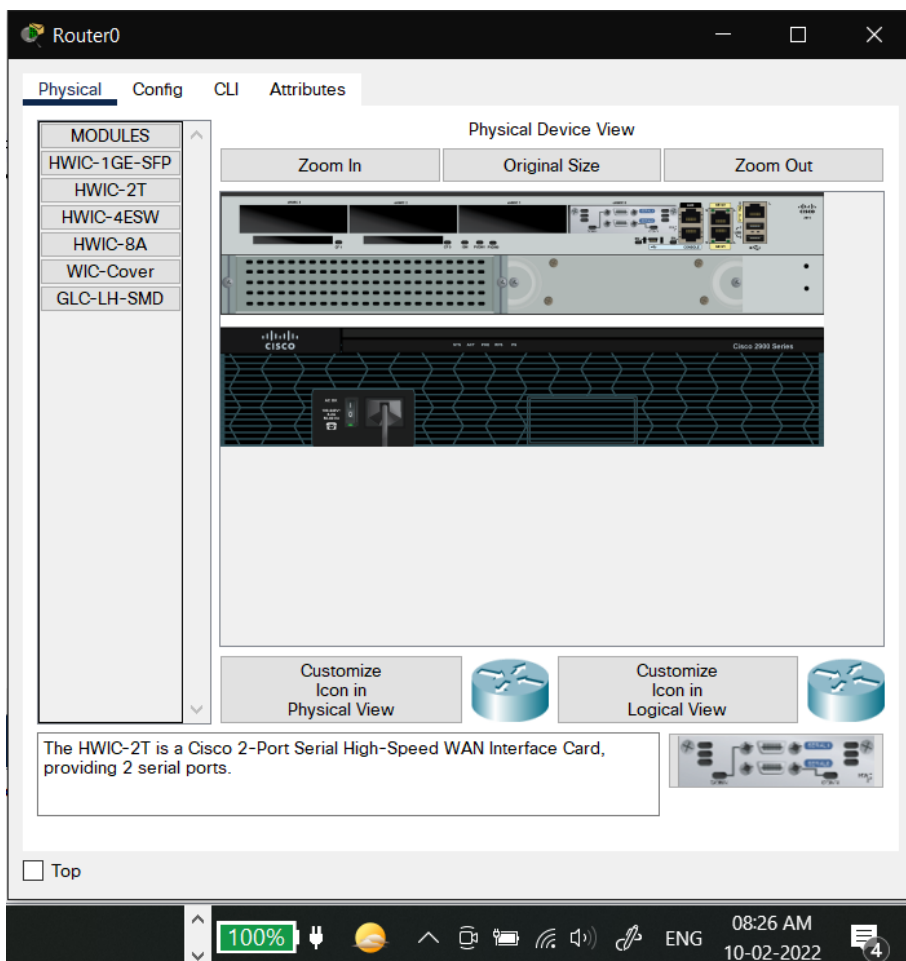
Device	Command Executed
--------	------------------

## Standard ACL

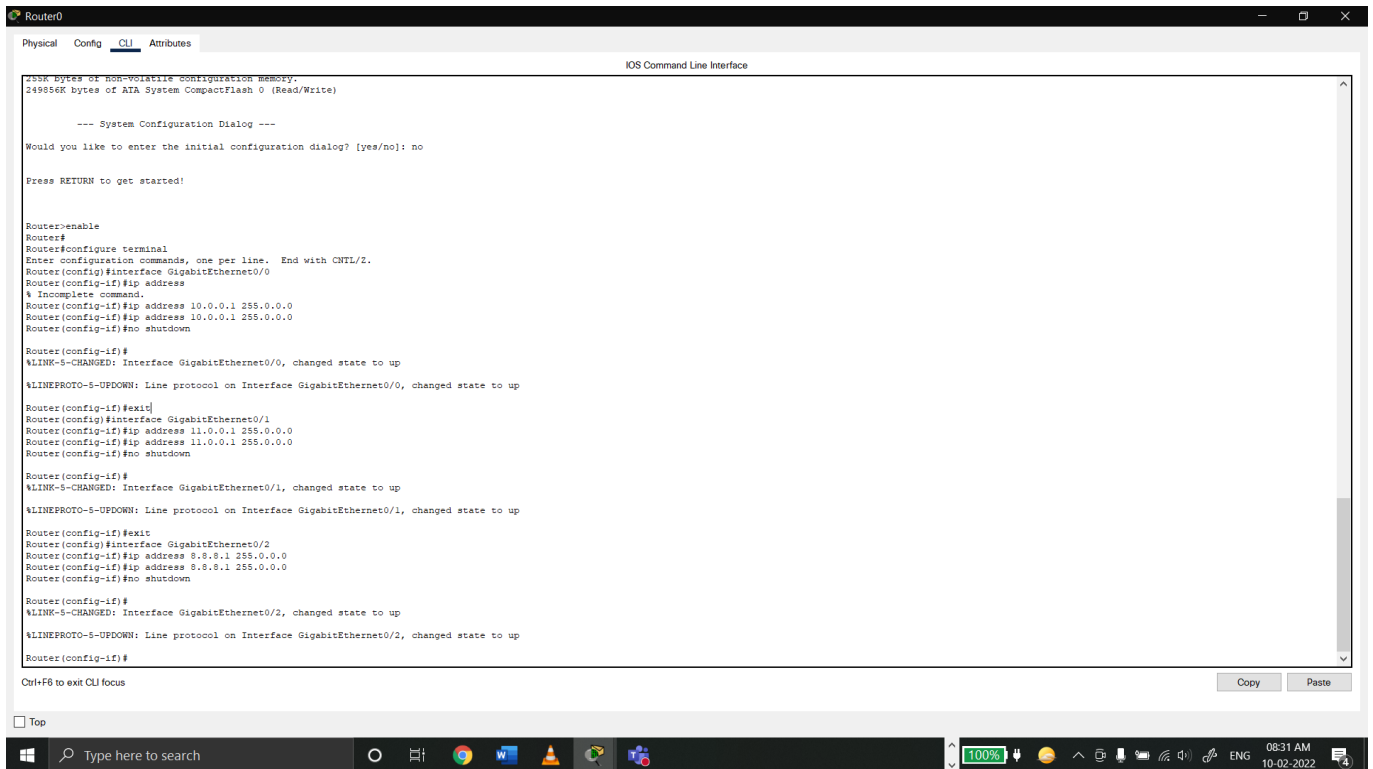
Router R0	<code>en</code>
	<code>conf t</code>
	<code>access-list 1 permit 10.0.0.0 0.0.0.255</code>
	<code>access-list 1 permit host 10.0.0.2</code>
	<code>access-list 1 deny 11.0.0.0 0.0.0.255</code>
	<code>int gig0/2</code>
	<code>ip access-group 1 out</code>
	<code>exit</code>

### Procedure:

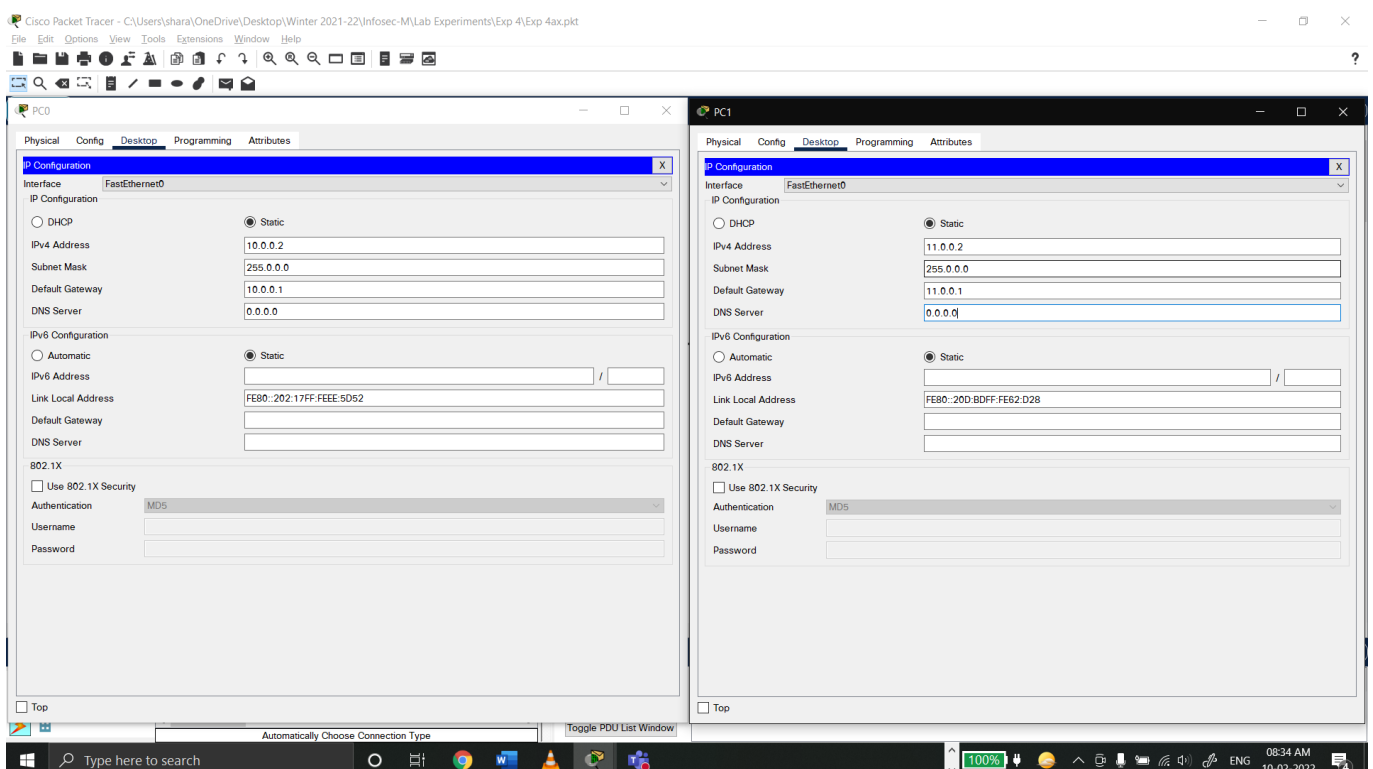
#### Step 1: HWIC-2T Module insertion in Router0



## Step 2: Router0 configuration



## Step 3: PC0 and PC1 IP configuration



## Step 4: Configuring standard access list in Router0

```

Router0
Physical Config CLI Attributes
IOS Command Line Interface
Router(config-if)#ip address 8.8.8.1 255.0.0.0
Router(config-if)#ip address 8.8.8.1 255.0.0.0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/2, changed
state to up

Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface GigabitEthernet0/2
Router(config-if)#access-list 1 permit 10.0.0.0 0.0.0.255
Router(config)#access-list 1 permit host 10.0.0.2
Router(config)#access-list 1 deny 11.0.0.0 0.0.0.255
Router(config)#int gig0/2
Router(config-if)#ip access-group 1 out
Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#
  
```

Ctrl+F6 to exit CLI focus

Copy Paste

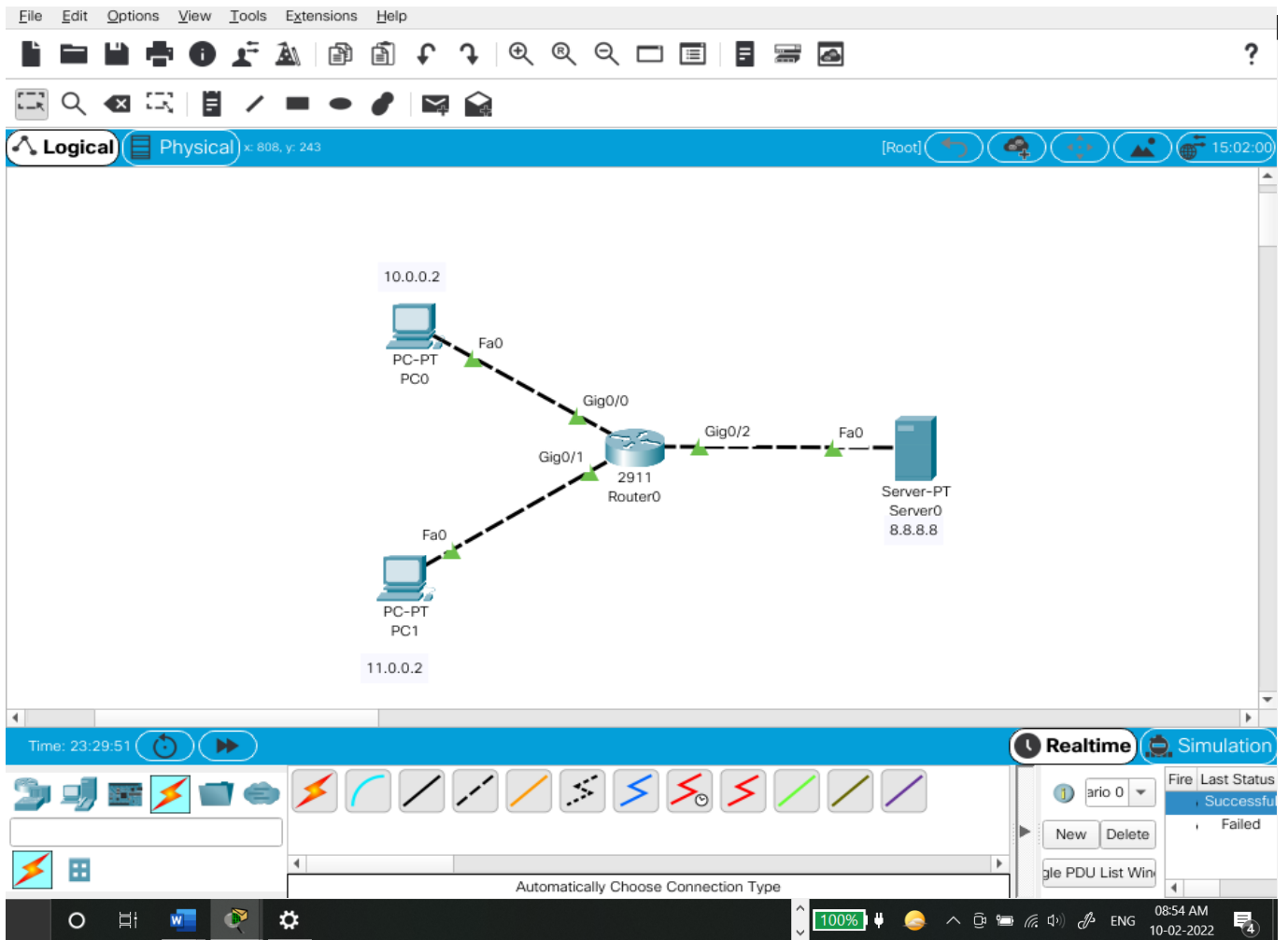
Top

100% 08:40 AM 10-02-2022

## Step 5: Sending PDUs, showcasing successful communication with PC0 and unsuccessful communication with PC1.

Realtime Simulation										
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC0	Server0	IC...		0.000	N	0	(e...	(delete)
	Failed	PC1	Server0	IC...		0.000	N	1	(e...	(delete)

## Final Topology:



### Exp. Extended Access List

To be more precise when matching a certain network traffic, extended access lists are used. Extended access lists are more difficult to configure and require more processor time than the standard access lists, but they enable a much more granular level of control.

With extended access lists, you can evaluate additional packet information, such as:

- source and destination IP address
- type of TCP/IP protocol (TCP, UDP, IP...)
- source and destination port numbers

#### Components for Ext. ACL:

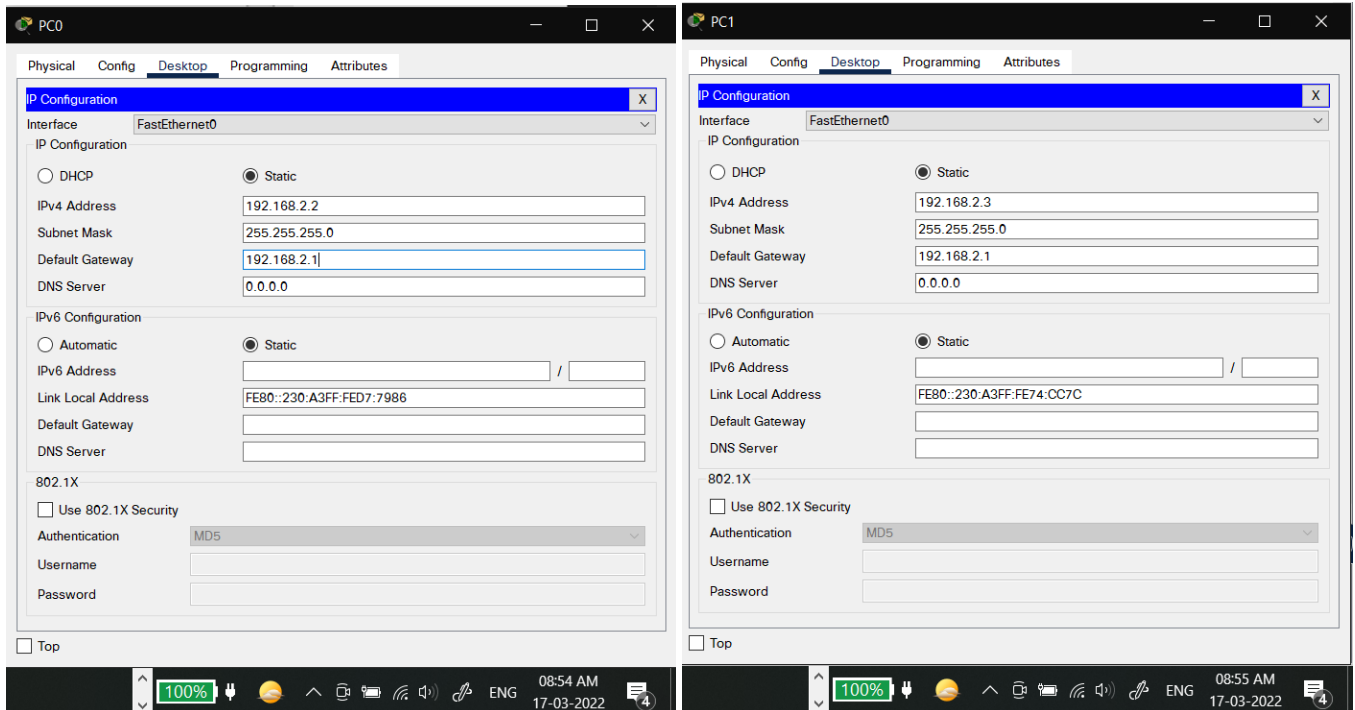
Device	Interface	IP Address	Subnet Mask	Default Gateway	SwitchPort
Router R1	Fa0/0	192.168.1.1	255.255.255.0	N/A	S1
	Fa0/1	192.168.2.1	255.255.255.0	N/A	S0
PC0	Fa0	192.168.2.2	255.255.255.0	192.168.2.1	S0
PC1	Fa0	192.168.2.3	255.255.255.0	192.168.2.1	S0
Server	Fa0	192.168.1.100	255.255.255.0	192.168.1.1	S1

#### Commands:

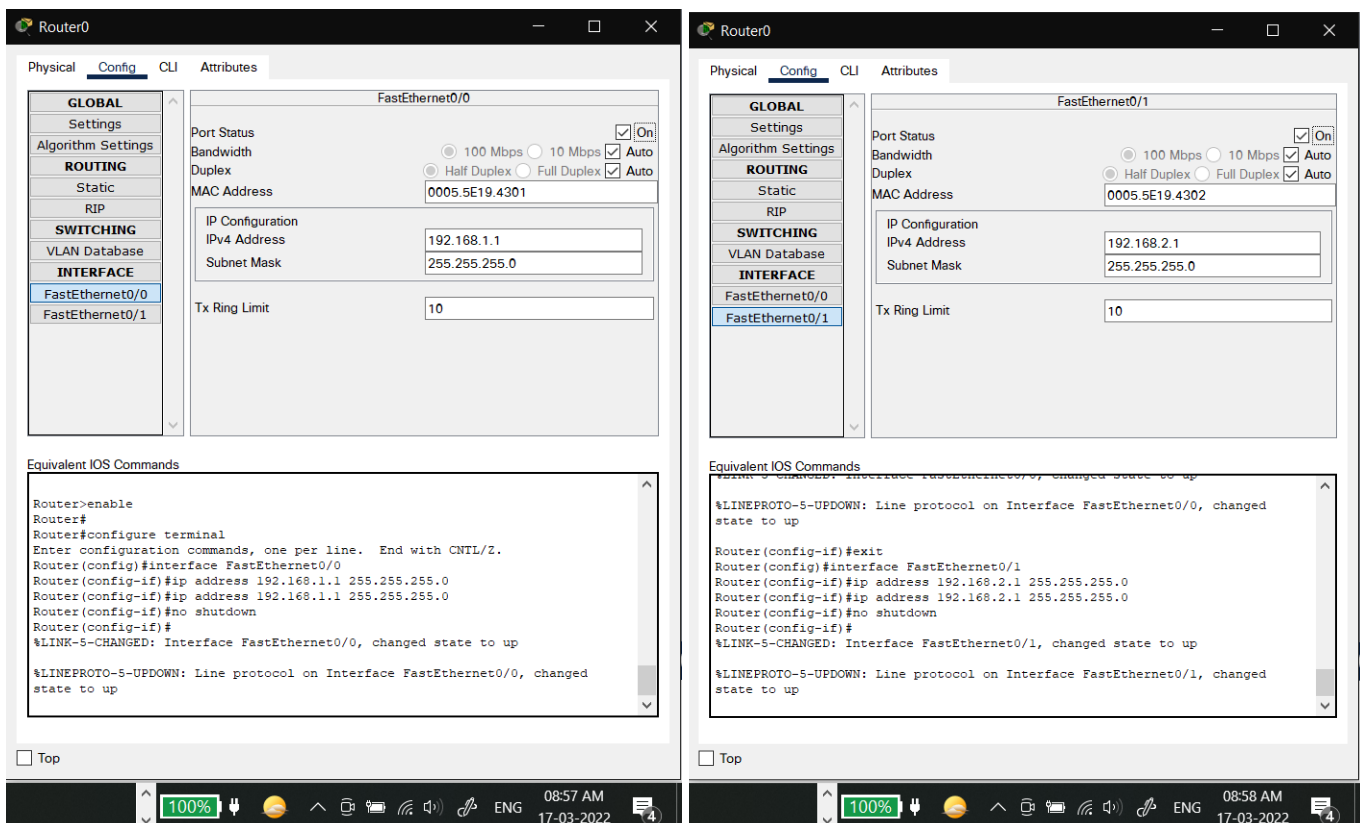
Device	Commands Executed
Extended ACL	
Router R0	<i>en</i>
	<i>conf t</i>
	<i>access-list 120 deny tcp host 192.168.2.2 host 192.168.1.100 eq 80</i>
	<i>access-list 120 deny tcp host 192.168.2.2 host 192.168.1.100 eq 21</i>
	<i>access-list 120 deny icmp host 192.168.2.2 host 192.168.1.100 echo</i>
	<i>Access-list 120 permit ip any any</i>
	<i>Interface fa0.1</i>
	<i>Ip access group 120 in</i>

end

## Step 1: PC0 and PC1 IP configurations

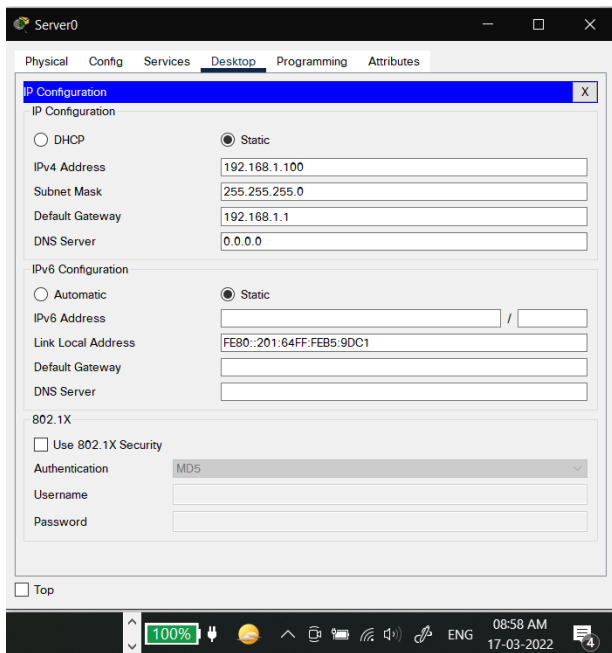


## Step 2: Router0 FastEthernet0/0 and FastEthernet0/1 configurations





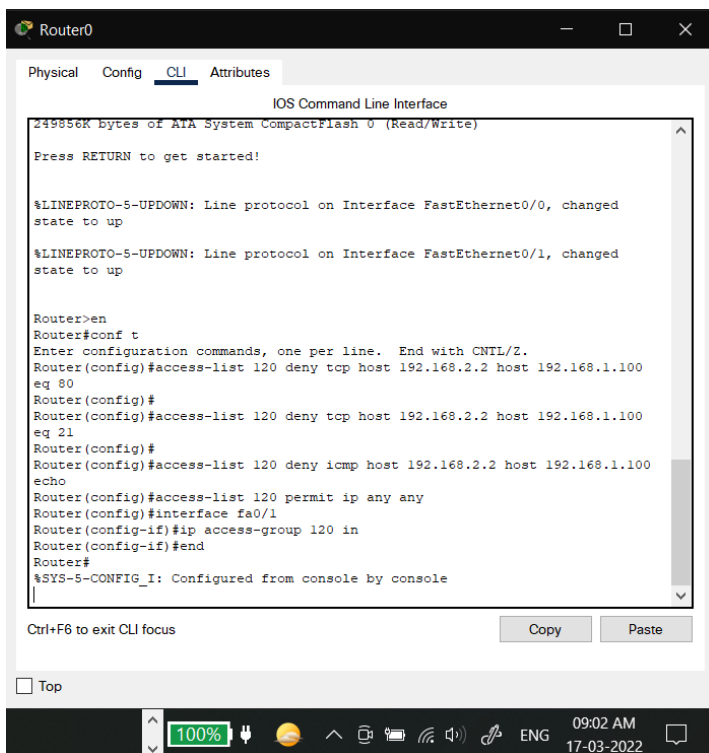
### Step 3: Server IP configuration



### Step 4: Sending PDUs, showcasing Successful Communication from PC0 and PC1 to Server

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC1	Server0	IC...		0.000	N	0	(e...	(delete)
	Successful	PC0	Server0	IC...		0.000	N	1	(e...	(delete)

### Step 5: Router0 CLI Access List Configuration



### Step 6: Showing the status of ICMP pings from PC0 and PC1 to the Server, respectively

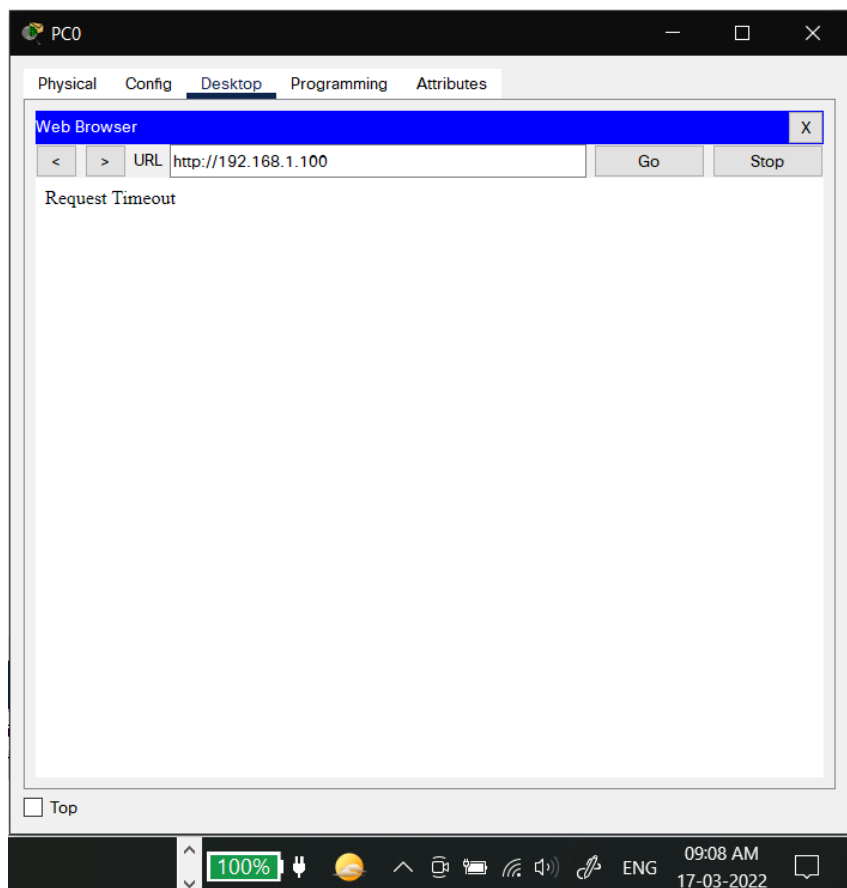
Realtime										
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Failed	PC0	Server0	IC...		0.000	N	0	(e...	(delete)

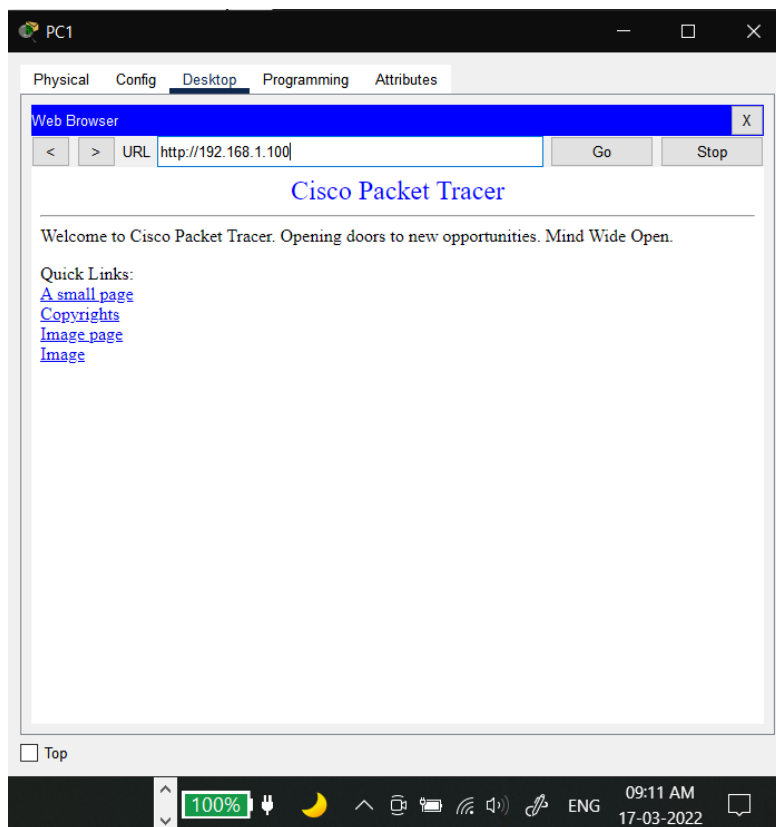
Realtime										
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC1	Server0	IC...		0.000	N	0	(e...	(delete)

### Step 7:

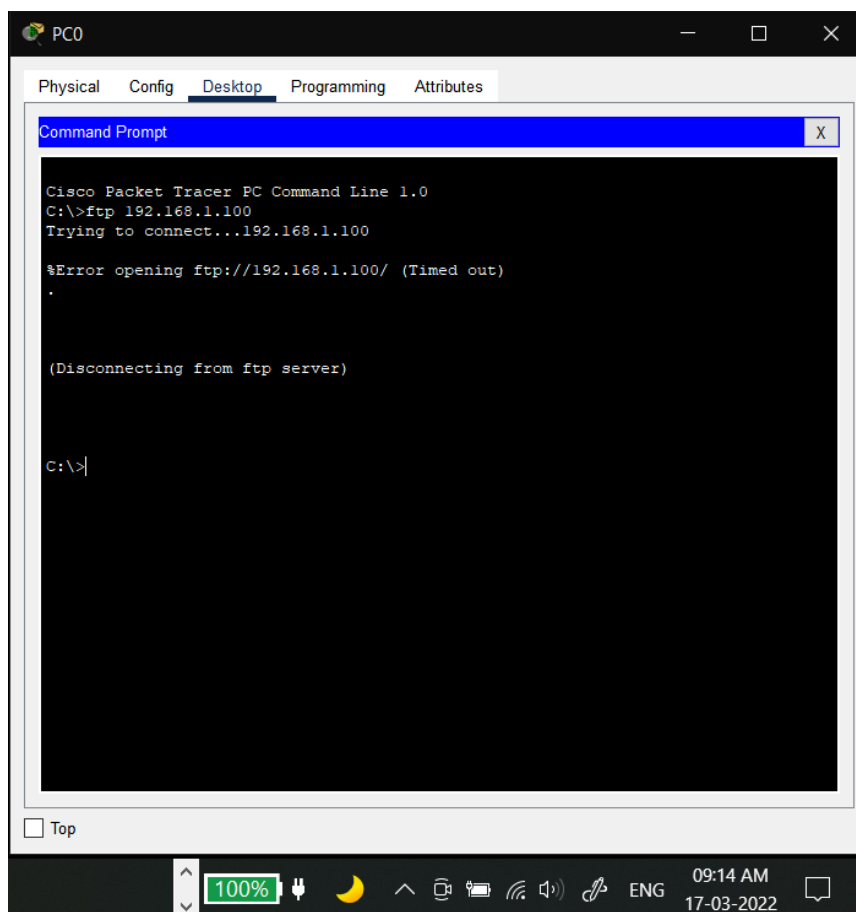
PC0 Web Browser (IP Packet): Unsuccessful

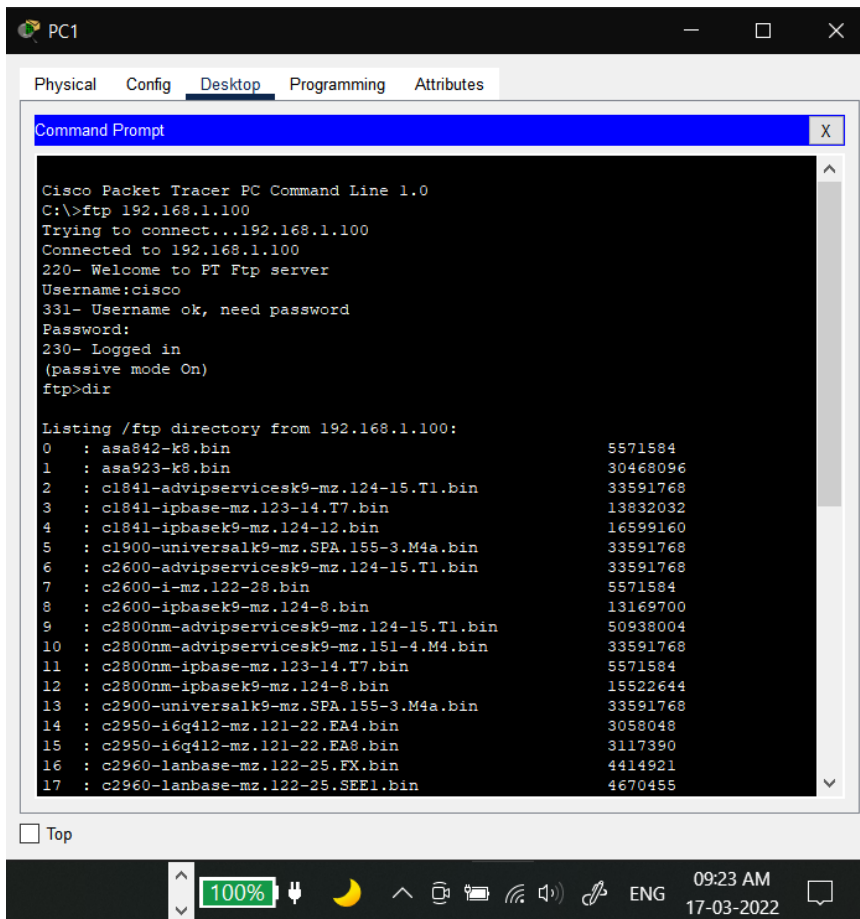
PC1 Web Browser (IP Packet): Successful





### Step 8: Showcasing PC0 and PC1's FTP Communication with Server





PC1

Physical Config Desktop Programming Attributes

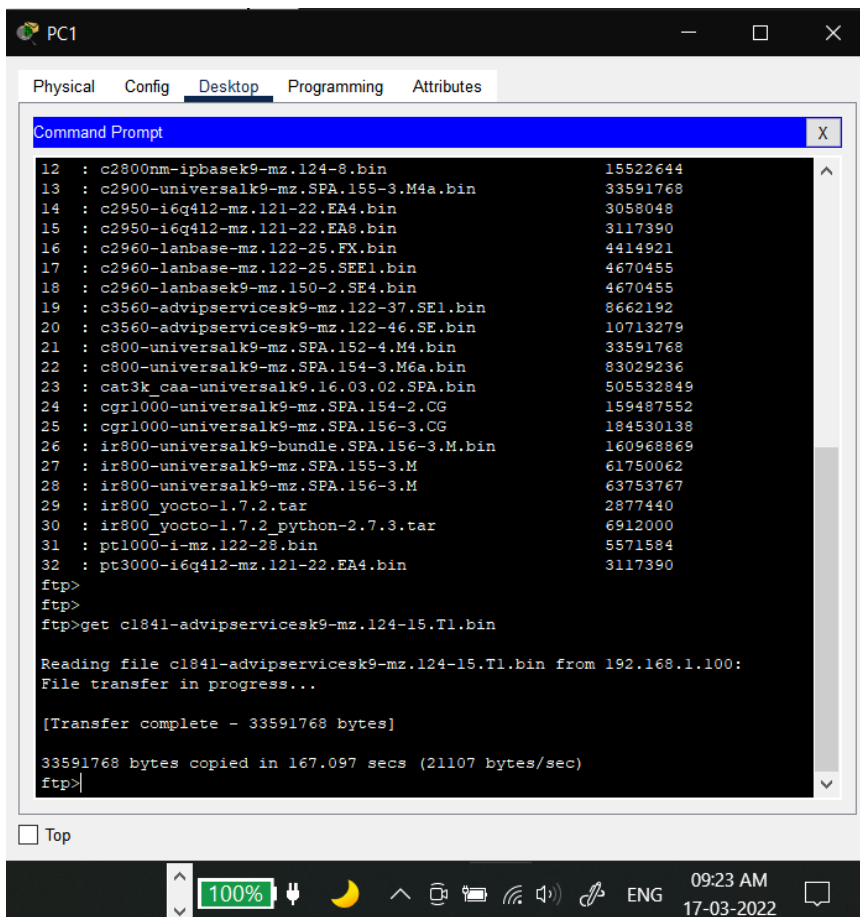
Command Prompt

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ftp 192.168.1.100
Trying to connect...192.168.1.100
Connected to 192.168.1.100
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>dir

Listing /ftp directory from 192.168.1.100:
 0 : asa842-k8.bin                      5571584
 1 : asa923-k8.bin                      30468096
 2 : c1841-advipservicesk9-mz.124-15.T1.bin 33591768
 3 : c1841-ipbase-mz.123-14.T7.bin       13832032
 4 : c1841-ipbasek9-mz.124-12.bin        16599160
 5 : c1900-universalk9-mz.SPA.155-3.M4a.bin 33591768
 6 : c2600-advipservicesk9-mz.124-15.T1.bin 33591768
 7 : c2600-i-mz.122-28.bin              5571584
 8 : c2600-ipbasek9-mz.124-8.bin         13169700
 9 : c2800nm-advipservicesk9-mz.124-15.T1.bin 50938004
10 : c2800nm-advipservicesk9-mz.151-4.M4.bin 33591768
11 : c2800nm-ipbase-mz.123-14.T7.bin     5571584
12 : c2800nm-ipbasek9-mz.124-8.bin       15522644
13 : c2900-universalk9-mz.SPA.155-3.M4a.bin 33591768
14 : c2950-i6q412-mz.121-22.EA4.bin     3058048
15 : c2950-i6q412-mz.121-22.EA8.bin     3117390
16 : c2960-lanbase-mz.122-25.FX.bin      4414921
17 : c2960-lanbase-mz.122-25.SEE1.bin    4670455
```

Top

100% 09:23 AM 17-03-2022



PC1

Physical Config Desktop Programming Attributes

Command Prompt

```
12 : c2800nm-ipbasek9-mz.124-8.bin          15522644
13 : c2900-universalk9-mz.SPA.155-3.M4a.bin 33591768
14 : c2950-i6q412-mz.121-22.EA4.bin        3058048
15 : c2950-i6q412-mz.121-22.EA8.bin        3117390
16 : c2960-lanbase-mz.122-25.FX.bin         4414921
17 : c2960-lanbase-mz.122-25.SEE1.bin       4670455
18 : c2960-lanbasek9-mz.150-2.SE4.bin       4670455
19 : c3560-advipservicesk9-mz.122-37.SE1.bin 8662192
20 : c3560-advipservicesk9-mz.122-46.SE.bin 10713279
21 : c800-universalk9-mz.SPA.152-4.M4.bin    33591768
22 : c800-universalk9-mz.SPA.154-3.M6a.bin   83029236
23 : cat3k-caa-universalk9.16.03.02.SPA.bin 505532849
24 : cgr1000-universalk9-mz.SPA.154-2.CG    159487552
25 : cgr1000-universalk9-mz.SPA.156-3.CG    184530138
26 : ir800-universalk9-bundle.SPA.156-3.M.bin 160968869
27 : ir800-universalk9-mz.SPA.155-3.M       61750062
28 : ir800-universalk9-mz.SPA.156-3.M       63753767
29 : ir800_yocto-1.7.2.tar                 2877440
30 : ir800_yocto-1.7.2_python-2.7.3.tar    6912000
31 : pt1000-i-mz.122-28.bin                5571584
32 : pt3000-i6q412-mz.121-22.EA4.bin       3117390

ftp>
ftp>
ftp>get c1841-advipservicesk9-mz.124-15.T1.bin

Reading file c1841-advipservicesk9-mz.124-15.T1.bin from 192.168.1.100:
File transfer in progress...

[Transfer complete - 33591768 bytes]

33591768 bytes copied in 167.097 secs (21107 bytes/sec)
ftp>
```

Top

100% 09:23 AM 17-03-2022

## Final Topology:

