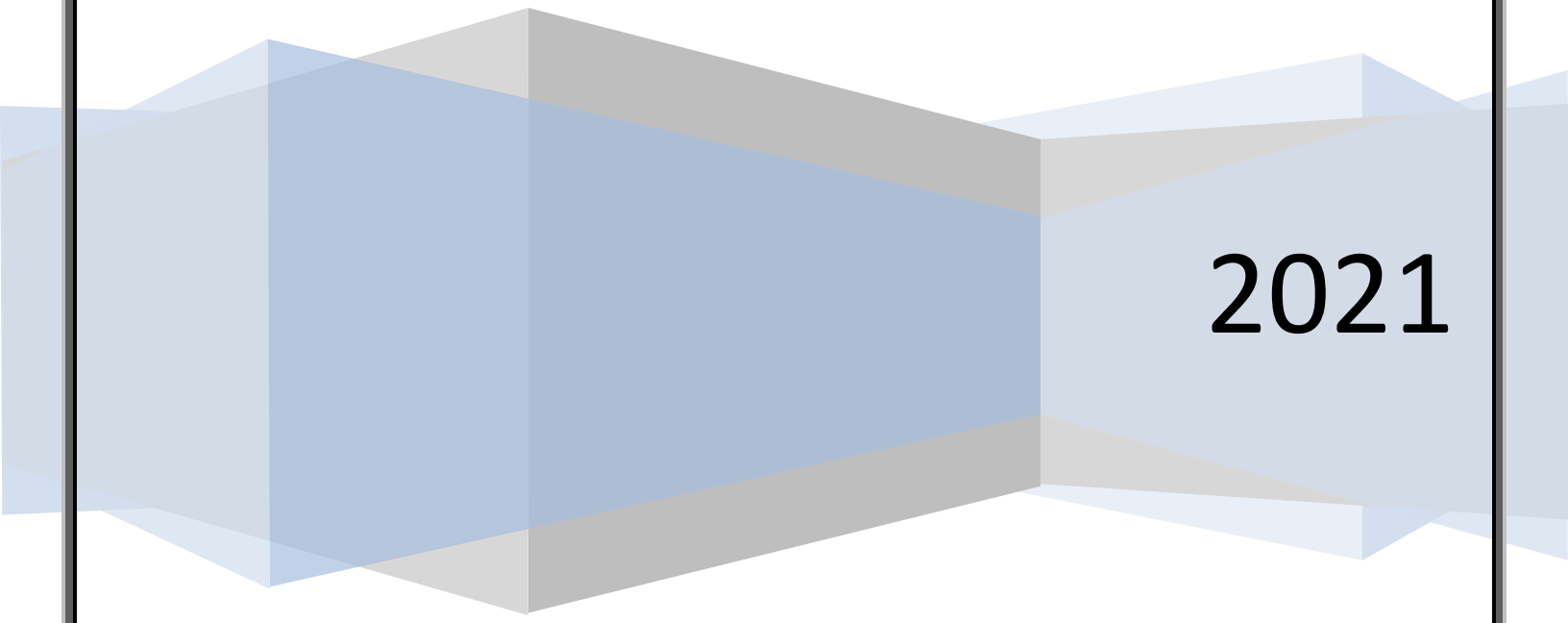
# SECURITY IN COMPUTING

## JOURNAL

**TYIT**



2021

| Practical no | Title | Date | Sign |
|---|---|---|---|
| 1 | Configure Cisco Routers for Syslog, NTP, and SSH Operations | | |
| 2 | Configuring Extended ACLs | | |
| 3 | Configure AAA Authentication | | |
| 4 | Configure IP ACLs to Mitigate Attacks | | |
| 5 | Configuring IPv6 ACLs | | |
| 6 | Configuring a Zone-Based Policy Firewall (ZPF) | | |
| 7 | Configure IOS Intrusion Prevention System (IPS) Using the CLI | | |
| 8 | Packet Tracer - Layer 2 Security | | |
| 9 | Layer 2 VLAN Security | | |

# PRACTICAL NO 1:

# Configure Cisco Routers for Syslog, NTP, and SSH Operations

## OSPF, MD5 Authentication

- OSPF is a routing protocol. Two routers speaking OSPF to each other exchange information about the routes they know about and the cost for them to getthere.
- When many OSPF routers are part of the same network, information about all ofthe routes in a network are learned by all of the OSPF routers within that network—technically called an **area**. (We'll talk more about area as we goon).
- Each OSPF router passes along information about the routes and costs they'veheard about to all of their adjacent OSPF routers, called**neighbors**.
- OSPF routers rely on **cost** to compute the shortest path through the networkbetween themselves and a remote router or networkdestination.
- The shortest path computation is done usingDjikstra's algorithm. This algorithm isn't uniquetoOSPF.Rather,it'samathematicalalgorithmthathappenstohaveanobvious application tonetworking.

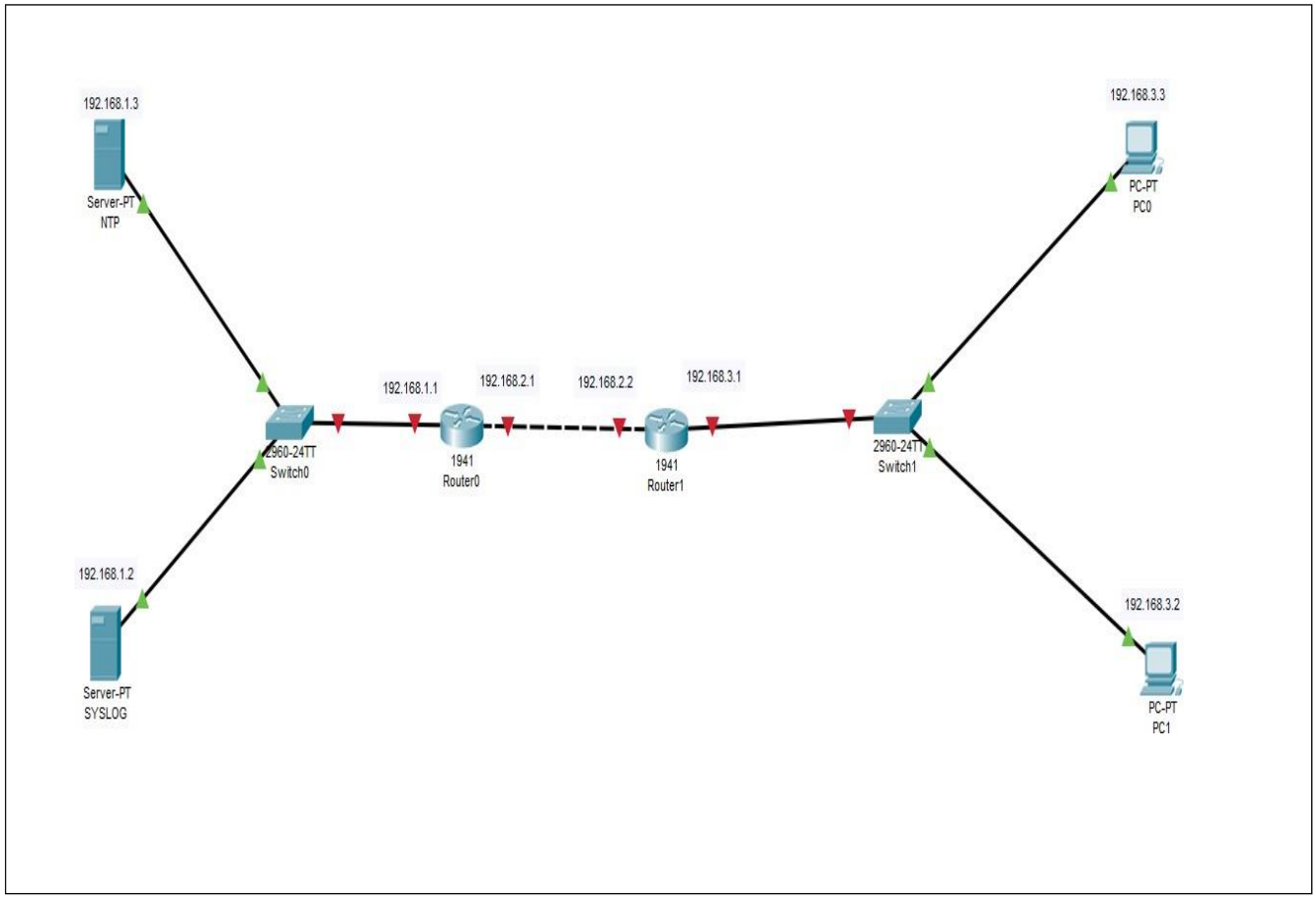
## MD5 Authentication

- MD5 authentication provides higher security than plain textauthentication.
- This method uses the MD5 algorithm to compute a hash value from the contents of the OSPF packet and a password (orkey).
- This hash value is transmitted in the packet, along with a key ID and a non-decreasing sequencenumber.
- The receiver, which knows the same password, calculates its own hashvalue.
- If nothing in the message changes, the hash value of the receiver should match thehash value of the sender which is transmitted with themessage.
- The key ID allows the routers to reference multiplepasswords.
- This makes password migration easier and moresecure.

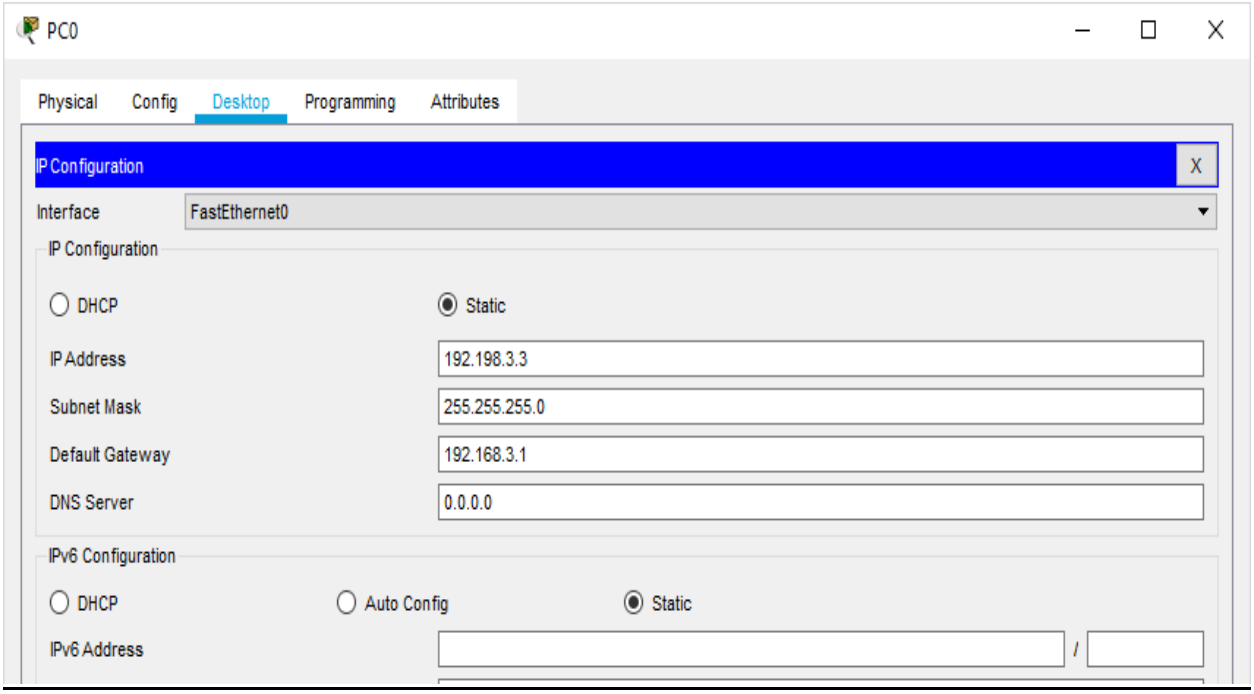
- For example, to migrate from one password to another, configure a password undera different key ID and remove the firstkey.
- The sequence number prevents replay attacks, in which OSPF packets arecaptured, modified, and retransmitted to arouter.
- As with plain text authentication, MD5 authentication passwords do not have to be the same throughout an area. However, they do need to be the same betweenneighbors.

## Example

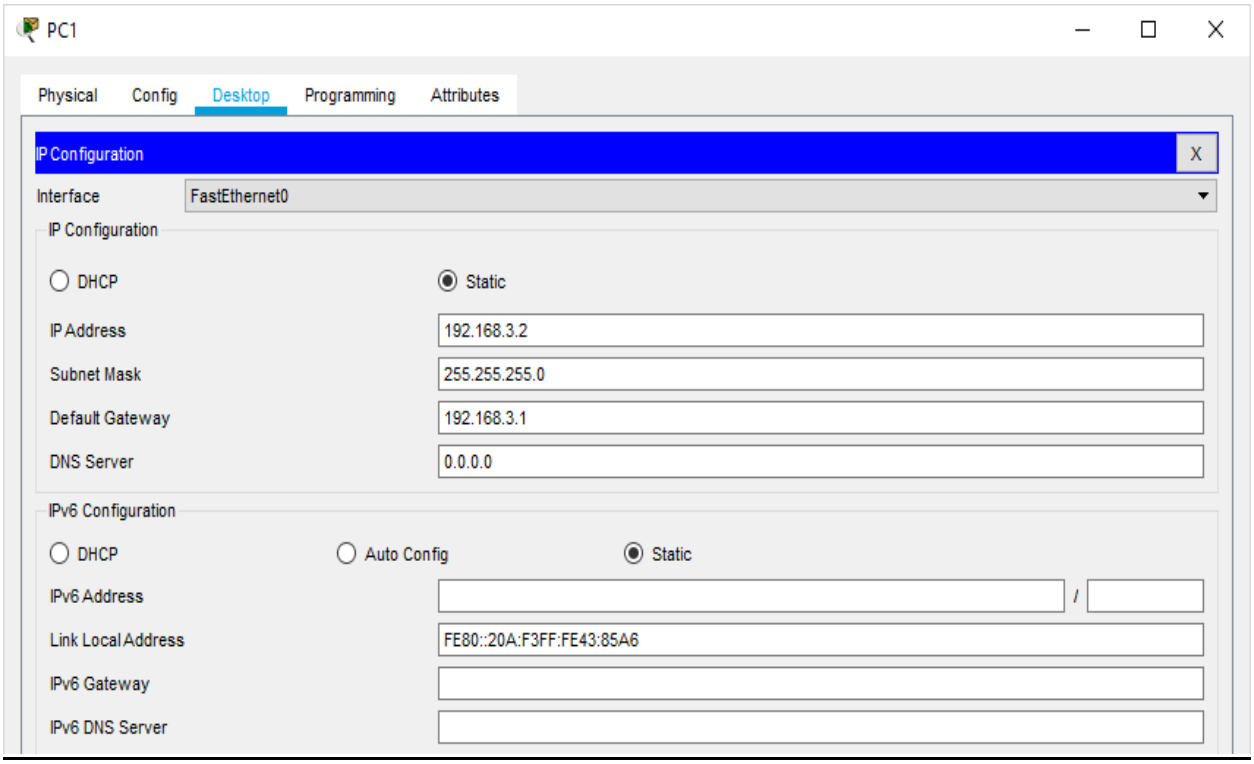
## Consider the following topology



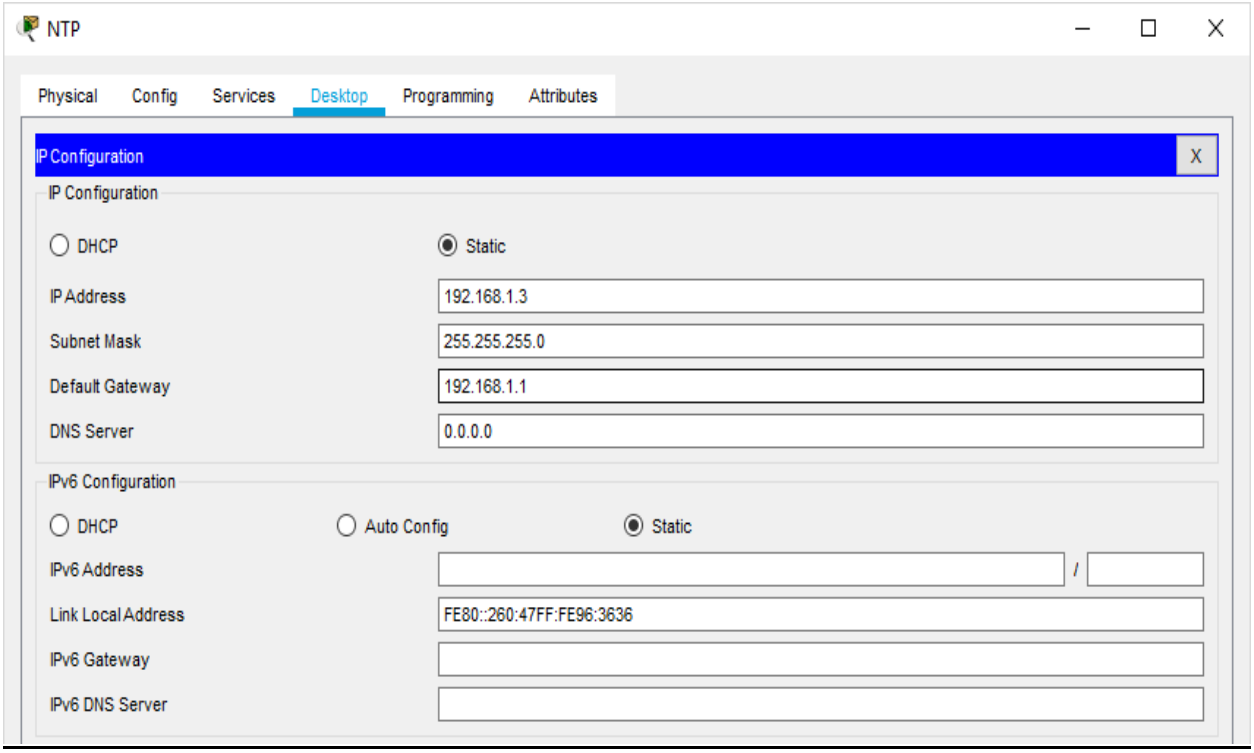
**ConfiguringPC0**



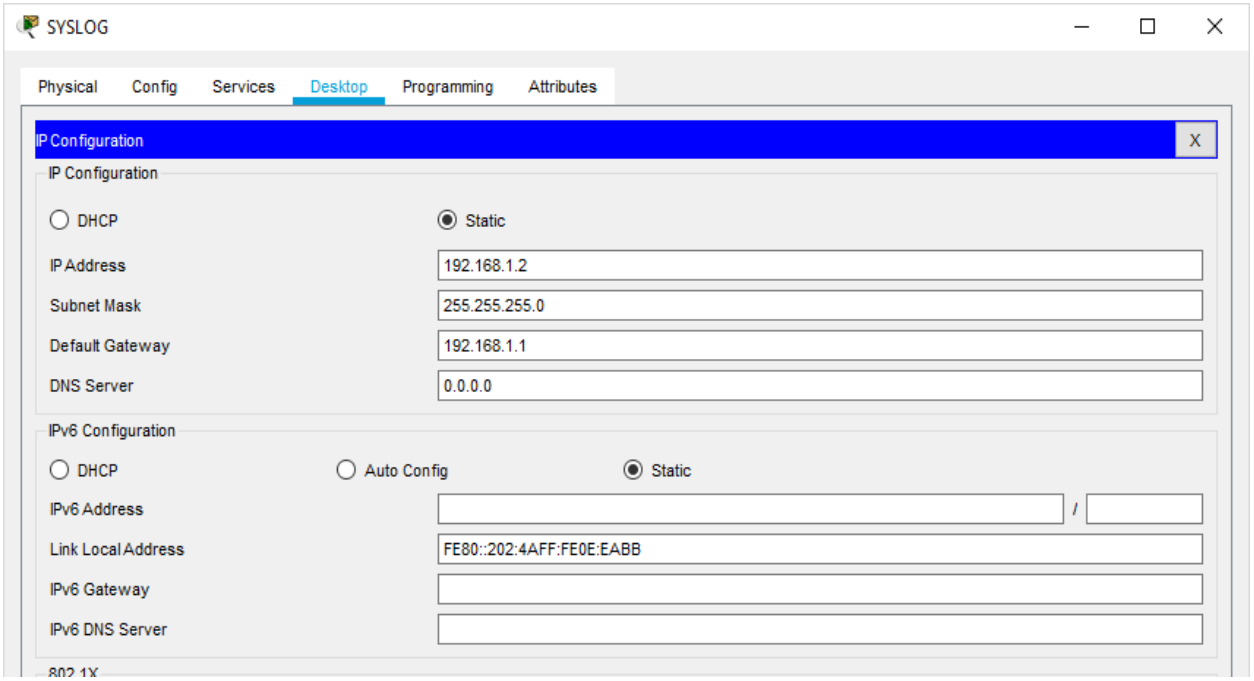

**ConfiguringPC1**



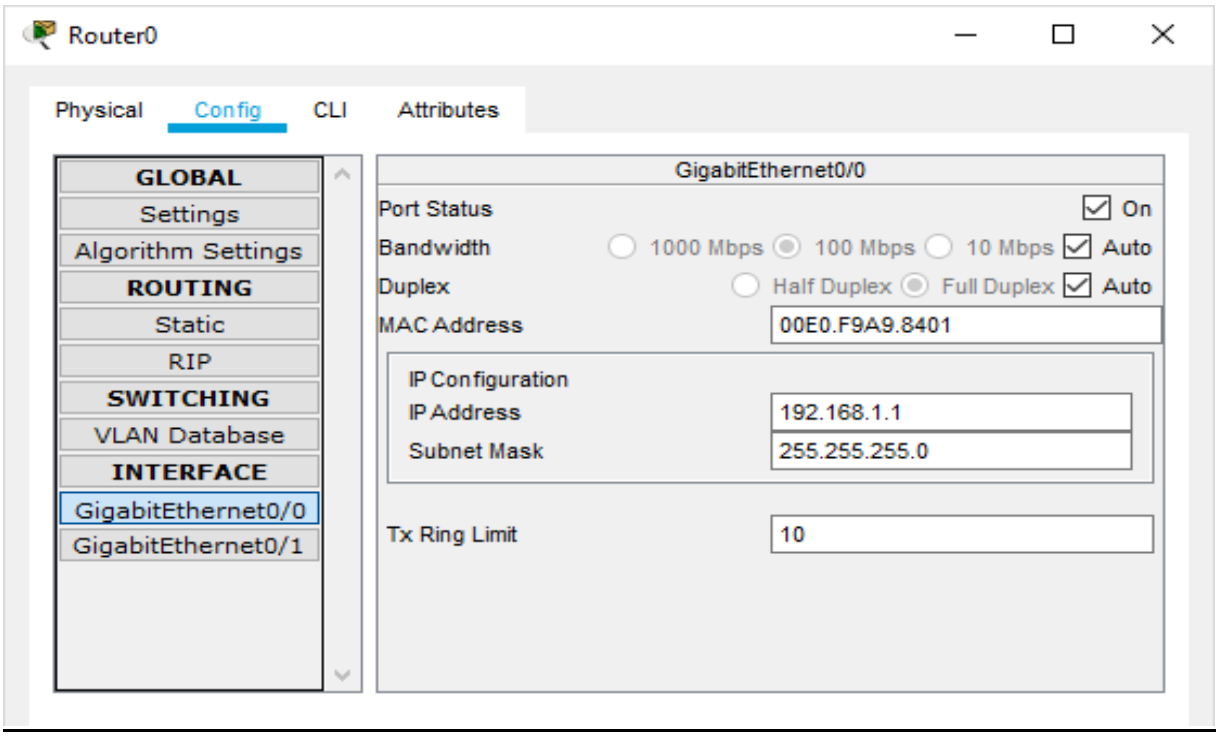
## Configuring NTP Server

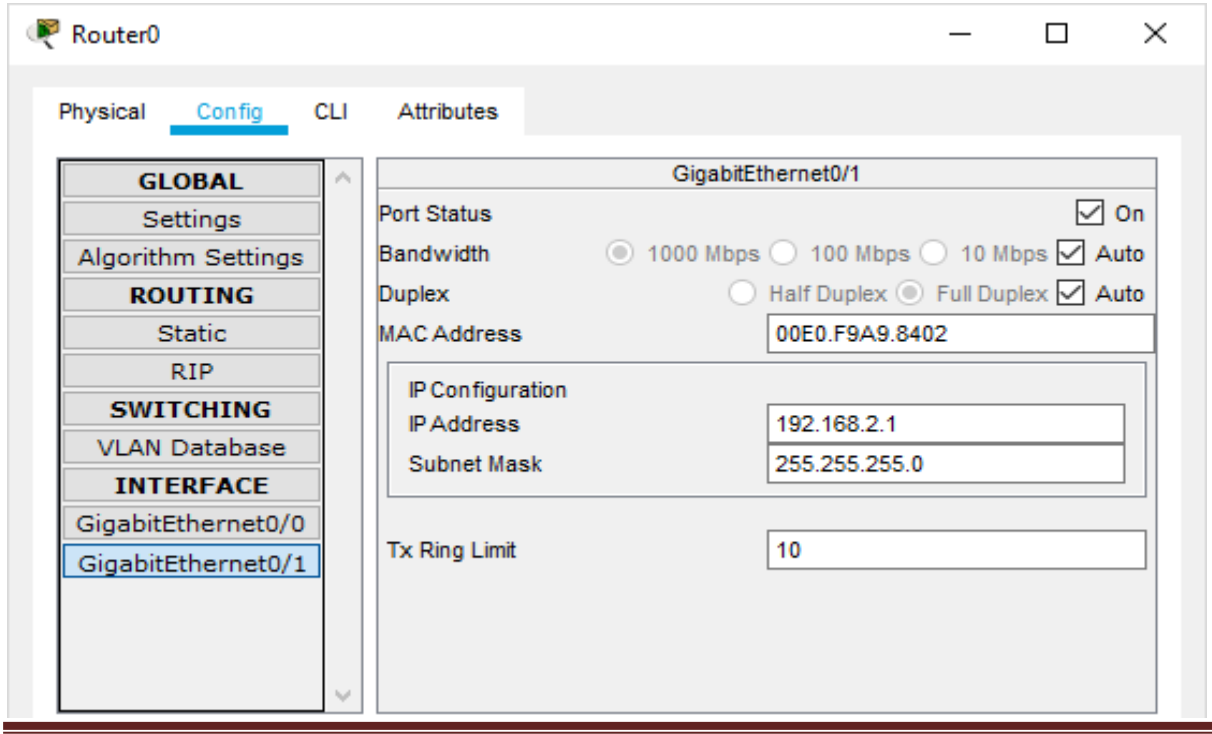



## Configuring SYSLOG Server

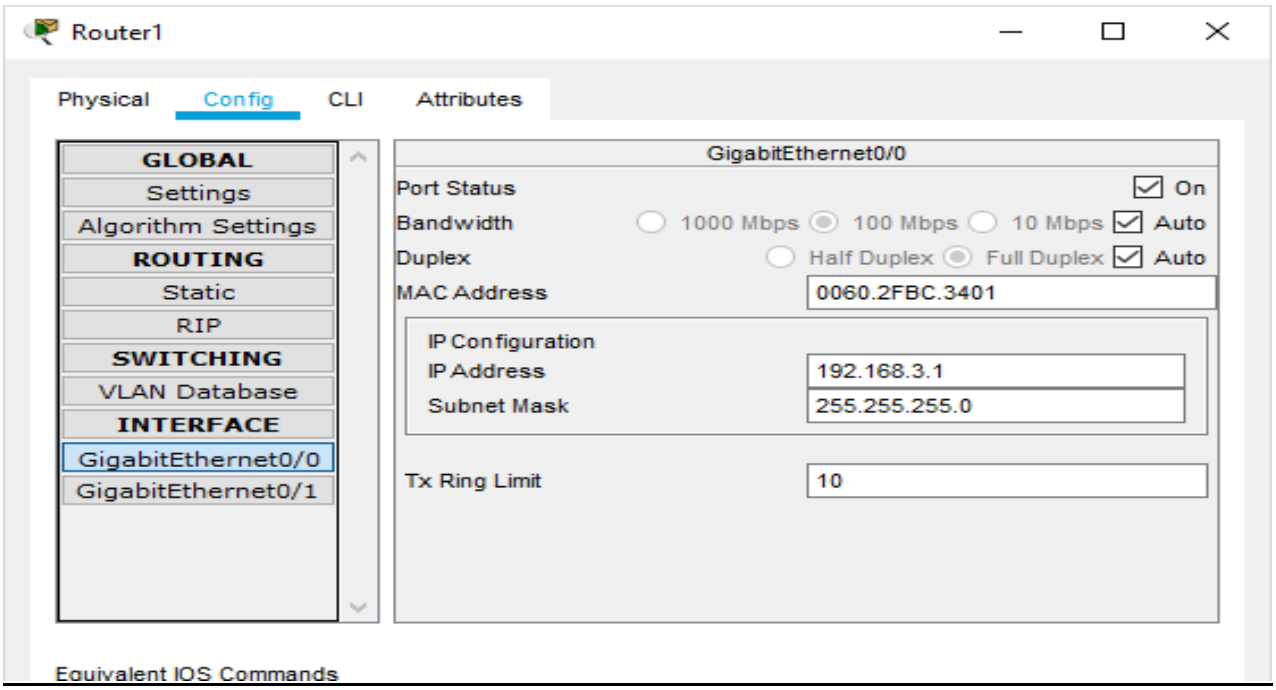


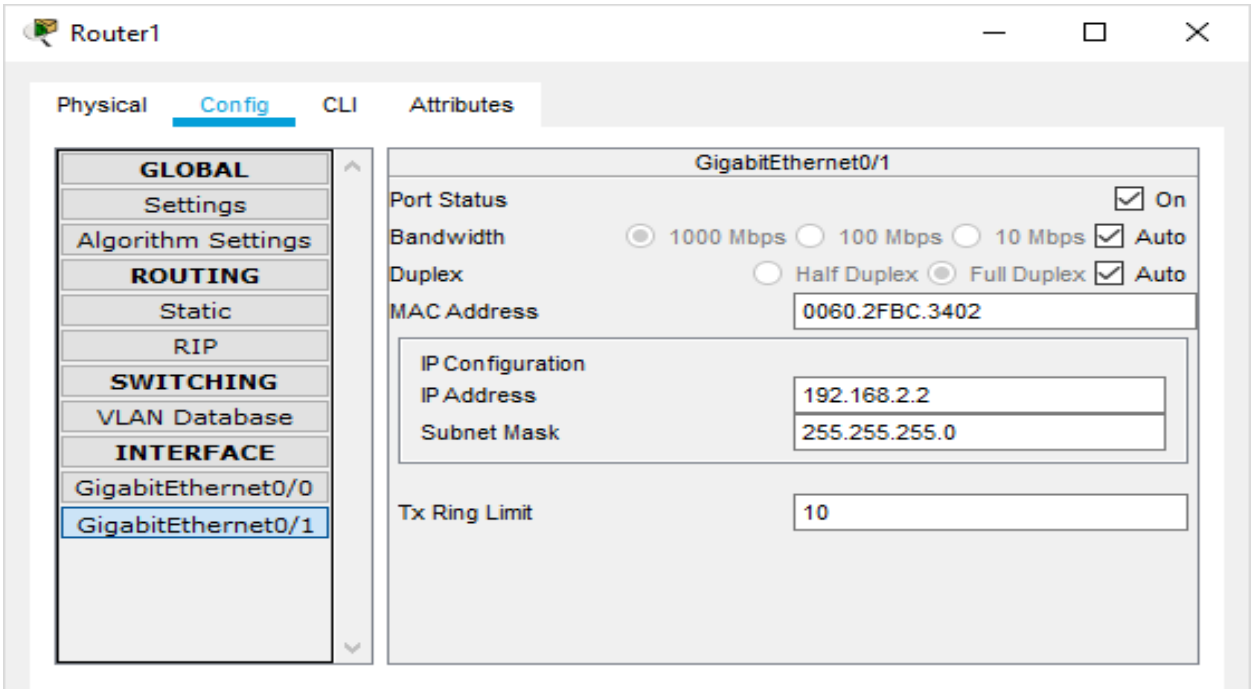
**Configuring Router0**



**Configuring Router1**



## Part 1: Configure OSPF MD5 Authentication

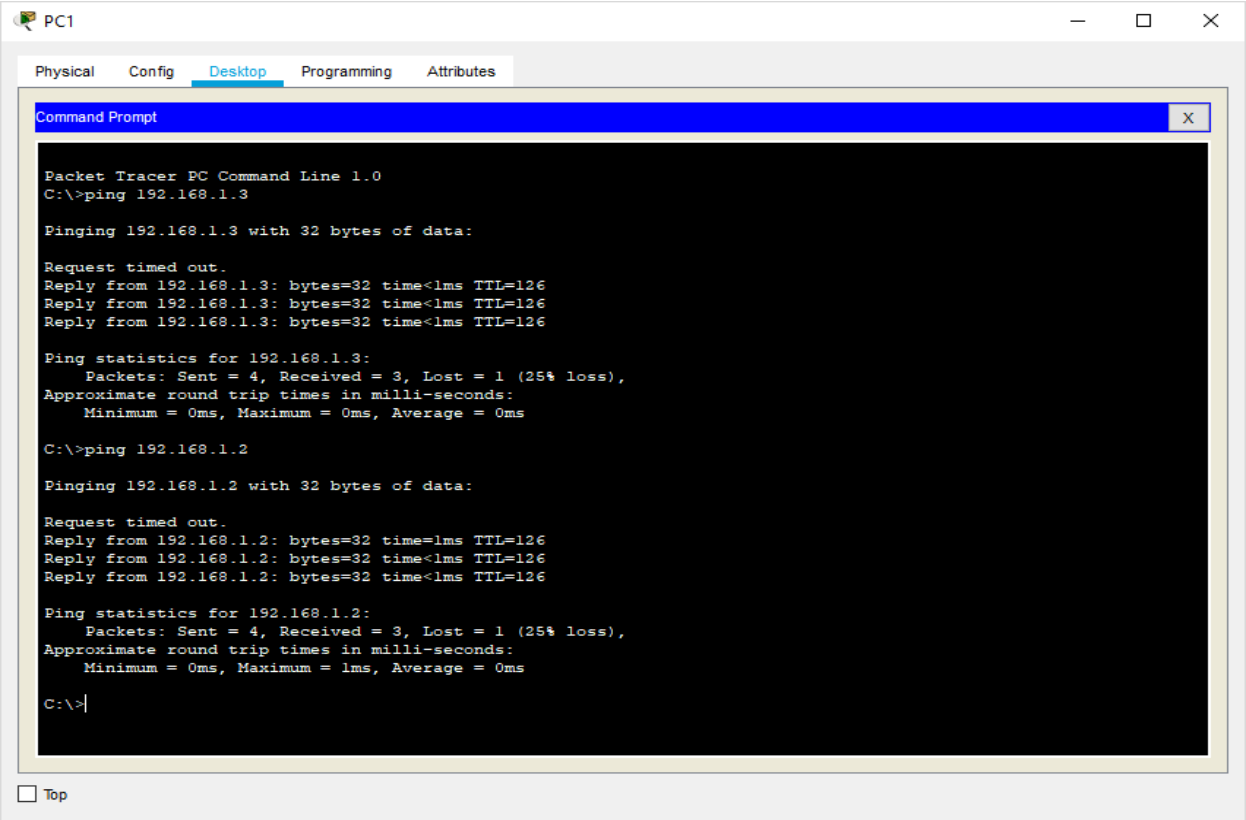
**ROUTER 0: Type the following command in the CLI mode**

```
Router>enable
Router#configure terminal
Router(config)#router ospf 1
Router(config-router)#network 192.168.1.0 0.255.255.255 area 1
Router(config-router)#network 192.168.2.0 0.255.255.255 area 1
Router(config-router)#exit
Router(config)#exit
Router#
```

**ROUTER 1: Type the following command in the CLI mode**

```
Router>enable
Router#configure terminal
Router(config)#router ospf 1
Router(config-router)#network 192.168.3.0 0.255.255.255 area 1
Router(config-router)#network 192.168.2.0 0.255.255.255 area 1
Router(config-router)#exit
Router(config)#exit
Router#
```

**Now we verify the connectivity by using the following**



Hence OSPF has been verified

## MD5 Authentication

### ROUTER 0: Type the following command in the CLI mode

```
Router>enable
Router#
Router#configure terminal
Router(config)#interface GigabitEthernet0/1
Router(config-if)#ip ospf authentication message-digest
Router(config-if)#ip ospf message-digest-key 1 md5 smile
Router(config-if)#exit
Router(config)#exit
```

### ROUTER 1: Type the following command in the CLI mode

```
Router>enable
Router#
Router#configure terminal
Router(config)#interface GigabitEthernet0/1
Router(config-if)#ip ospf authentication message-digest
Router(config-if)#ip ospf message-digest-key 1 md5 smile
Router(config-if)#exit
Router(config)#exit
```

## Verify the MD5 Authentication using the following command in the CLI mode of Router0

Router#show ip ospf  interface gigabitEthernet 0/1

**We get the following output:**

```
GigabitEthernet0/1 is up, line protocol is up
Internet address is 192.168.2.1/24, Area 1
Process ID 1, Router ID 192.168.2.1, Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State BDR, Priority 1
Designated Router (ID) 192.168.3.1, Interface address 192.168.2.2
Backup Designated Router (ID) 192.168.2.1, Interface address 192.168.2.1
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
```

Hello due in 00:00:06
Index 2/2, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1, Adjacent neighbor count is 1
Adjacent with neighbor 192.168.3.1 (Designated Router)
Suppress hello for 0 neighbor(s)
**Message digest authentication enabled**
Youngest key id is 1

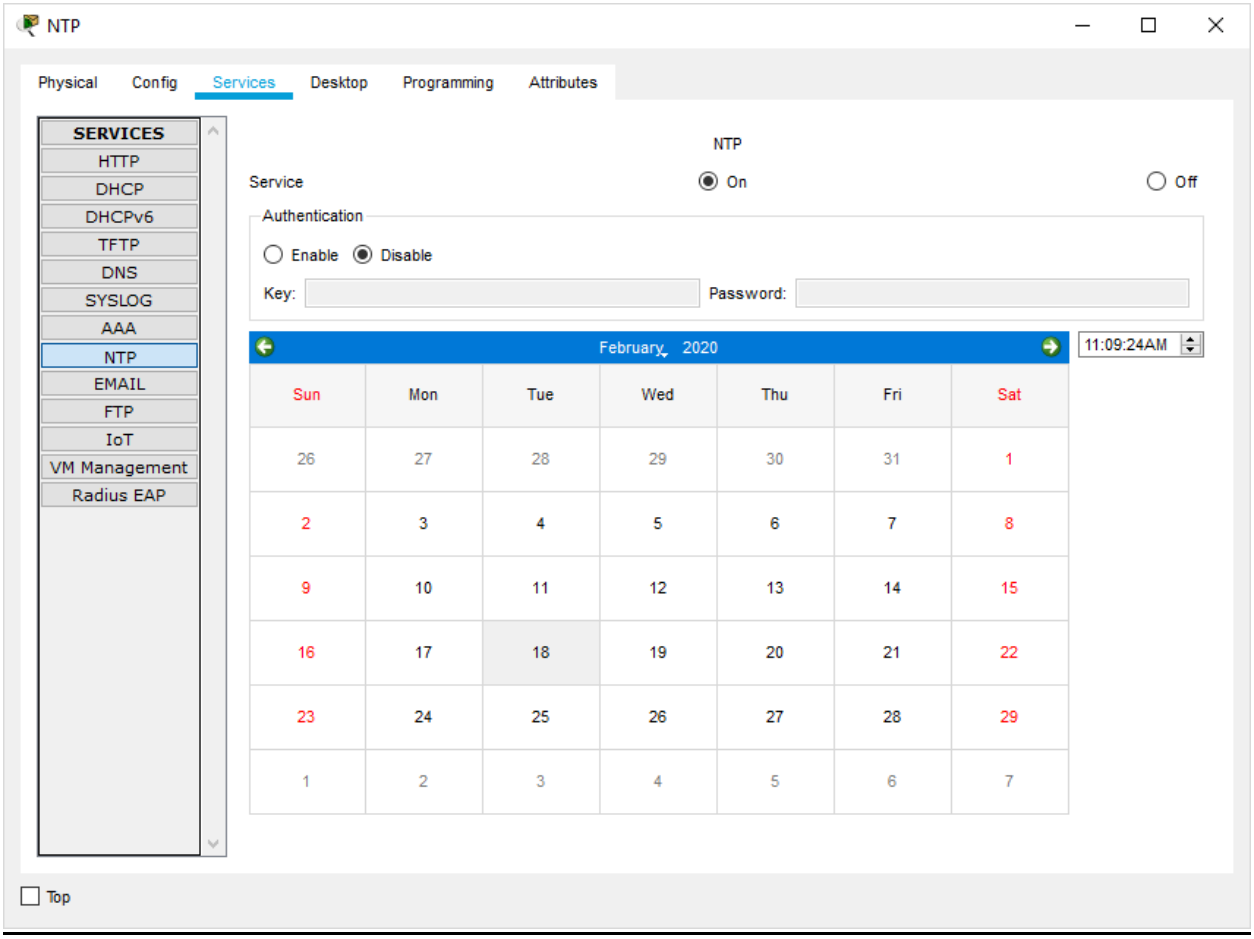
## MD5 Authentication has been verified

## b) NTP

- Network Time Protocol (NTP) is a TCP/IP protocol used tosynchronize computer clocks across datanetworks.
- NTP was developed in the 1980s by D.L. Mills at the University of Delaware to achieve highly accurate time synchronization and to sustain the effectsof variable latency over packet-switched data networks through a jitterbuffer.

We use the same topology to study the given protocol

## Configure NTP Server and enable the NTP service




**We must disable the NTP service on other servers else output won't be obtained**

**Now Go to CLI Mode of Router4 and type the following commands on both theRouters**

```
Router#config
Router#configure t
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ntp server 192.168.1.3
Router(config)#ntp up
Router(config)#ntp update-calendar
Router(config)#exit
Router#
```

**To verify the Output we use the following command**

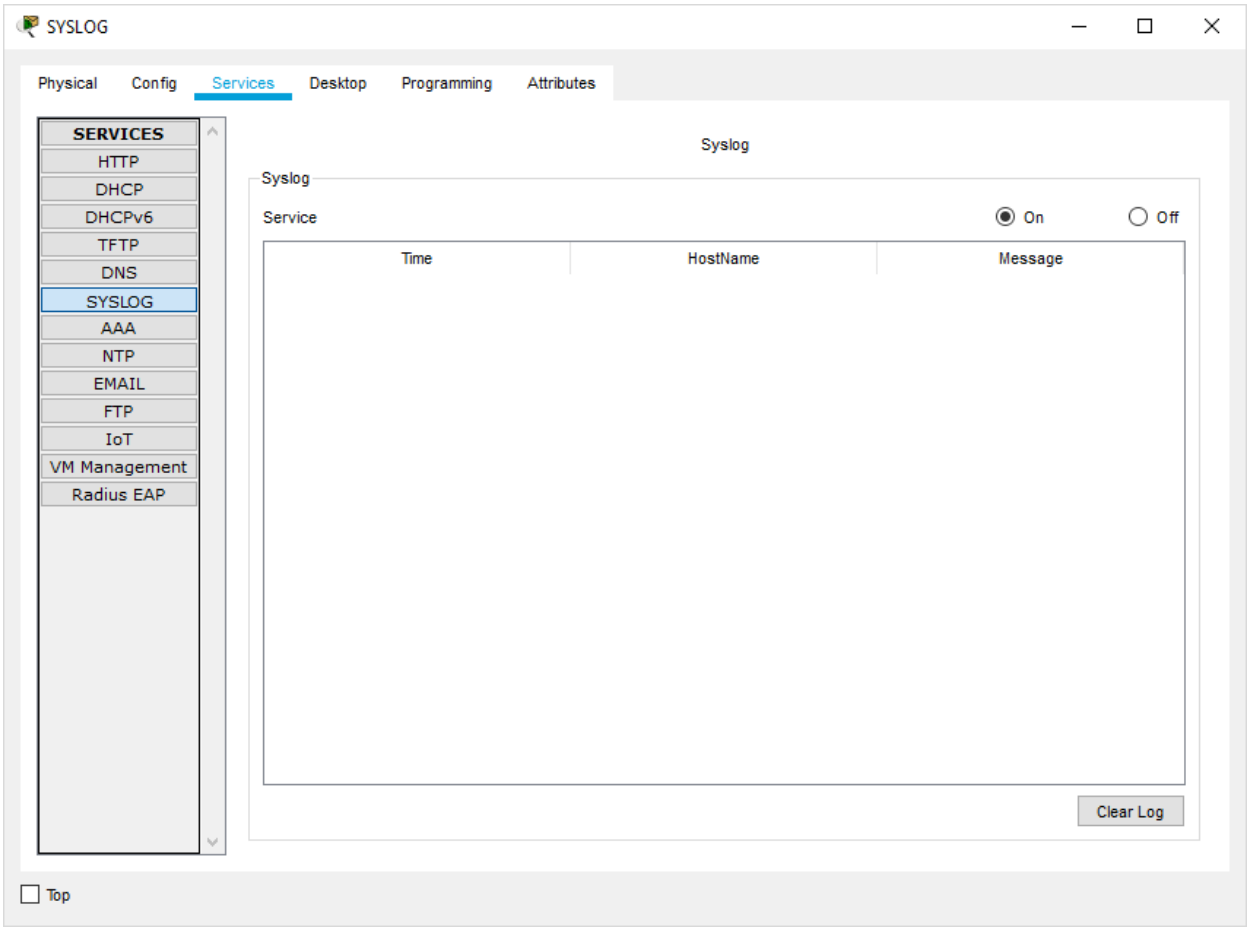
```
Router#show clock
11:14:58.985 UTC Tue Feb 18 2020
Router#
```

## c) SYSLOG server

**Configure SYSLOG Server and enable the service**

- Syslog is a way for network devices to send event messages to a loggingserver – usually known as a Syslog server.
- The Syslog **protocol** is supported by a wide range of devices and can be usedto log different types ofevents.
- For example, a router might send messages about users logging on toconsole sessions, while a web-server might log access-deniedevents.

## Turn ON the SYSLOG service on the server

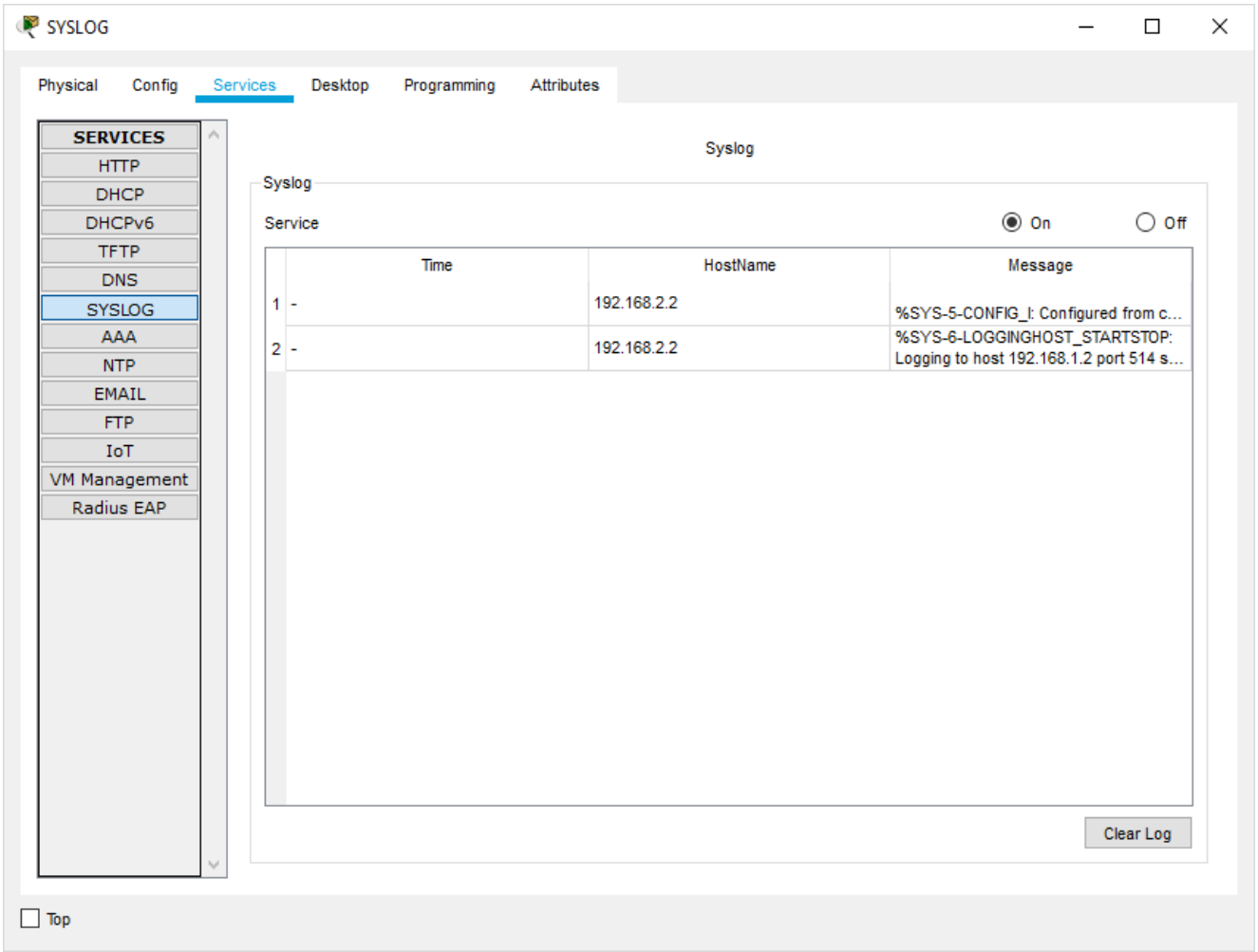



**And Turn OFF on all other Servers**

**Now Go to CLI Mode of any Router and type the following commands in all theRouters.**

```
Router#
Router#configure terminal
Router(config)#logging 192.168.1.2
Router(config)#exit
Router#
```

**Output:**



## d) SSH

- An **SSH server** is a software program which uses the secure shell protocol to accept connections from remotecomputers.
- The way **SSH works** is by making use of a client-server model to allow for authentication of two remote systems and encryption of the data that passes betweenthem.
- It organizes the secure connection by authenticating the client and opening the correct shell environment if the verification issuccessful.

**Now Go to CLI Mode of Router0 and type the following commands.**

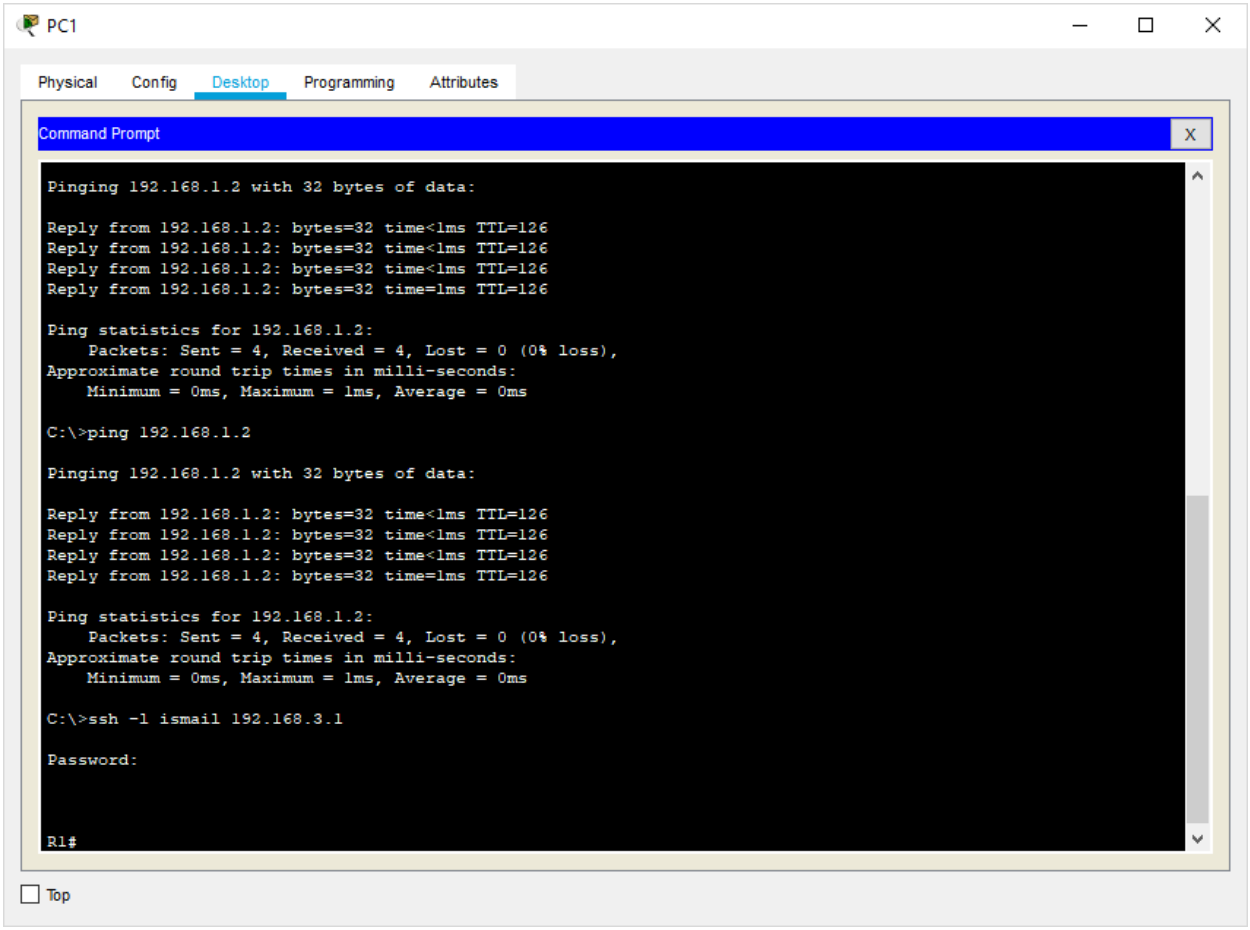
```
Router#configure terminal
Router(config)#ip domain-name ismail.com
Router(config)#hostname R1
R1(config)#
R1(config)#crypto key generate rsa


The name for the keys will be: R1.ismail.com
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.


R1(config)#line vty 0 4
R1(config-line)#transport input ssh
R1(config-line)#login local
R1(config-line)#exit
R1(config)#username ismail privilege 15 password cisco
R1(config)#
```

**Output: Go to cmd of PC1 and type the command**

**ssh –l ismail 192.168.3.1 and type the password cisco**




**Hence SSH is also verified**

SIC JOURNAL TYIT

# PRACTICAL NO 2: Configure ACLs

**The Cisco Access Control List (ACL)** are used for filtering traffic based on a given filtering criteria on a router or switch interface. Based on the conditions supplied by the ACL, a packet is allowed or blocked from further movement.

Cisco ACLs are available for several types of routed protocols including IP, IPX, AppleTalk, XNS, DECnet, and others. However, we will be discussing ACLs pertaining to TCP/IP protocol only.

ACLs for TCP/IP traffic filtering are primarily divided into two types:

- Standard Access Lists, and
- Extended Access Lists

## Standard Access Control Lists:

Standard IP ACLs range from 1 to 99. A Standard Access List allows you to permit or deny traffic FROM
specific IP addresses. The destination of the packet and the ports involved can be

anything. This is the command syntax format of a standard ACL.

**access-list** *access-list-number* {permit|deny} {host|source source-

wildcard|any} Standard ACL

example:

access-list 10 permit 192.168.2.0 0.0.0.255

This list allows traffic from all addresses in the range 192.168.2.0 to 192.168.2.255

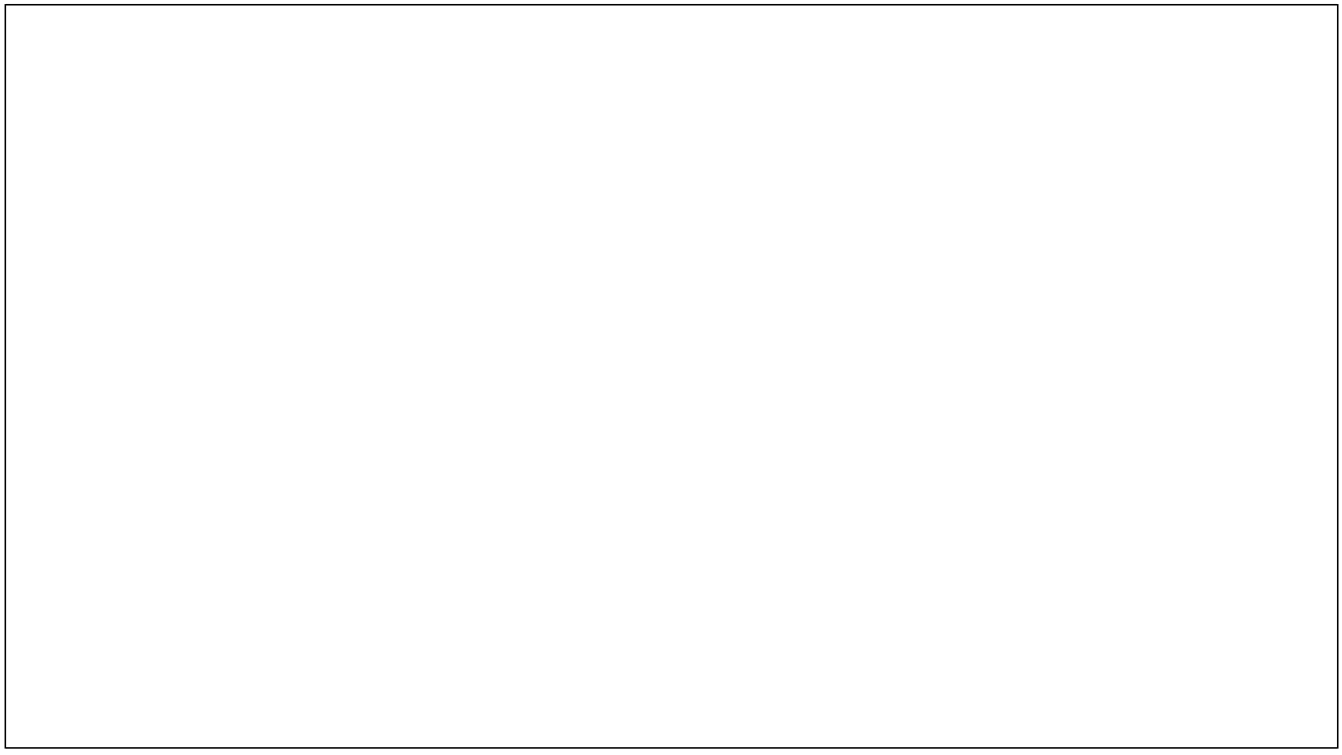
Note that when configuring access lists on a router, you must identify each access list uniquely by assigning either a name or a number to the protocol's access list.

There is an implicit deny added to every access list. If you entered the command:

show access-list 10

The output looks like:

access-list 10 permit 192.168.2.0 0.0.0.255 access-list 10 deny any



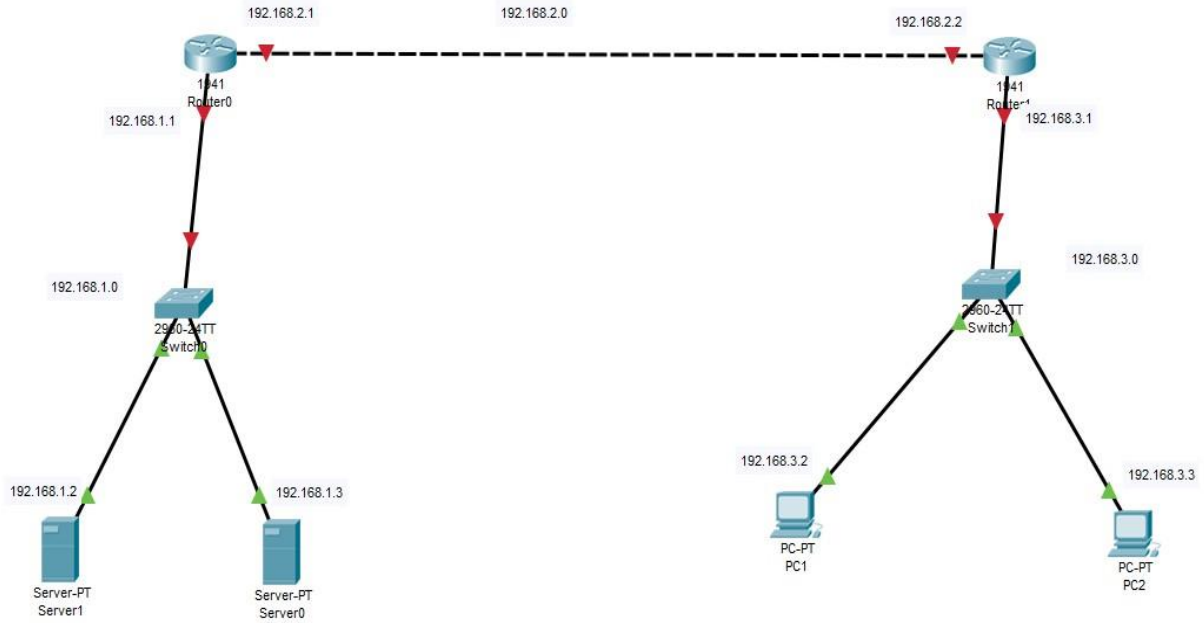
SIC JOURNAL TYIT

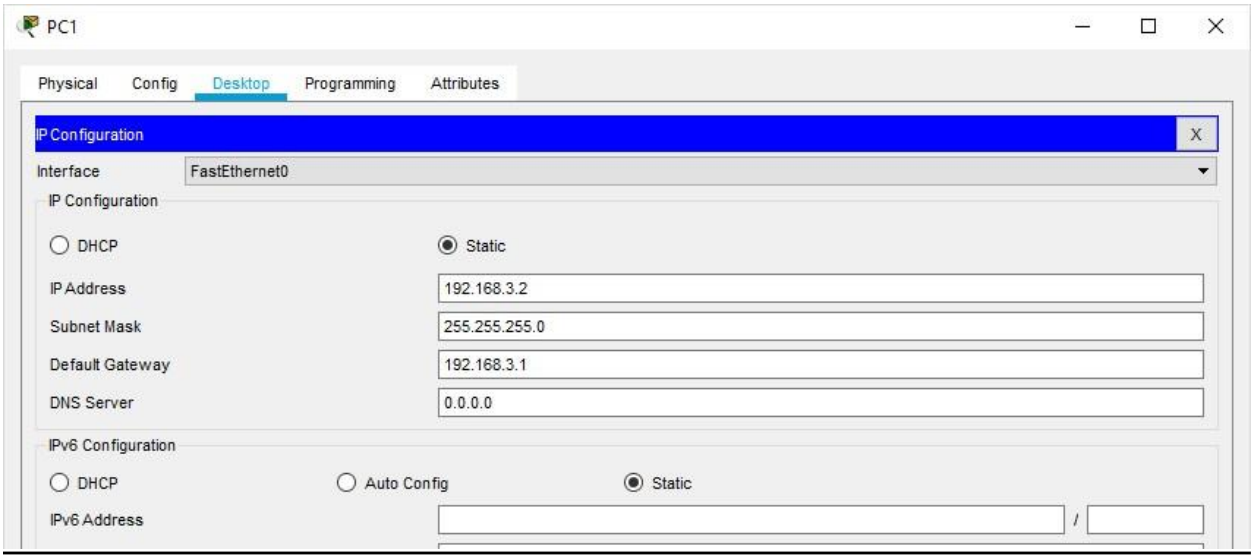
**access-list** access-list-number {deny | permit} protocol source source-wildcard *destination* destination-wildcard [precedence precedence]
Note that the above syntax is simplified, and given for general understanding only.
Extended ACL example:
access-list 110 - Applied to traffic leaving the office (outgoing)
access-list 110 permit tcp 92.128.2.0 0.0.0.255 any eq 80
ACL 110 permits traffic originating from any address on the 92.128.2.0 network. The 'any' statement means that the traffic is allowed to have any destination address with the limitation of going to port 80. The value of 0.0.0.0/255.255.255.255 can be specified as 'any'.

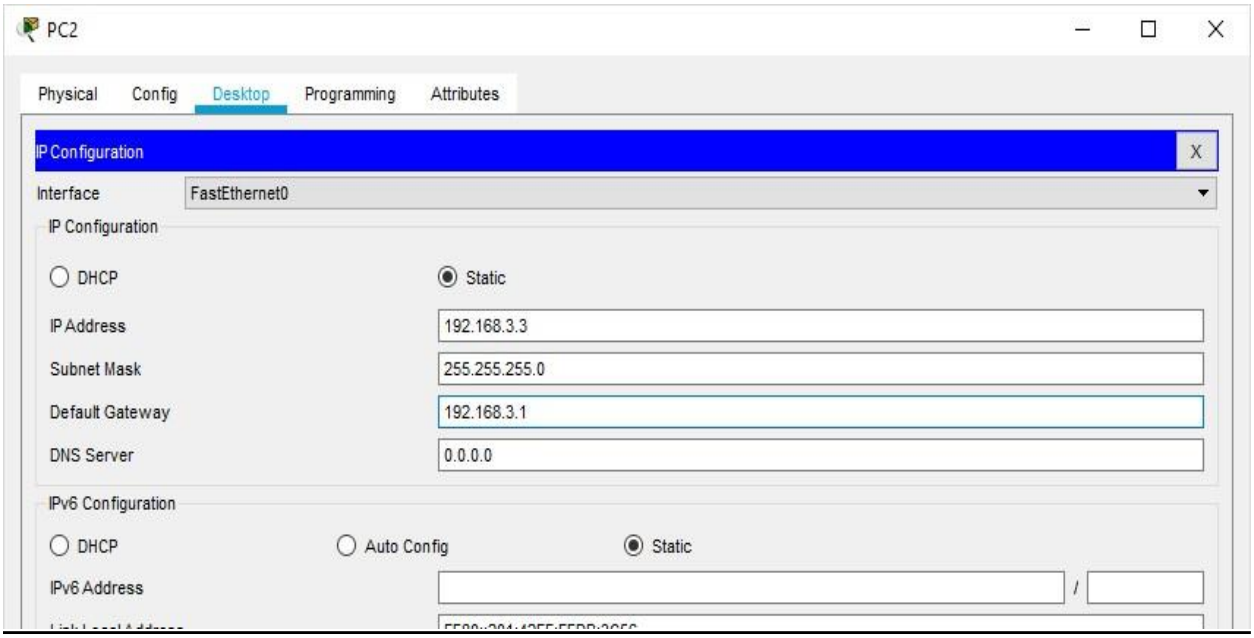
**Applying an ACL to a router interface:**

After the ACL is defined, it must be applied to the interface (inbound or outbound). The syntax for applying an ACL to a router interface is given below:
interface <interface>
ip access-group {number|name} {in|out}
An Access List may be specified by a name or a number. "in" applies the ACL to the inbound traffic, and "out" applies the ACL on the outbound traffic.
Example: To apply the standard ACL created in the previous example, use the following commands:
Rouer(config)#interface serial0
Rouer(config-if)#ip access-group 10 out

## Consider the following topology




PC1
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IP Address
192.168.3.2
Subnet Mask
255.255.255.0
Default Gateway
192.168.3.1
DNS Server
0.0.0.0
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address

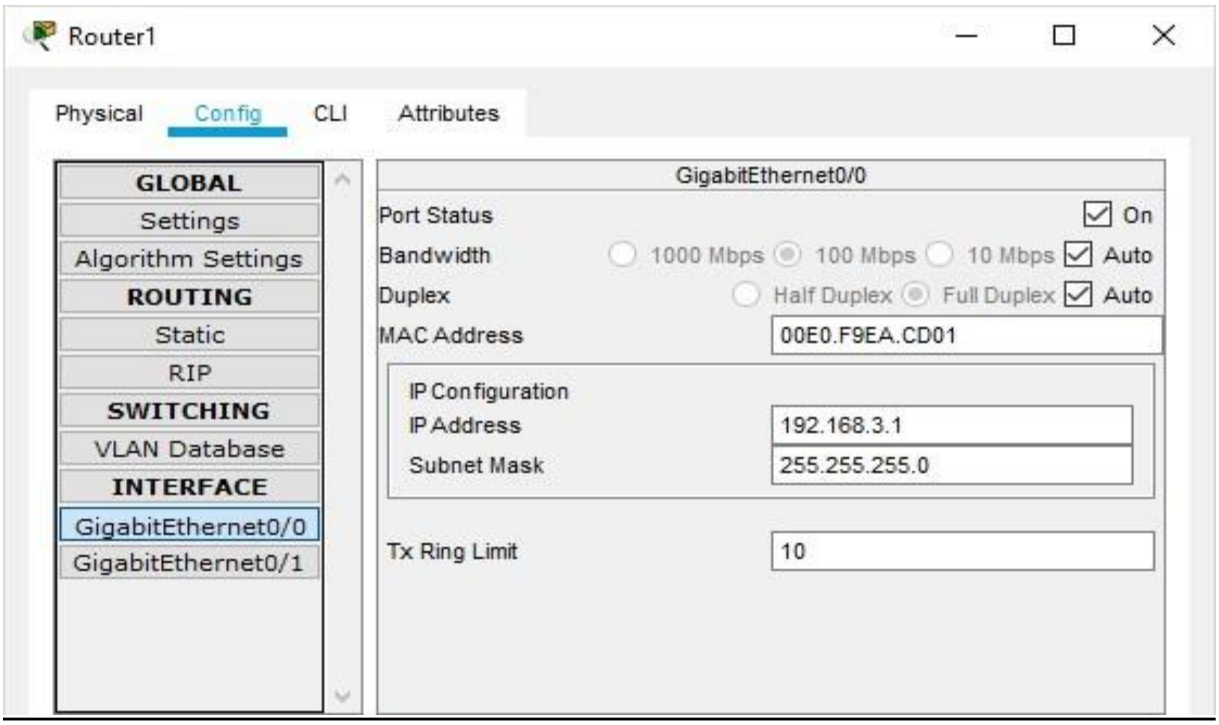

PC2
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IP Address
192.168.3.3
Subnet Mask
255.255.255.0
Default Gateway
192.168.3.1
DNS Server
0.0.0.0
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address

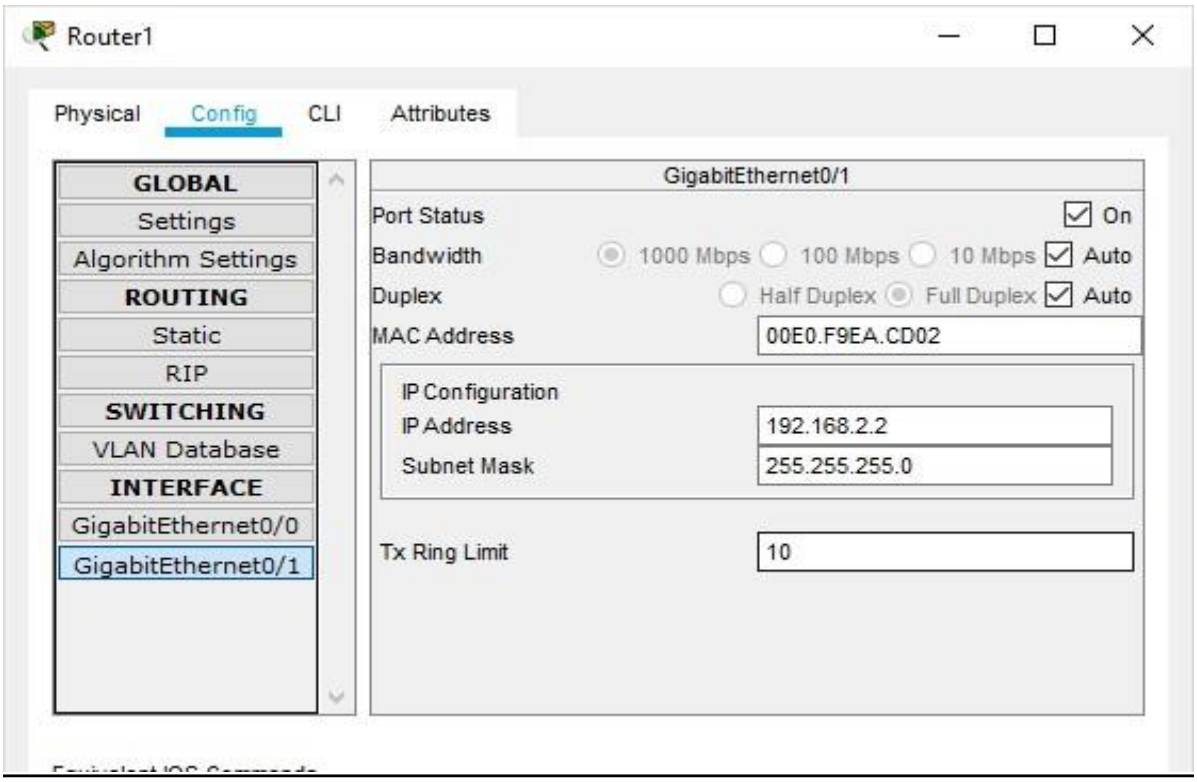
SIC JOURNAL TYIT

## Part 1: Configure, Apply and Verify an Extended Numbered ACL

**Configuring PC1**

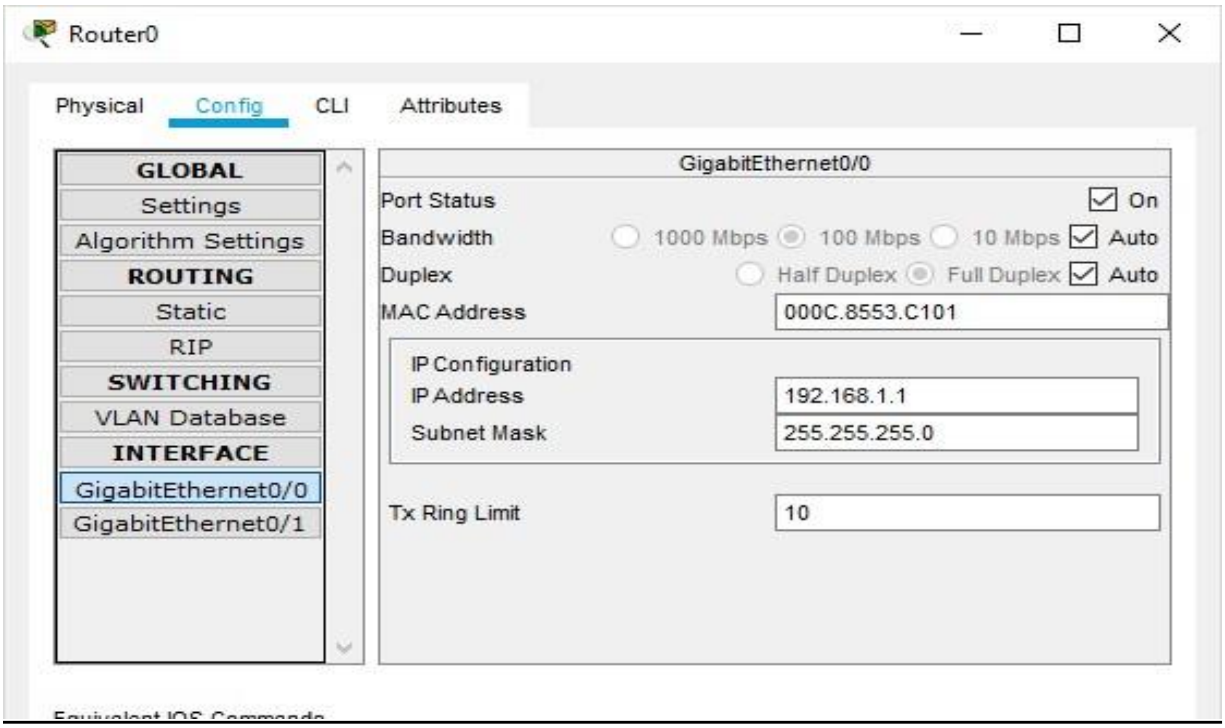
**Configuring PC2**

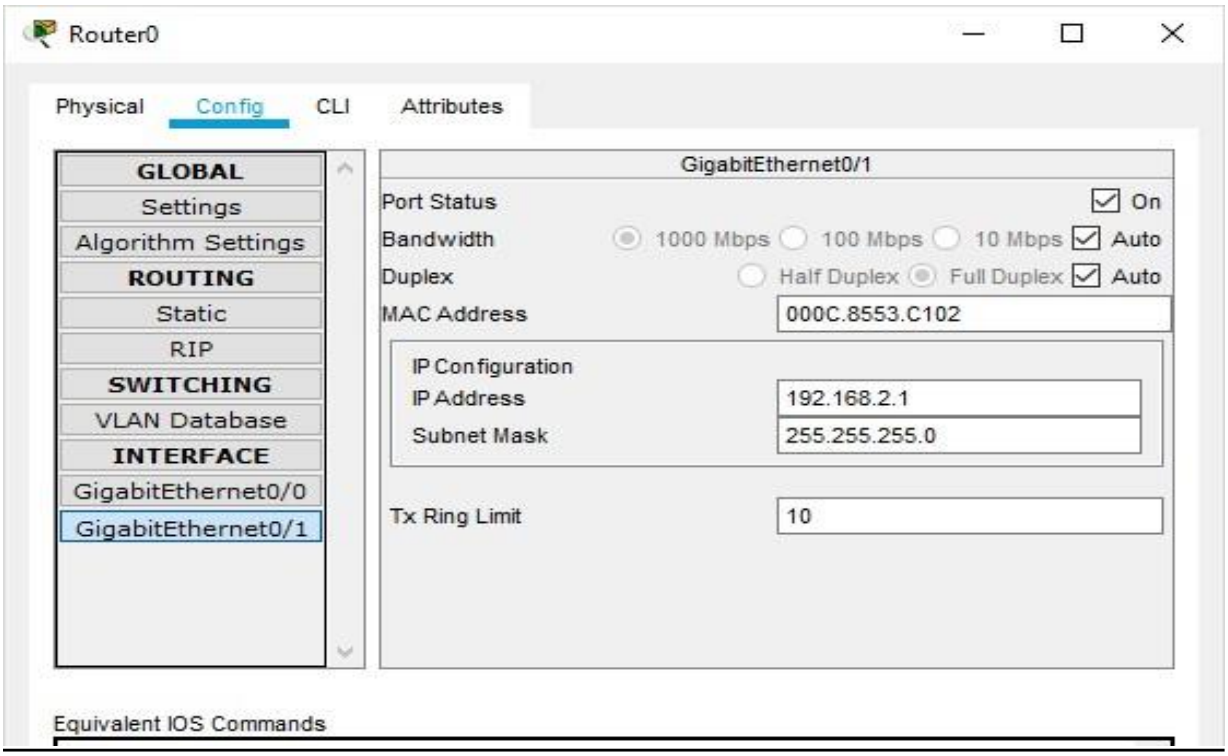

Router1
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0
GigabitEthernet0/1
GigabitEthernet0/0
Port Status
On
Bandwidth
1000 Mbps
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
00E0.F9EA.CD01
IP Configuration
IP Address
192.168.3.1
Subnet Mask
255.255.255.0
Tx Ring Limit
10


Router1
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0
GigabitEthernet0/1
GigabitEthernet0/1
Port Status
On
Bandwidth
1000 Mbps
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
00E0.F9EA.CD02
IP Configuration
IP Address
192.168.2.2
Subnet Mask
255.255.255.0
Tx Ring Limit
10

SIC JOURNAL TYIT

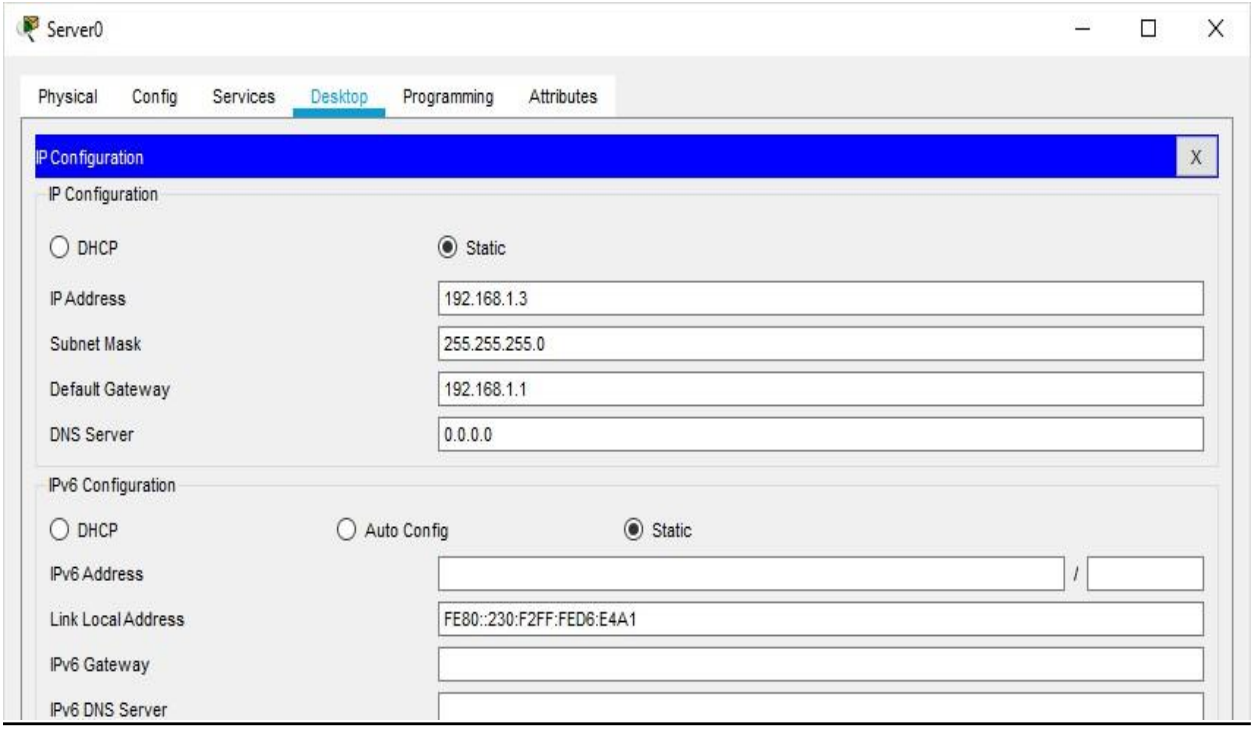
**Configuring Router1**

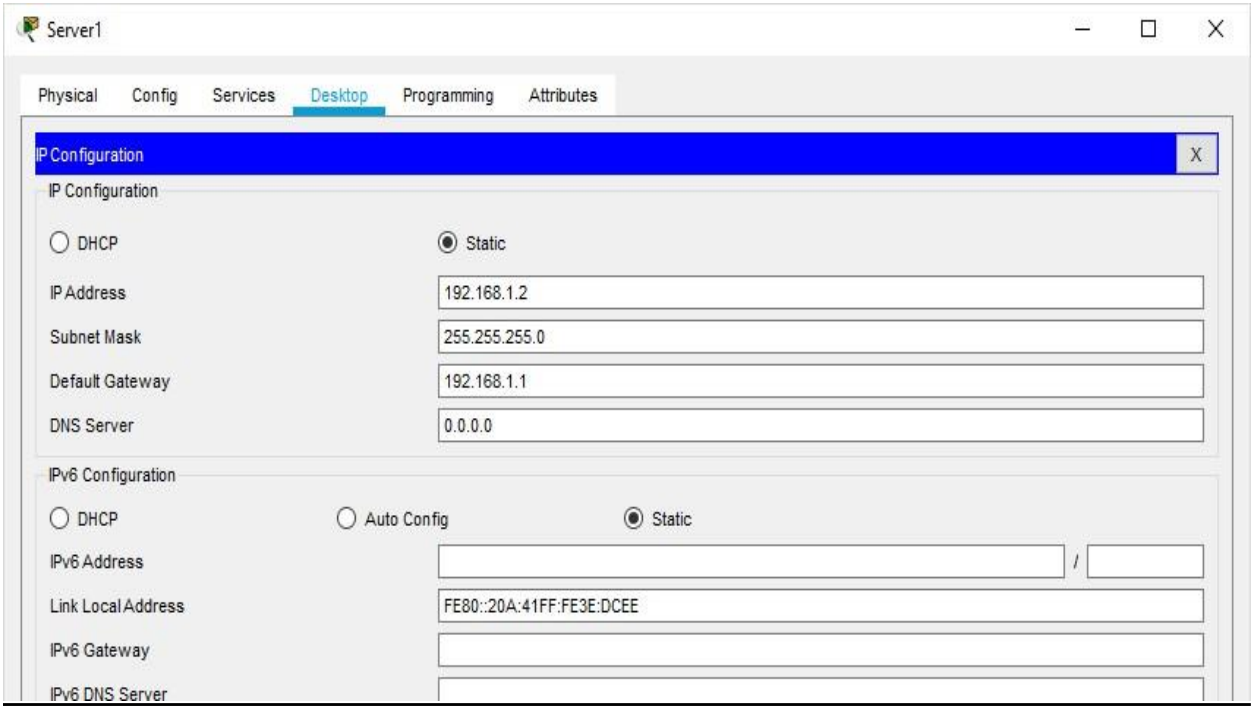

Router0
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0
GigabitEthernet0/1
GigabitEthernet0/0
Port Status
On
Bandwidth
1000 Mbps
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
000C.8553.C101
IP Configuration
IP Address
192.168.1.1
Subnet Mask
255.255.255.0
Tx Ring Limit
10


Router0
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0
GigabitEthernet0/1
GigabitEthernet0/1
Port Status
On
Bandwidth
1000 Mbps
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
000C.8553.C102
IP Configuration
IP Address
192.168.2.1
Subnet Mask
255.255.255.0
Tx Ring Limit
10
Equivalent IOS Commands

SIC JOURNAL TYIT

**Configuring Router0**


Server0
Physical
Config
Services
Desktop
Programming
Attributes
IP Configuration
X
IP Configuration
DHCP
Static
IP Address
192.168.1.3
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.1
DNS Server
0.0.0.0
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address
FE80::230:F2FF:FED6:E4A1
IPv6 Gateway
IPv6 DNS Server


Server1
Physical
Config
Services
Desktop
Programming
Attributes
IP Configuration
X
IP Configuration
DHCP
Static
IP Address
192.168.1.2
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.1
DNS Server
0.0.0.0
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address
FE80::20A:41FF:FE3E:DCEE
IPv6 Gateway
IPv6 DNS Server

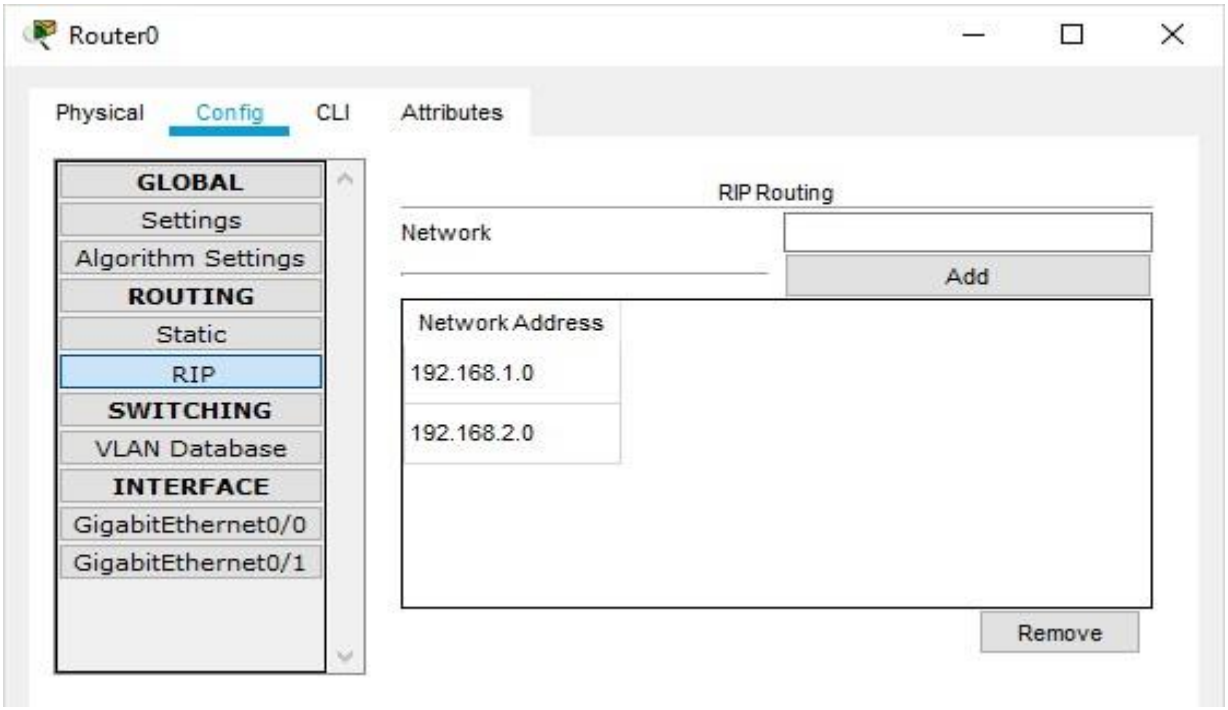
SIC JOURNAL TYIT

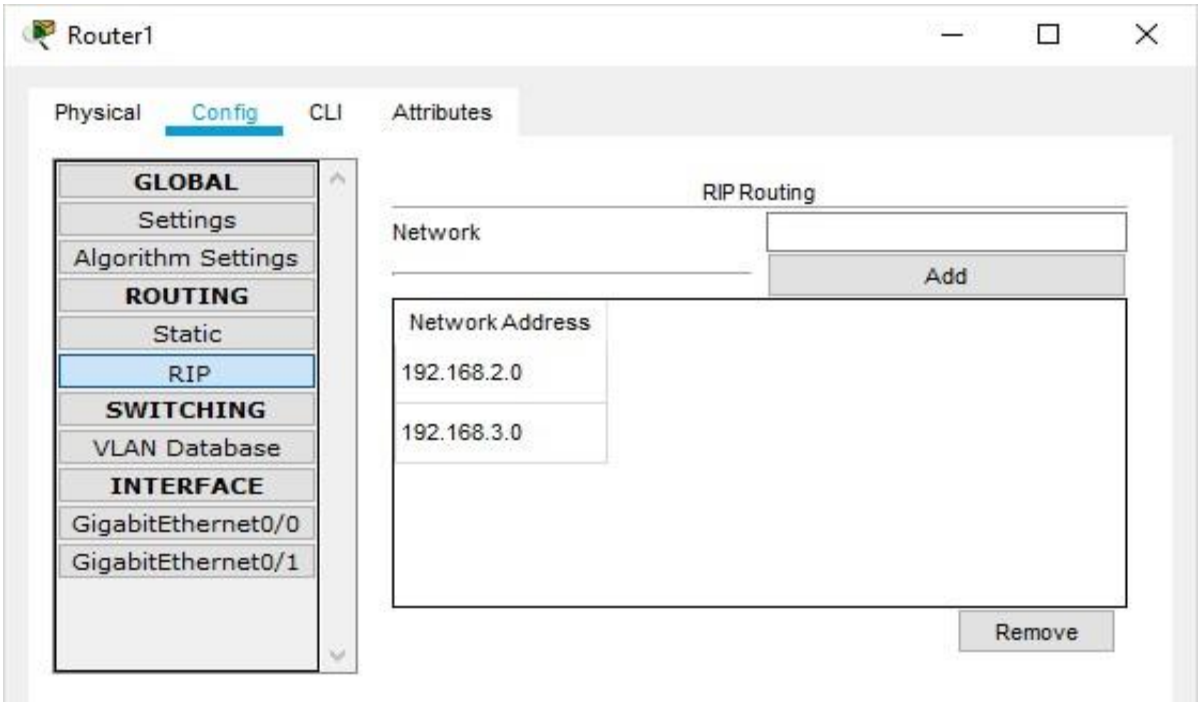
**Configuring Server0**

**Configuring Server1**

SIC JOURNAL TYIT

**Set the RIP protocol on both the Routers as follows**




**Check the connectivity by using the ping command**

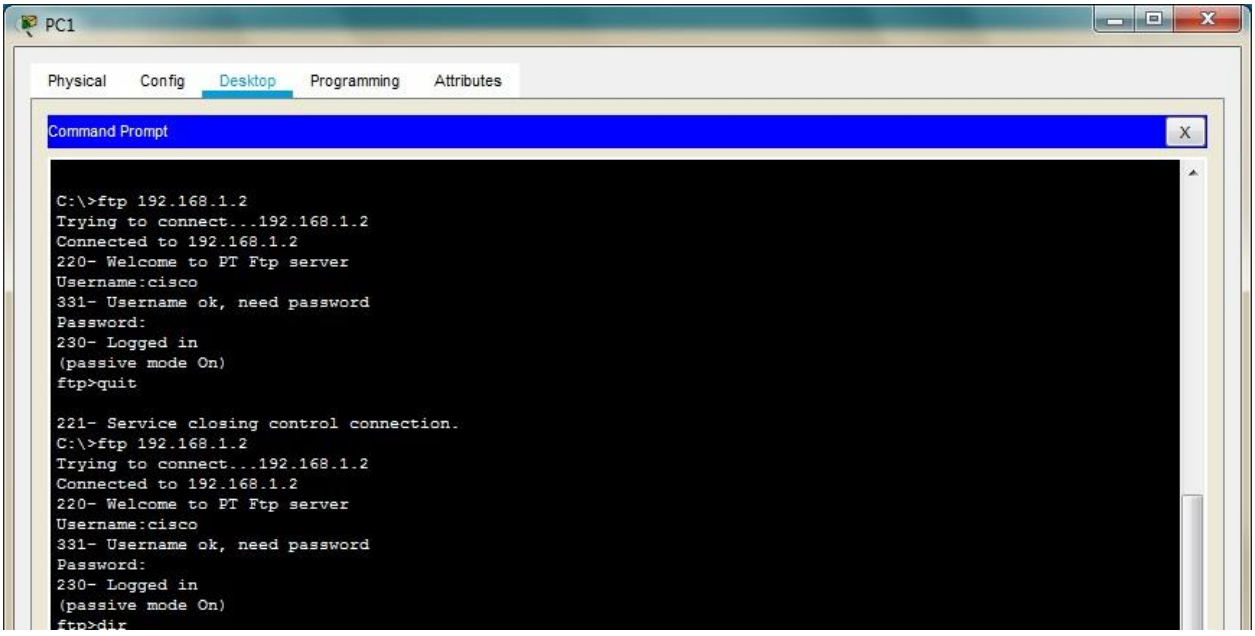
SIC JOURNAL TYIT

**Part 1: Configure, Apply and Verify an Extended Numbered ACL**

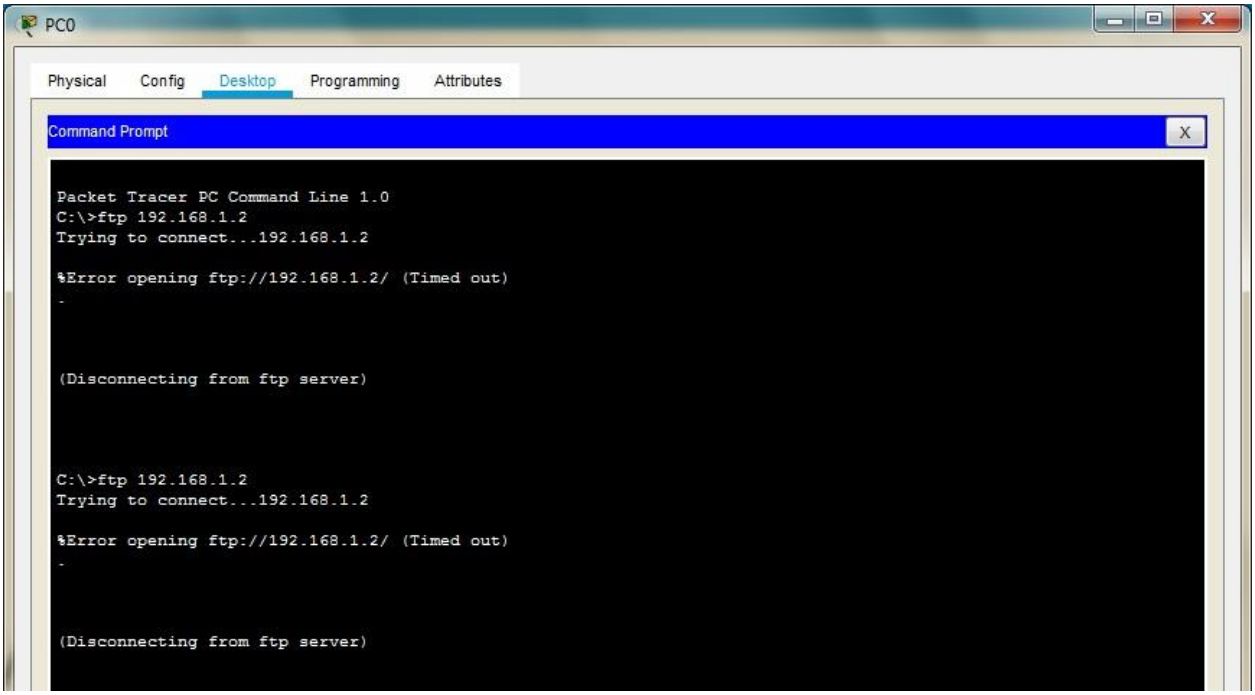
**Type the following commands in Router1**

```
Router#configure  terminal
Router(config)#
Router(config)#access-list 100 permit tcp host 192.168.3.2 host 192.168.1.2 eq ftp
Router(config)#interface GigabitEthernet0/1
Router(config-if)#ip access-group 100 out
Router(config-if)#exit
Router(config)#
```

**Now verify the ftp (ftp 192.168.1.2) command from both the PCs, one would be successful (PC1) and other (PC0) would fail**



SIC JOURNAL TYIT




## Part 2: Configure, Apply and Verify an Extended Named ACL

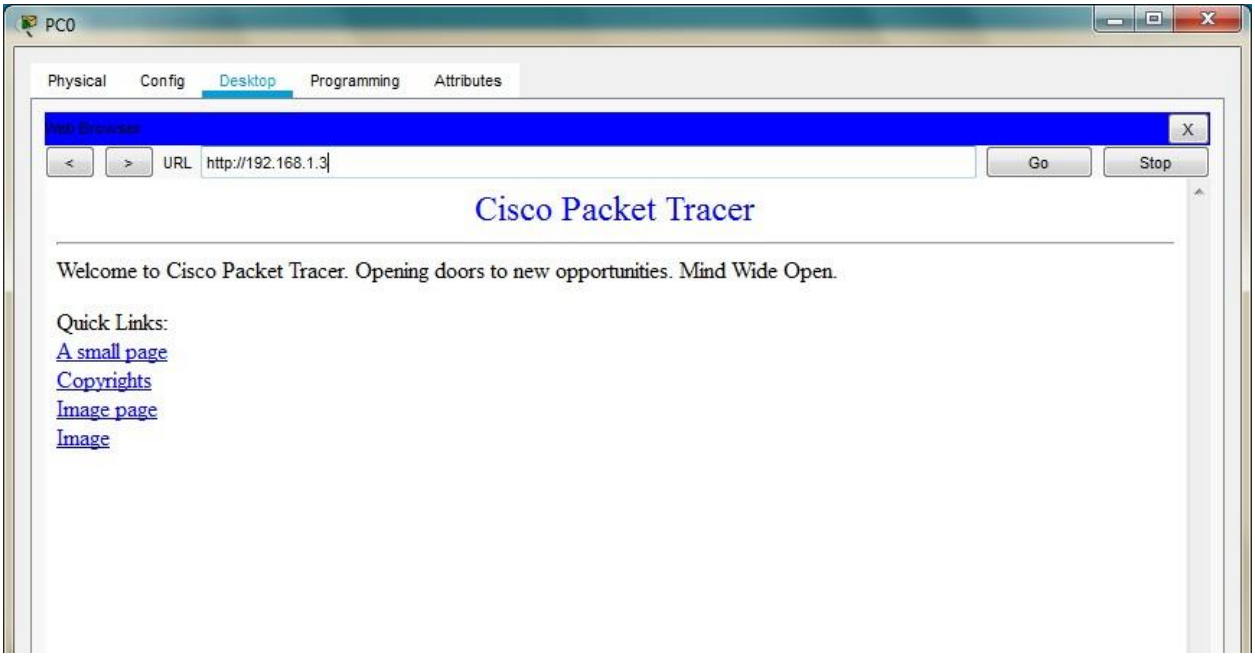
We use the same topology for this case

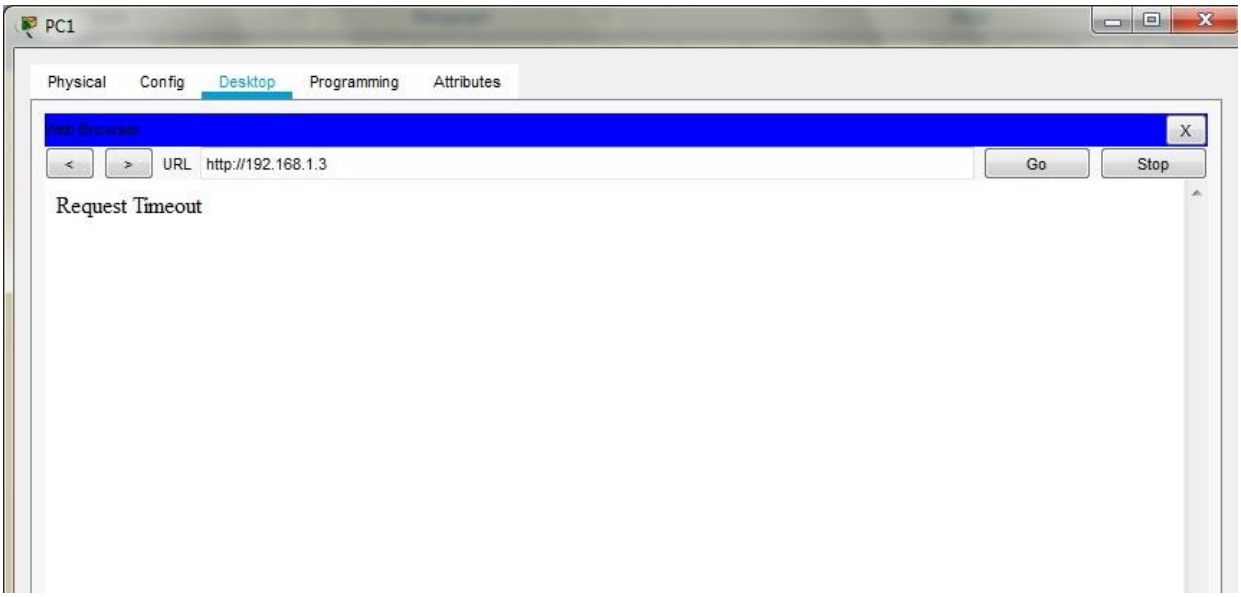
Type the following command in the CLI mode of Router1

Router> Router>en
Router#configure
terminal
Router(config)#ip access-list extended SMILE
Router(config-ext-nacl)#permit tcp host 192.168.3.3 host 192.168.1.3 eq www
Router(config-ext-nacl)#exit
Router(config)#
Router(config)#interface GigabitEthernet0/1
Router(config-if)#ip access-group SMILE out
Router(config-if)#exit
Router(config)#

**Now verify the www (192.168.1.3) command from both the PCs browser, one would be successful (PC0) and other (PC1) would fail**

SIC JOURNAL TYIT




**Hence Extended Numbered ACLs as well as Extended Named ACLs have been verified**

| | |
|---|---|
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |

# PRACTICALNO3:ConfigureAAA Authenticationon CiscoRouters

Toprovideacentralizedmanagementsystemfor theauthentication,authorizationandaccounting(AAA framework),AccessControlServer (ACS) isused.For thecommunicationbetweentheclientandthe ACSserver,twoprotocolsareusednamelyTACACS+and RADIUS.

**TACACS+**
Terminal AccessControllerAccessControlSystem(TACACS+) isCiscoproprietaryprotocolwhichis usedfor thecommunicationoftheCiscoclientandCiscoACSserver.ItusesTCPportnumber 49which makesitreliable.

**RADIUS–**
RemoteAccessDial InUser Service (RADIUS)isanopenstandardprotocolusedfor thecommunication betweenanyvendor AAAclientandACSserver.Ifoneoftheclientor serverisfromanyothervendor (otherthanCisco) thenwehavetouse RADIUS.Itusesportnumber 1812forauthenticationand authorizationand1813foraccounting.

| TACACS+ | RADIUS |
|---|---|
| Ciscoproprietaryprotocolopenstandardprotocol | |
| ItusesTCPastransmissionprotocol | ItusesUDPastransmissionprotocol |
| ItusesTCPportnumber49. | ItusesUDPportnumber1812for authenticationandauthorizationand1813 foraccounting. |
| Authentication,AuthorizationandAccountingis separatedinTACACS+.combinedinRADIUS. | AuthenticationandAuthorizationis |
| AlltheAAApacketsareencrypted.encrypted. | Onlythepasswordsareencryptedwhilethe otherinformationsuchasusername, accountinginformationetcarenot |
| PreferablyusedforACS. | usedwhenISEisused |
| Itprovidesmoregranularcontroli.ecanspecify theparticularcommandforauthorization. | Noexternalauthorizationofcommands supported. |
| TACACS+offersmultiprotocolsupport | No multiprotocolsupport. |

| | |
|---|---|
| | |

Usedfordeviceadministration. usedfornetworkaccess

**Similarities–**

TheprocessisstartbyNetworkAccessDevice (NAD–clientofTACACS+or RADIUS).NADcontactthe TACACS+or RADIUSserver andtransmittherequestforauthentication(usernameandpassword) tothe server.First,NAD obtainusernamepromptandtransmittheusernametotheserver andthenagainthe server iscontactbyNAD toobtainpasswordpromptandthenthepasswordissendtotheserver.
Theserver replieswithaccess-acceptmessage ifthecredentialsarevalidotherwisesendanaccess-rejectmessagetotheclient.Furtherauthorisationandaccountingisdifferentinbothprotocolsas authenticationandauthorisationiscombined inRADIUS

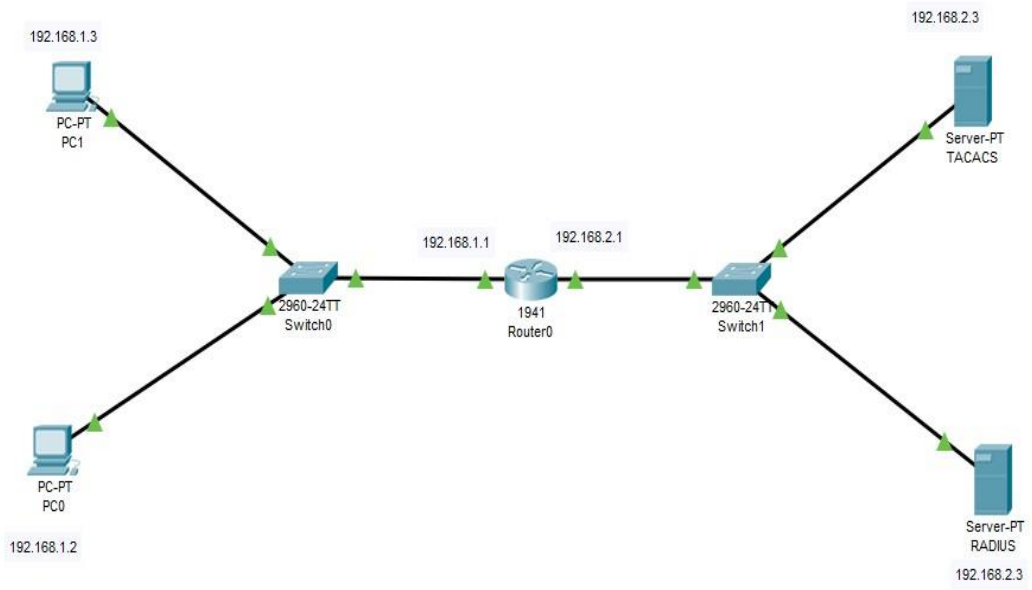
**Advantages(TACACS+overRADIUS)–**

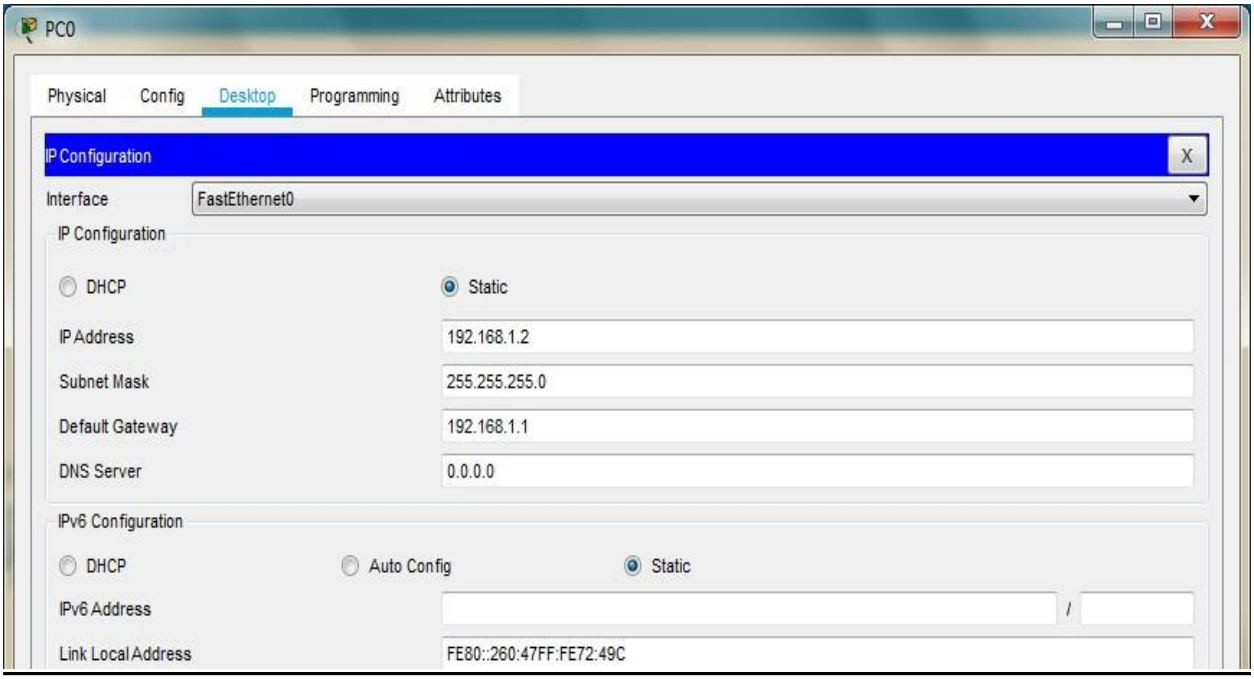
1. AsTACACS+usesTCPthereforemorereliablethanRADIUS.
2. TACACS+providesmorecontroloverheauthorizationofcommandswhileinRADIUS, noexternalauthorizationofcommandsissupported.
3. AlltheAAApacketsareencryptedinTACACS+whileonlythepasswordsareencrypted inRADIUSi.emoresecure.

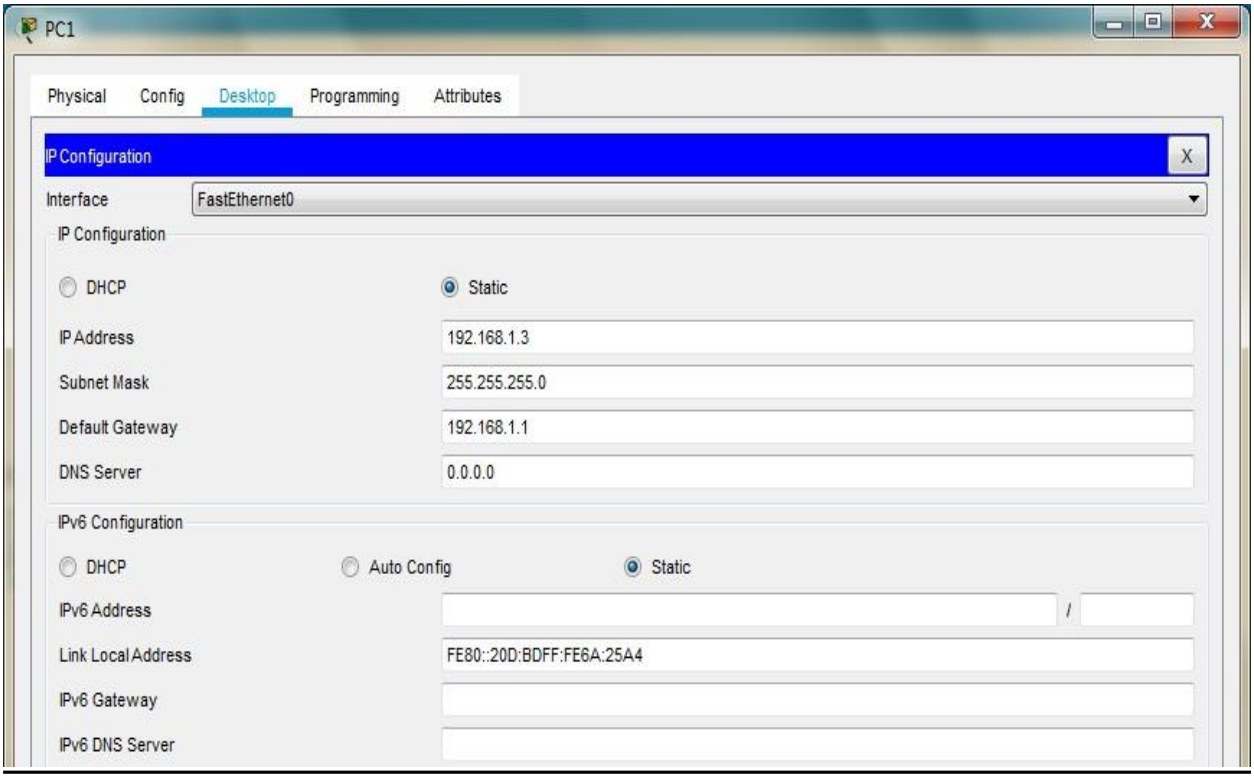
**Advantage(RADIUSoverTACACS+)–**

1. AsitisopenstandardthereforeRADIUScanbeusedwithothervendorsdevicewhile becauseTACACS+is Ciscoproprietary,itcanbeusedwithCiscodevicesonly.
2. IthasmoreextensiveaccountingsupportthanTACACS+.

WeusethefollowingTopologyfor thepresentcase

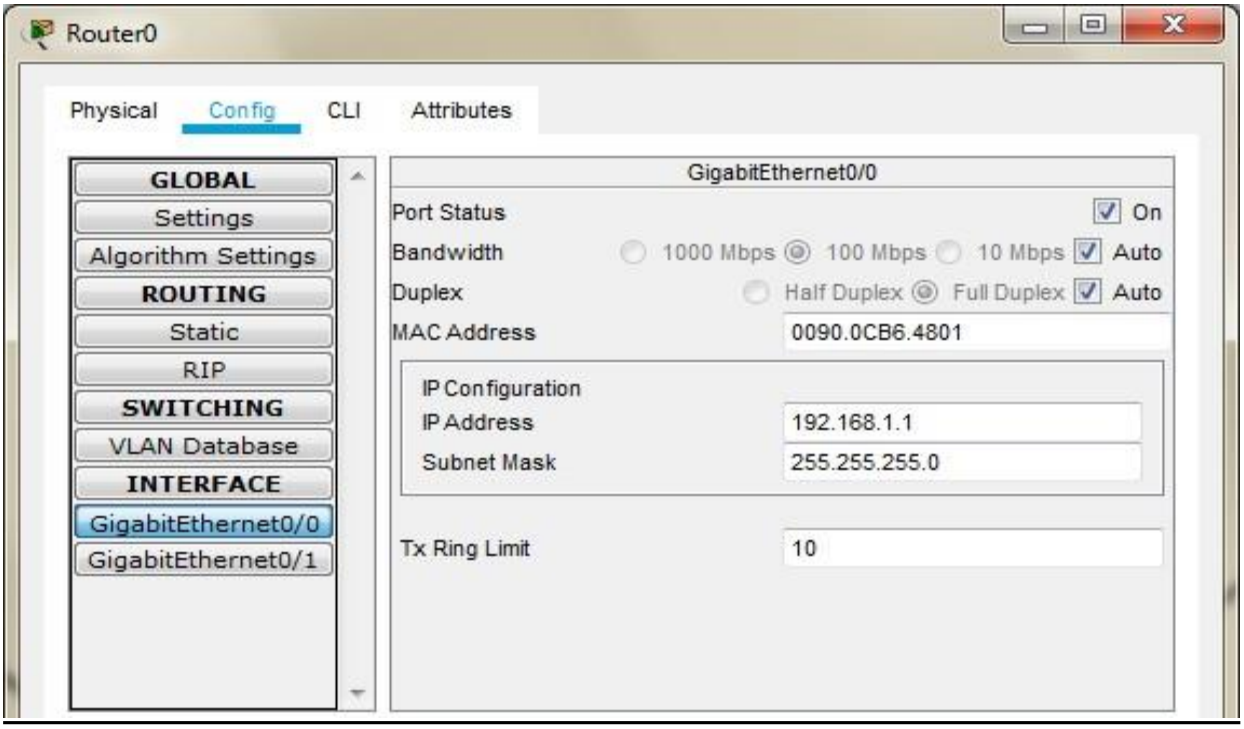


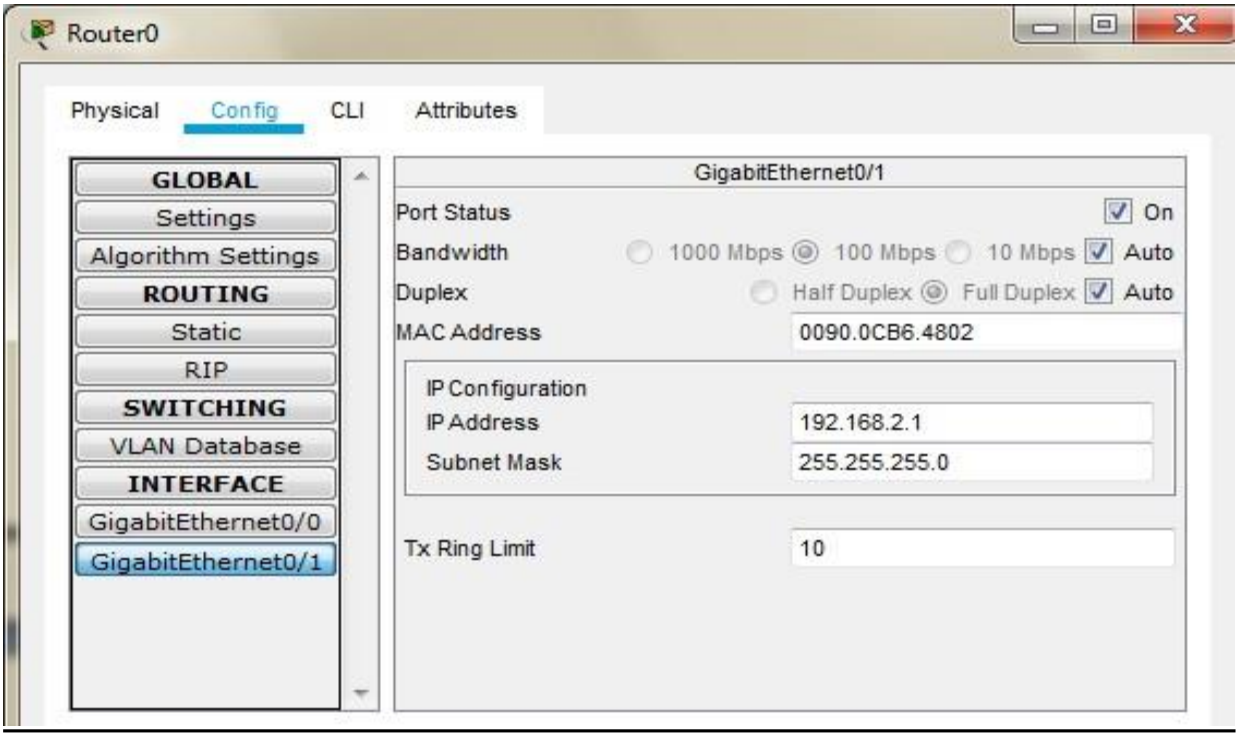

PC0
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IP Address
192.168.1.2
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.1
DNS Server
0.0.0.0
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address
FE80::260:47FF:FE72:49C


PC1
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IP Address
192.168.1.3
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.1
DNS Server
0.0.0.0
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address
FE80::20D:BDFF:FE6A:25A4
IPv6 Gateway
IPv6 DNS Server

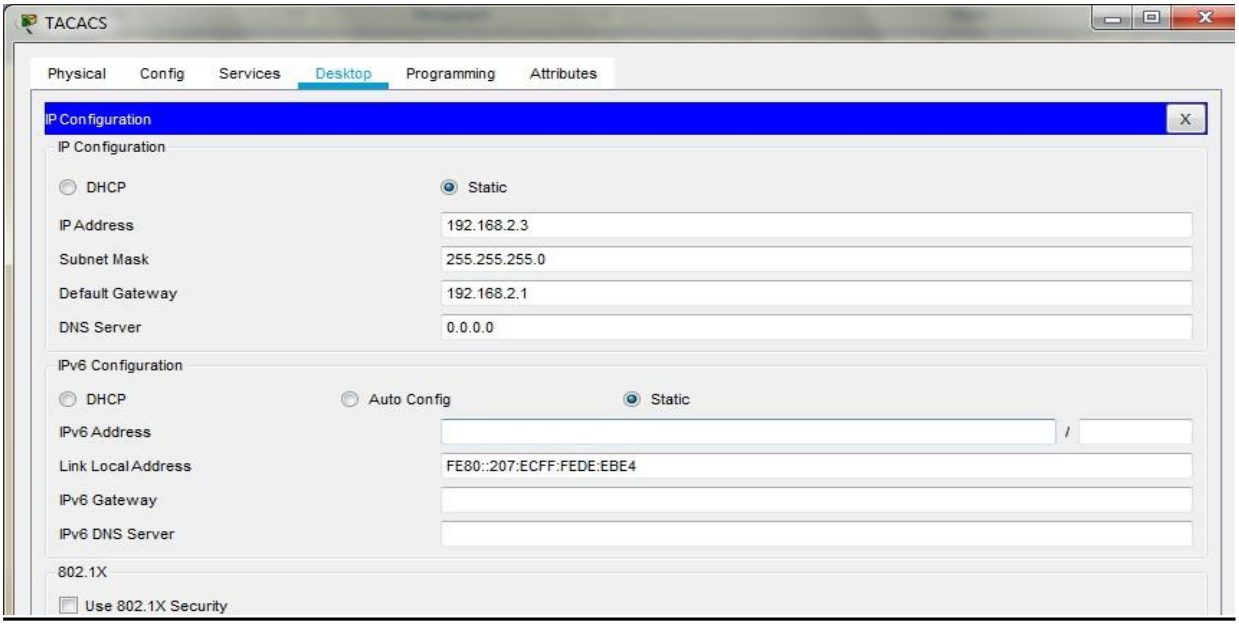
**ConfiguringPC0**

**ConfiguringPC1**


Router0
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0
GigabitEthernet0/1
GigabitEthernet0/0
Port Status
On
Bandwidth
1000 Mbps
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
0090.0CB6.4801
IP Configuration
IP Address
192.168.1.1
Subnet Mask
255.255.255.0
Tx Ring Limit
10

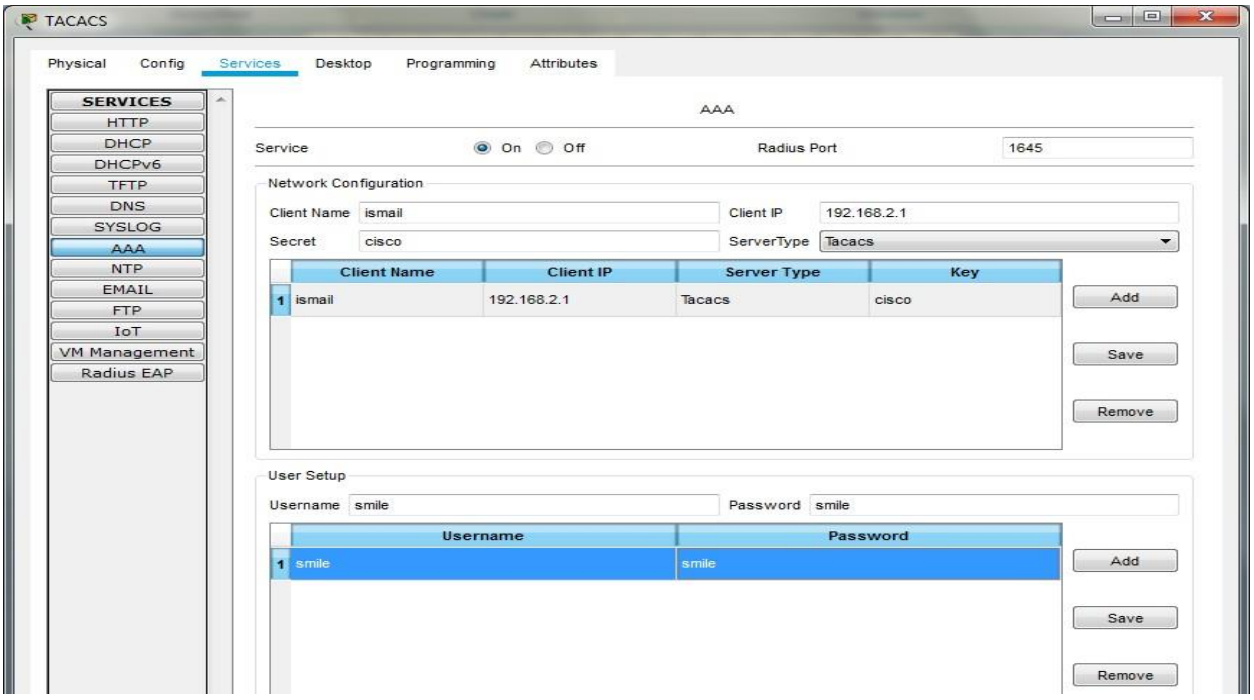

Router0
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0
GigabitEthernet0/1
GigabitEthernet0/1
Port Status
On
Bandwidth
1000 Mbps
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
0090.0CB6.4802
IP Configuration
IP Address
192.168.2.1
Subnet Mask
255.255.255.0
Tx Ring Limit
10

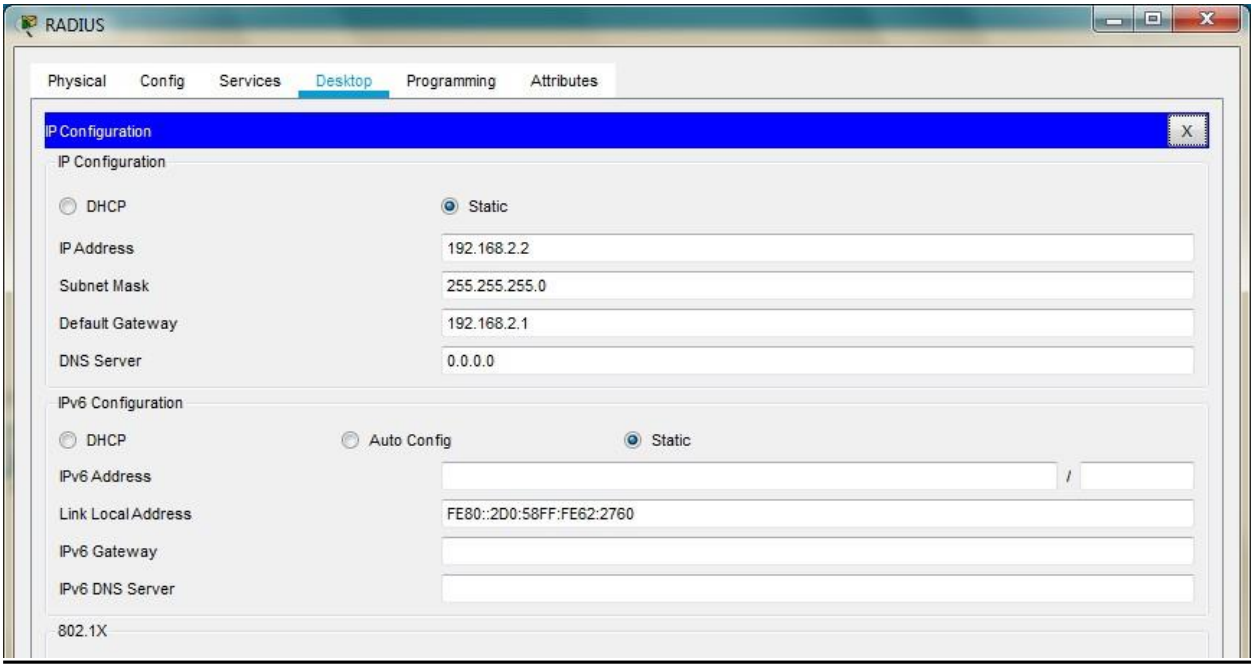
**ConfiguringRouter0**


TACACS
Physical
Config
Services
Desktop
Programming
Attributes
IP Configuration
X
IP Configuration
DHCP
Static
IP Address
192.168.2.3
Subnet Mask
255.255.255.0
Default Gateway
192.168.2.1
DNS Server
0.0.0.0
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
/
Link Local Address
FE80::207:ECFF:FEDE:EBE4
IPv6 Gateway
IPv6 DNS Server
802.1X
Use 802.1X Security

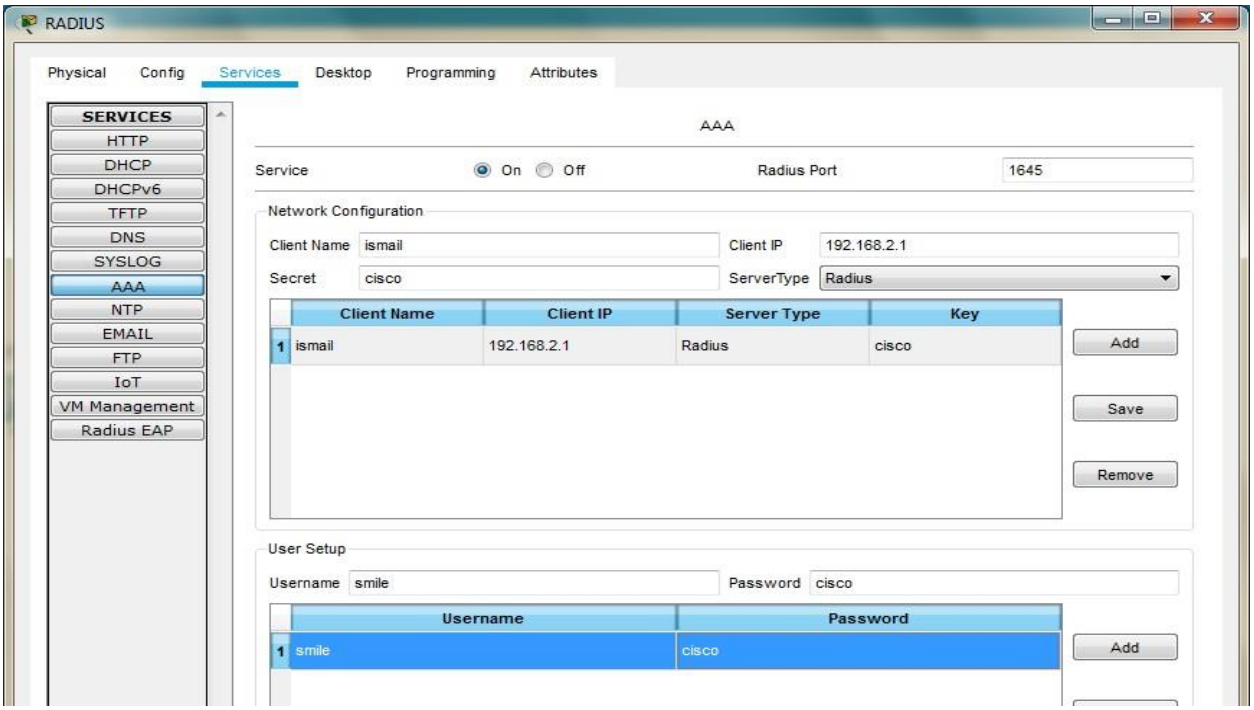
**ConfiguringServer0(AsTACACS)**

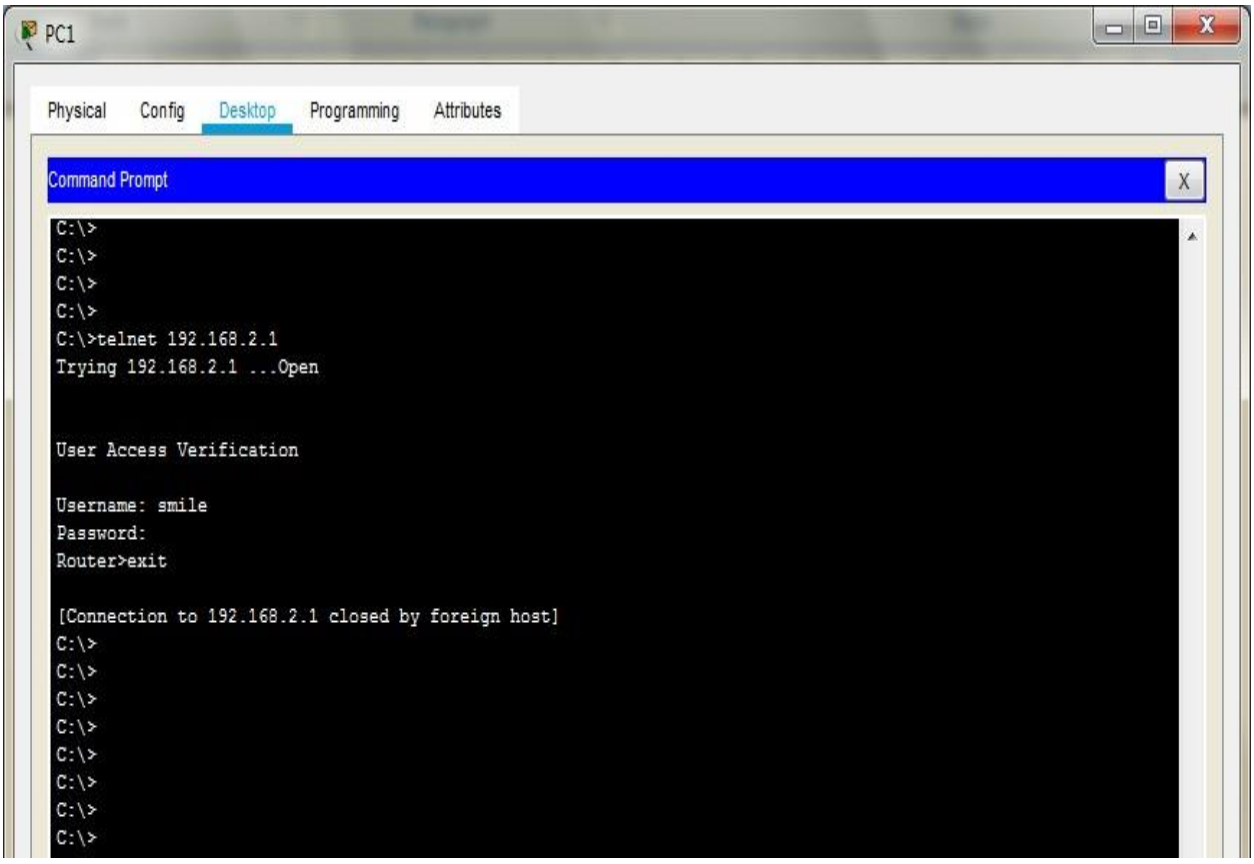
WhileconfiguringtheTACACS/RADIUSservertheClientIPaddress mustbe the RouterIP




RADIUS
Physical
Config
Services
Desktop
Programming
Attributes
IP Configuration
X
IP Configuration
DHCP
Static
IP Address
192.168.2.2
Subnet Mask
255.255.255.0
Default Gateway
192.168.2.1
DNS Server
0.0.0.0
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
/
Link Local Address
FE80::2D0:58FF:FE62:2760
IPv6 Gateway
IPv6 DNS Server
802.1X

**ConfiguringServer1(As RADIUS)**



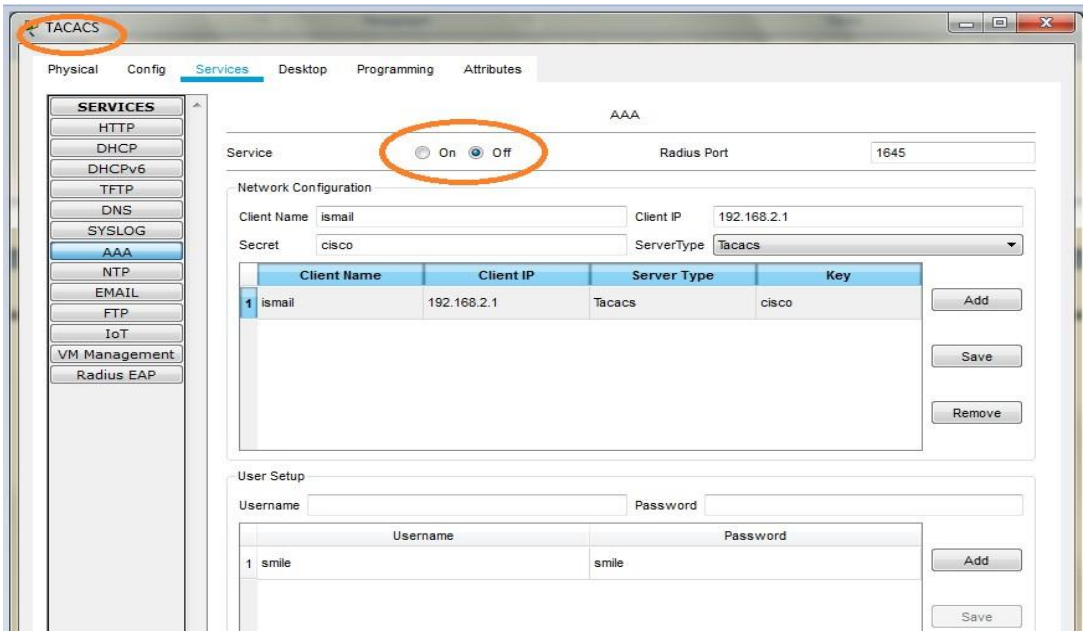

PC1
Physical
Config
Desktop
Programming
Attributes
Command Prompt
C:\>
C:\>
C:\>
C:\>
C:\>telnet 192.168.2.1
Trying 192.168.2.1 ...Open
User Access Verification
Username: smile
Password:
Router>exit
[Connection to 192.168.2.1 closed by foreign host]
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>

**Typethefollowingcommandsinthe CLImodeof theRouter0**

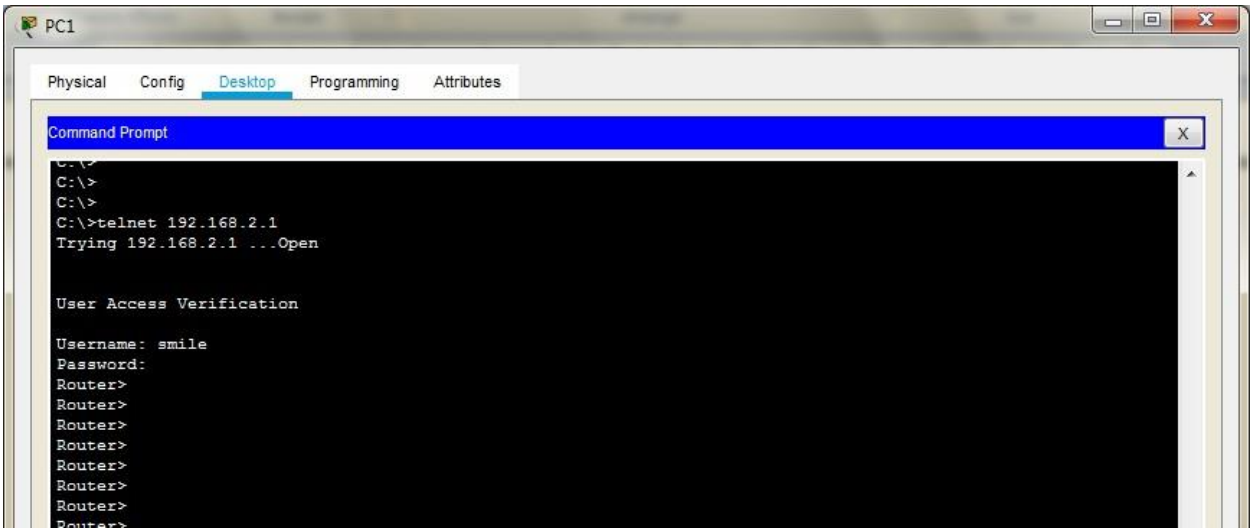
```
Router>enable
Router#configureterminal
Router(config)#aaa new-
model
Router(config)#tacacs-server host 192.168.2.3  key cisco
Router(config)#radius-server host 192.168.2.2   key cisco
Router(config)#aaa authentication login ismail  group tacacs+ group radius local
Router(config)#line vty 0 4
Router(config-line)#login authentication ismail
Router(config-line)#exit
Router(config)#
```

TheAuthenticationcanbe donebytypingthecommand**telnet 192.168.2.1(**theRouterIP**)**in anyofthe PCs
Wegetapromptto typetheusernameandpassword,theusername andpasswordsetinTACACSare entered
Username:smile
Password:smile
Wegetthefollowing

Inorderto authenticatethe RADIUSserverweneedto turnOFFtheTACACSservice




Weagainenterthecommand**telnet 192.168.2.1(**theRouter IP**)**andentertheusernameandpassword ofthe RADIUSserver(Username:smile,Password:cisco)
Wegetthefollowing




Thelocallogincanalsobe verifiedbyturning OFFbothTACACSandRADIUSservice.Theusernameand Passwordarebothcisco(bydefault)
Hencethe authenticationthroughbothTACACSandRADIUS

SIC JOURNAL TYIT

# PRACTICAL NO 4: Configure IP ACLs to Mitigate Attacks.

**Access Control Lists (ACLs)**

Network administrators must figure out how to deny unwanted access to the network while allowing internal users appropriate access to necessary services. Although security tools, such as passwords, callback equipment, and physical security devices are helpful, they often lack the flexibility of basic traffic filtering and the specific controls most administrators prefer.

For example, a network administrator may want to allow users access to the Internet, but not permit external users telnet access into the LAN.

Routers provide basic traffic filtering capabilities, such as blocking Internet traffic, with access control lists (ACLs).

An ACL is a sequential list of permit or deny statements that apply to addresses or upper-layer protocols.

The router examines each packet to determine whether to forward or drop it, based on the conditions specified in the ACL.

Some ACL decision points are:

1) IP source address
2) IP destination addresses
3) UDP or TCP protocols
4) Upper-layer (TCP/UDP) port numbers

ACLs must be defined on a:

1) Per-protocol (IP, IPX, AppleTalk)
2) Per direction (in or out)
3) Per port (interface) basis.
4) ACLs control traffic in one direction at a time on an interface.
5) A separate ACL would need to be created for each direction, one for inbound and one for outbound traffic.
6) Finally every interface can have multiple protocols and directions defined.

An ACL is a group of statements that define whether packets are accepted or rejected coming into an interface or leaving an interface.

1) ACL statements operate in sequential, logical order (top down).
2) If a condition match is true, the packet is permitted or denied and the rest of the ACL statements are not checked.
3) If all the ACL statements are unmatched, an implicit "deny any"

□

SIC JOURNAL TYIT

statement is placed at the end of the list by default. (not visible)

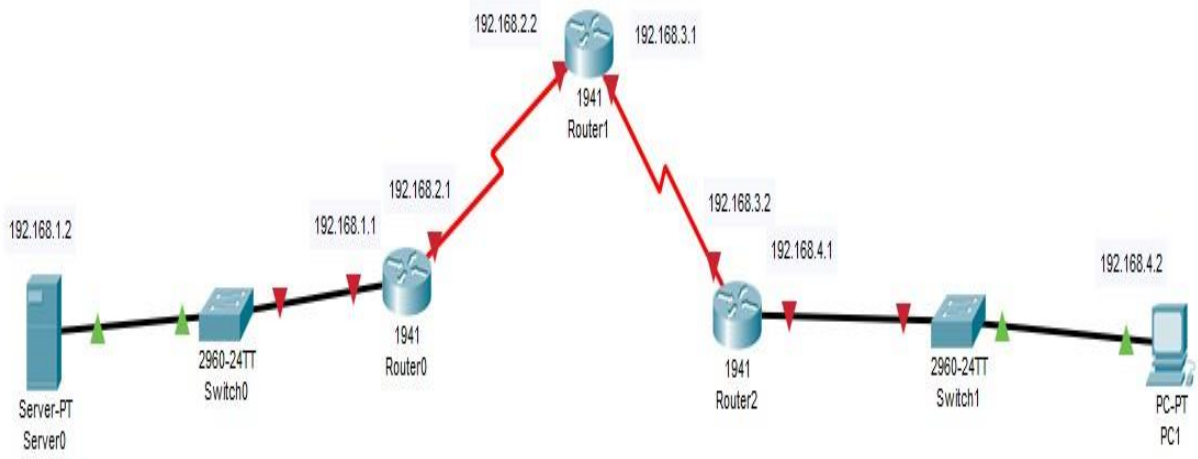
When first learning how to create ACLs, it is a good idea to add the implicit deny at the end of ACLs to reinforce the dynamic presence of the command line.

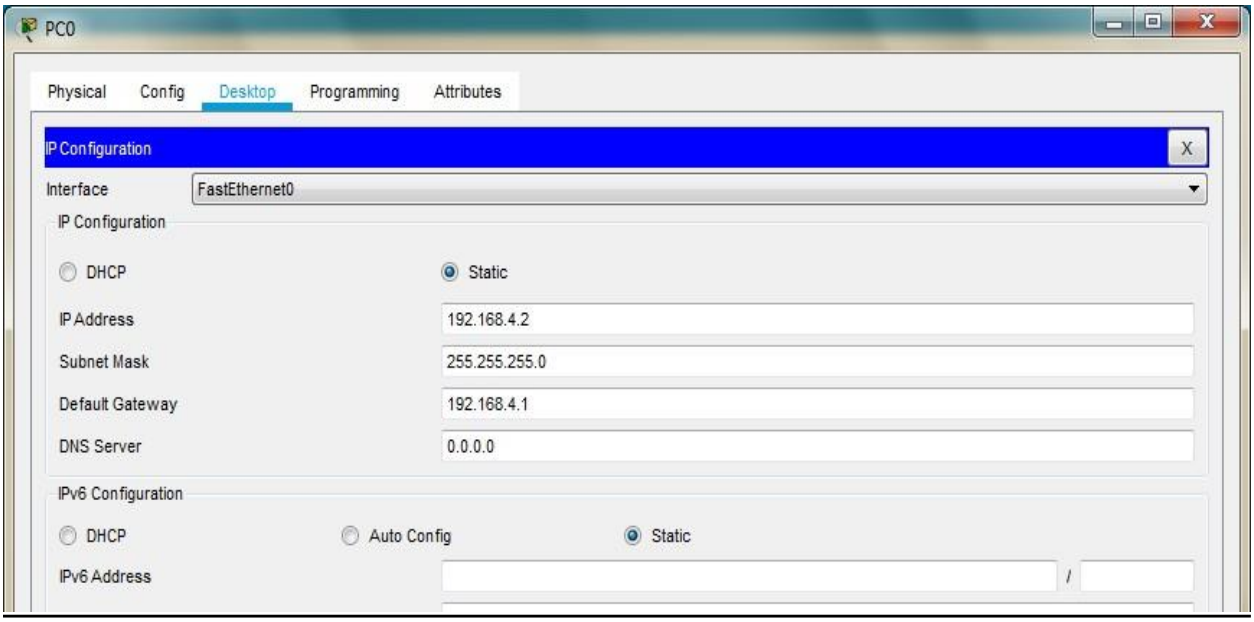
Standard IP ACLs
Can only filter on source IP addresses

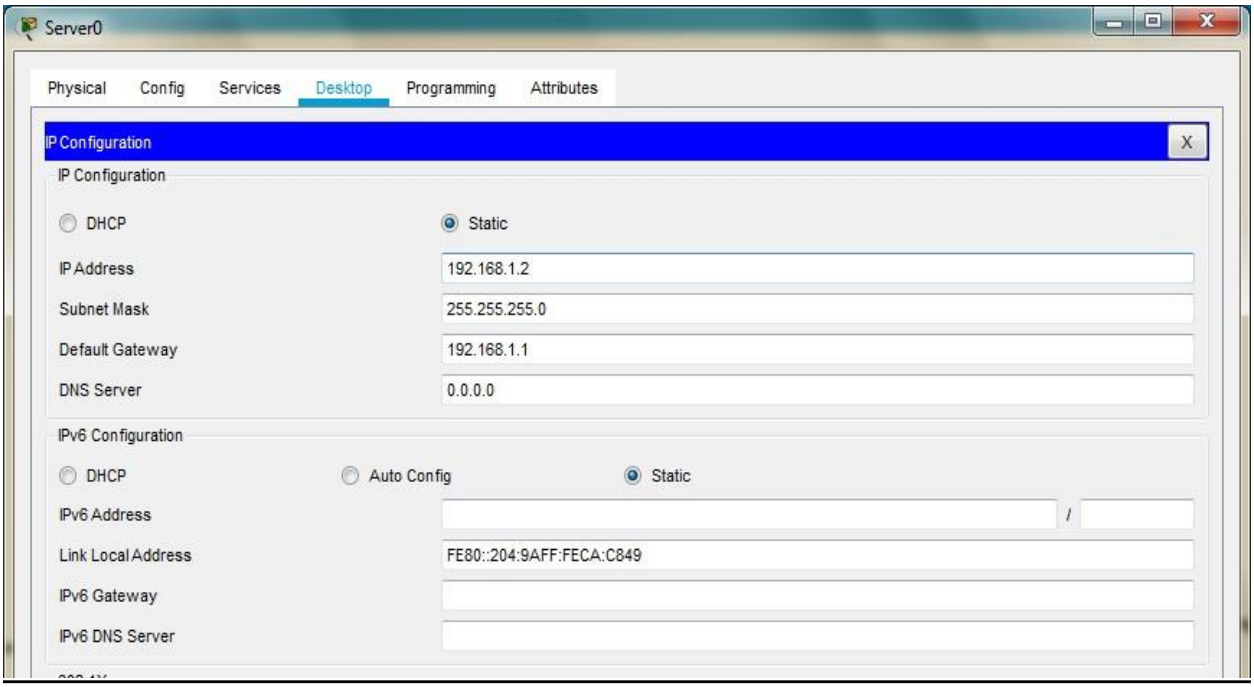
Extended IP ACLs Can filter on:
1) Source IP address
2) Destination IP address
3) Protocol (TCP, UDP)
4) Port Numbers (Telnet – 23, http – 80, etc.) and other parameters

An access list is a sequential series of commands or filters. These lists tell the router what types of packets to: accept or deny Acceptance and denial can be based on specified conditions. ACLs applied on the router's interfaces

**We use the following topology to study the present case**



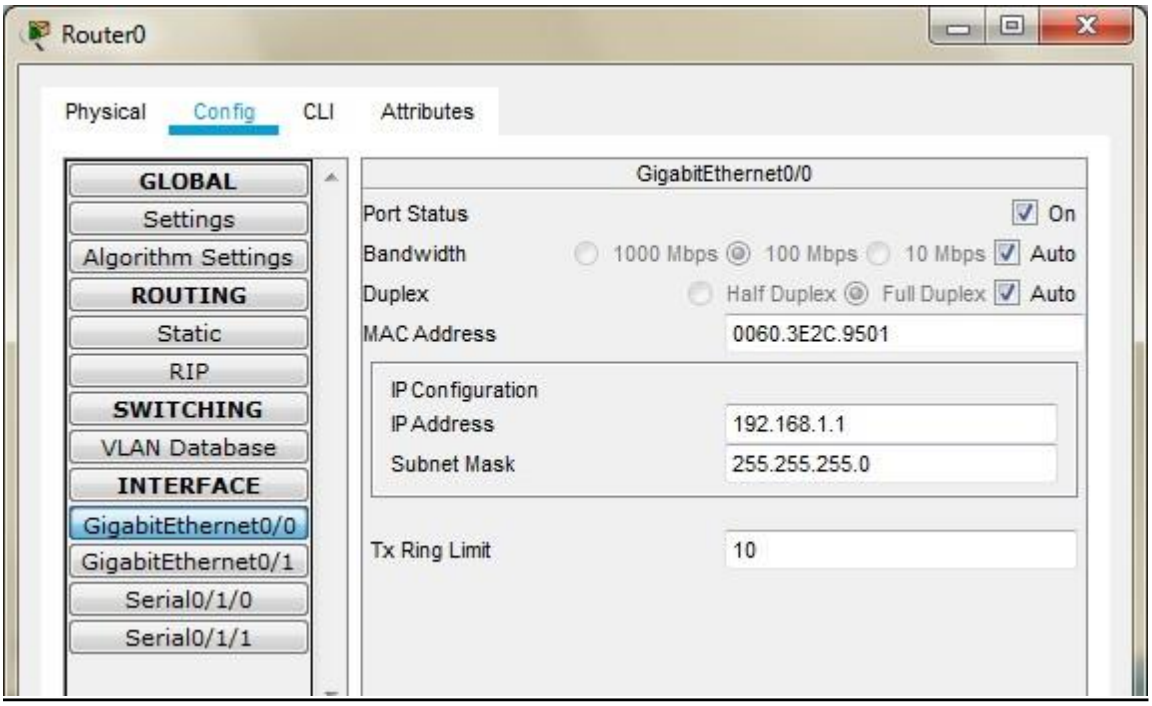

PC0
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IP Address
192.168.4.2
Subnet Mask
255.255.255.0
Default Gateway
192.168.4.1
DNS Server
0.0.0.0
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address

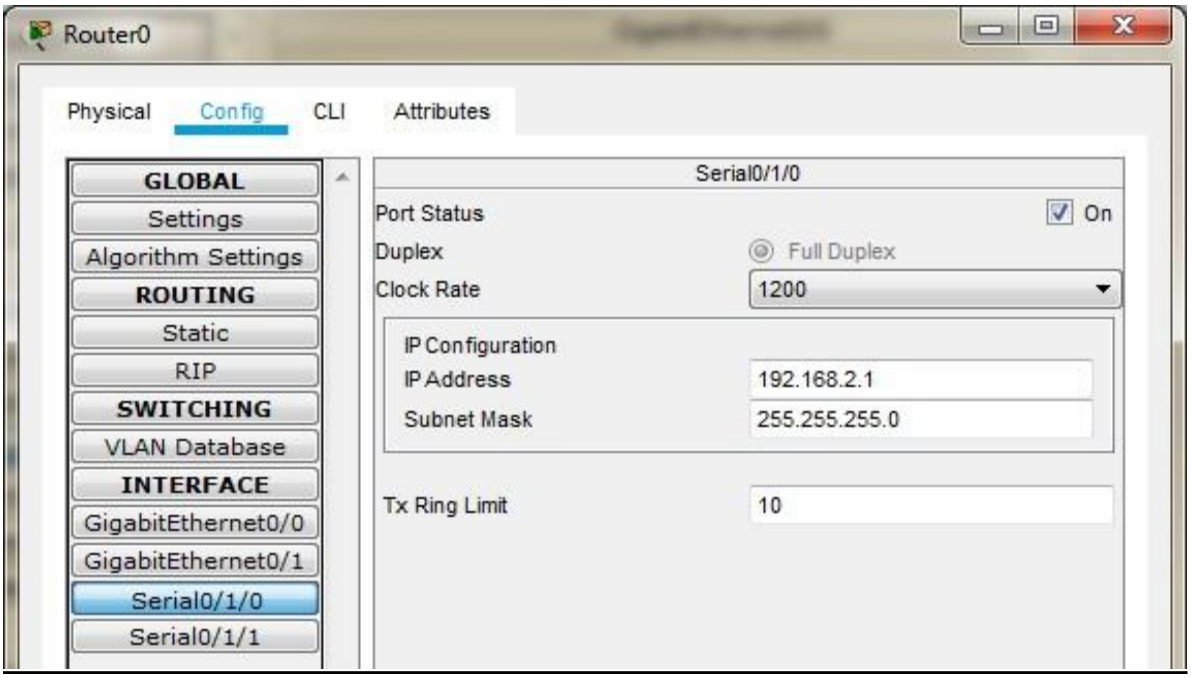

Server0
Physical
Config
Services
Desktop
Programming
Attributes
IP Configuration
X
IP Configuration
DHCP
Static
IP Address
192.168.1.2
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.1
DNS Server
0.0.0.0
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
Link Local Address
FE80::204:9AFF:FECA:C849
IPv6 Gateway
IPv6 DNS Server

SIC JOURNAL TYIT

**Configuring PC1**

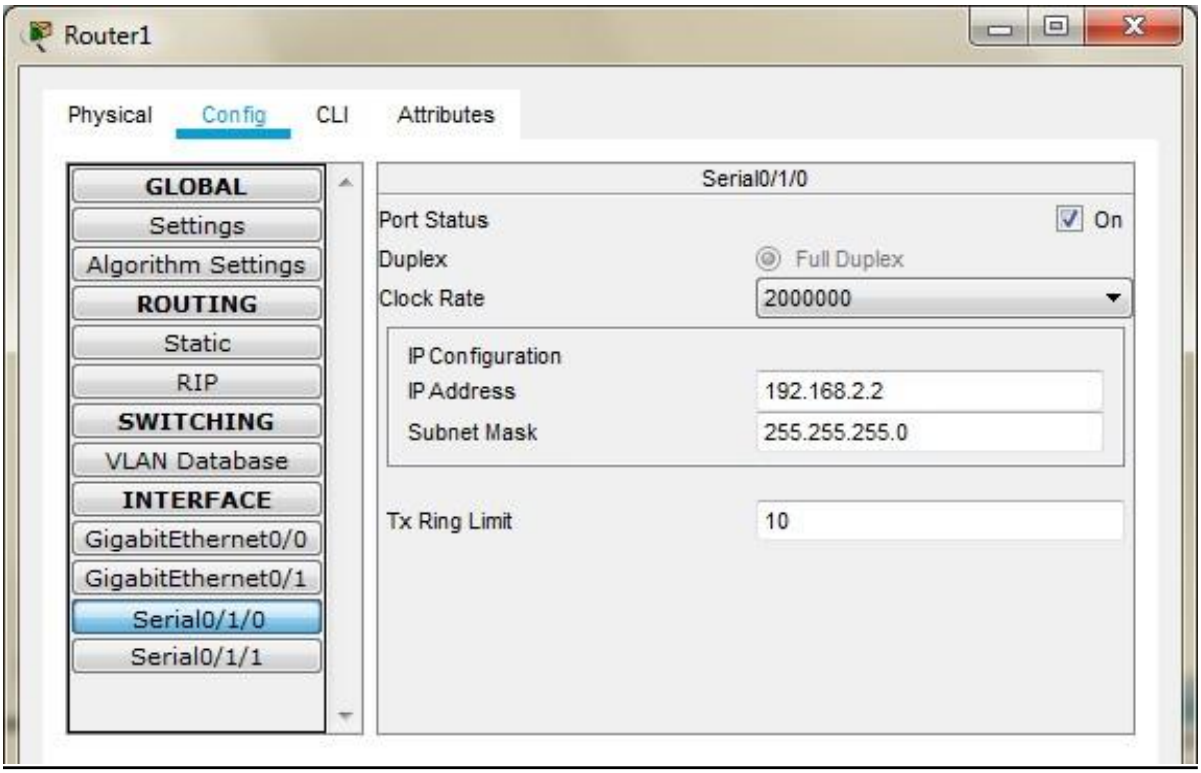
**Configuring Server0**

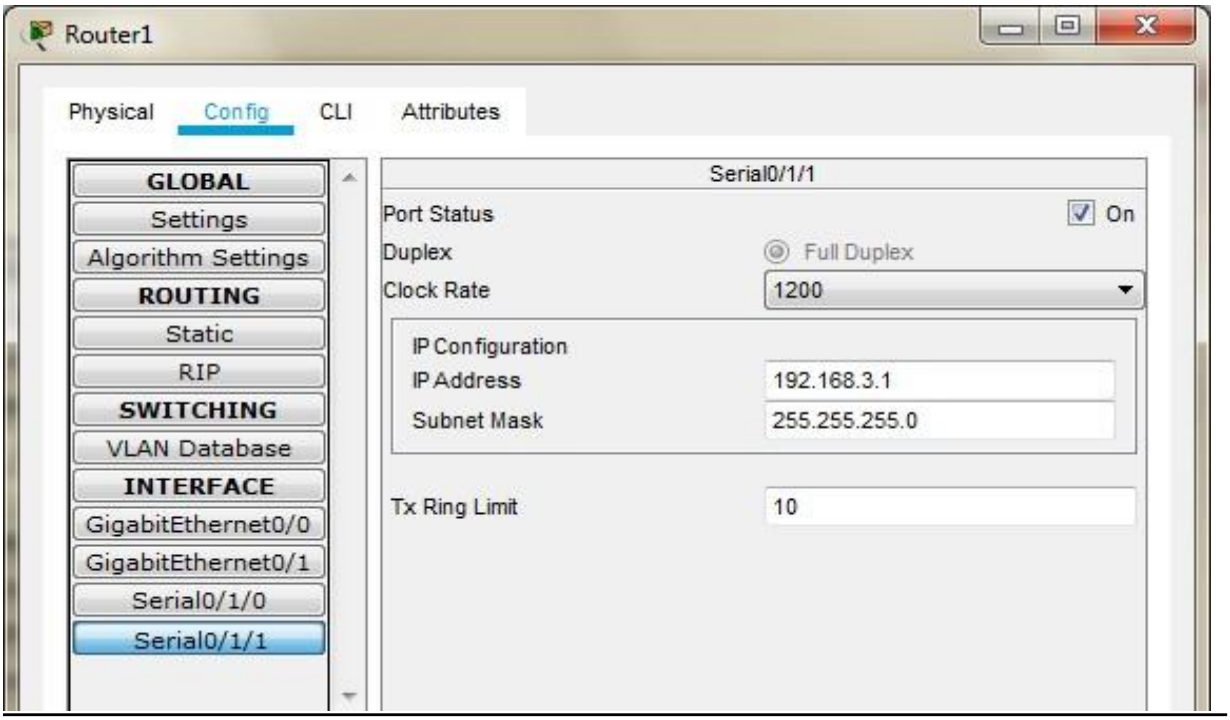

Router0
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0
GigabitEthernet0/1
Serial0/1/0
Serial0/1/1
GigabitEthernet0/0
Port Status
On
Bandwidth
1000 Mbps
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
0060.3E2C.9501
IP Configuration
IP Address
192.168.1.1
Subnet Mask
255.255.255.0
Tx Ring Limit
10


Router0
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0
GigabitEthernet0/1
Serial0/1/0
Serial0/1/1
Serial0/1/0
Port Status
On
Duplex
Full Duplex
Clock Rate
1200
IP Configuration
IP Address
192.168.2.1
Subnet Mask
255.255.255.0
Tx Ring Limit
10

SIC JOURNAL TYIT

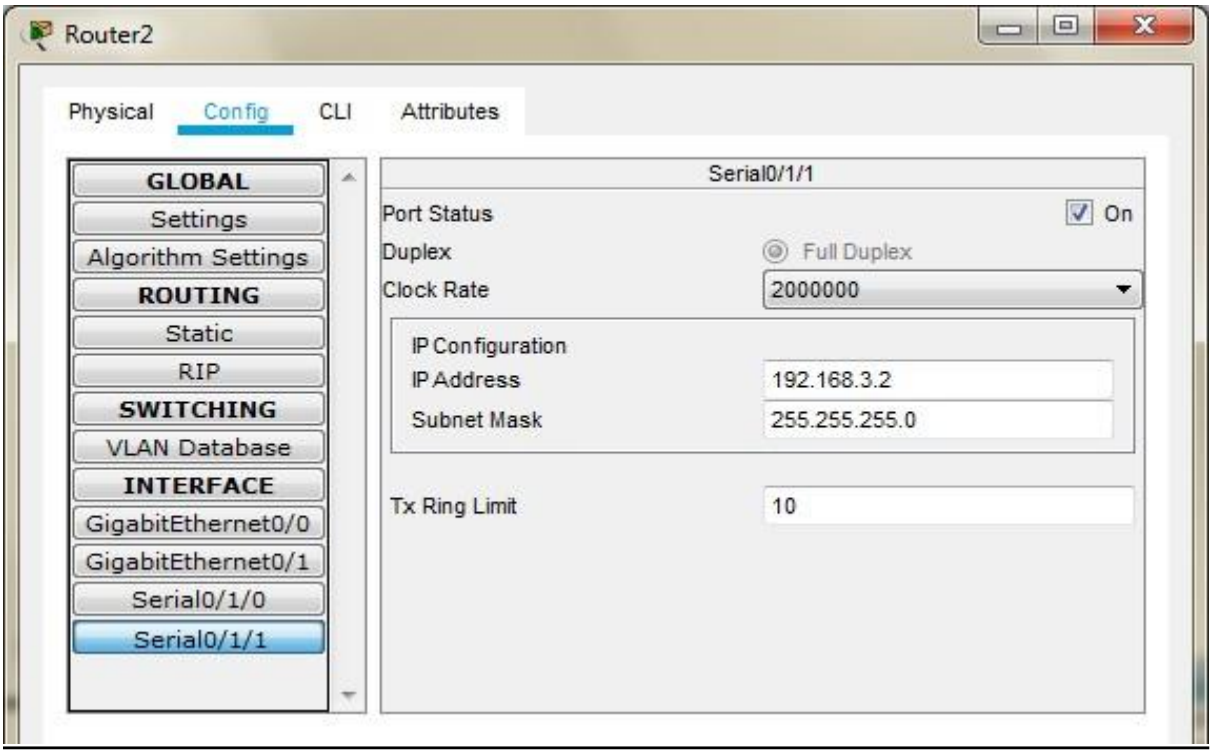
**Configuring Router0**

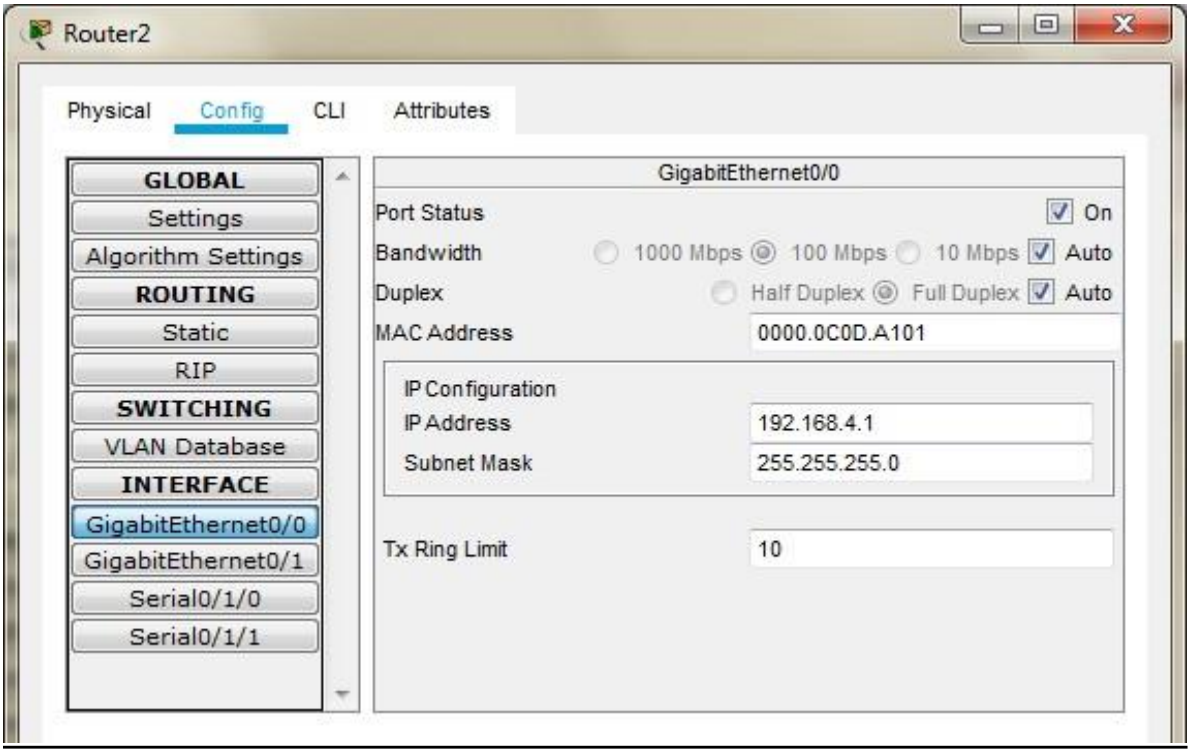

Router1
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0
GigabitEthernet0/1
Serial0/1/0
Serial0/1/1
Serial0/1/0
Port Status
On
Duplex
Full Duplex
Clock Rate
2000000
IP Configuration
IP Address
192.168.2.2
Subnet Mask
255.255.255.0
Tx Ring Limit
10


Router1
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0
GigabitEthernet0/1
Serial0/1/0
Serial0/1/1
Serial0/1/1
Port Status
On
Duplex
Full Duplex
Clock Rate
1200
IP Configuration
IP Address
192.168.3.1
Subnet Mask
255.255.255.0
Tx Ring Limit
10

SIC JOURNAL TYIT

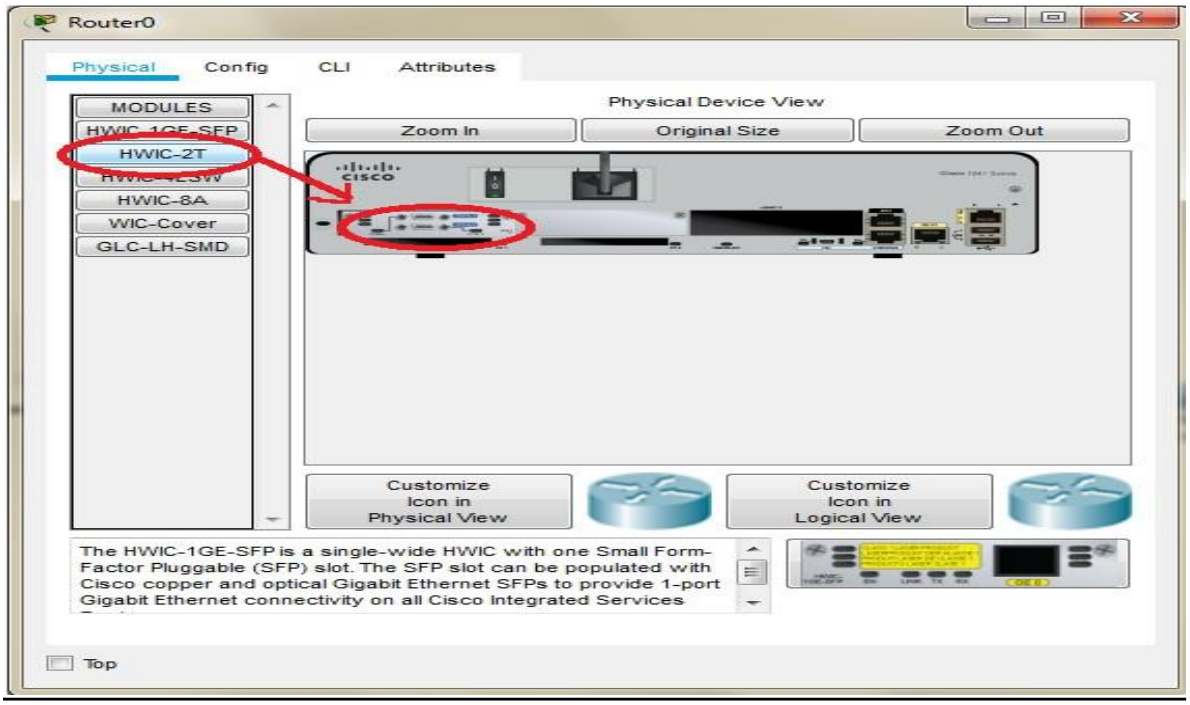
**Configuring Router1**

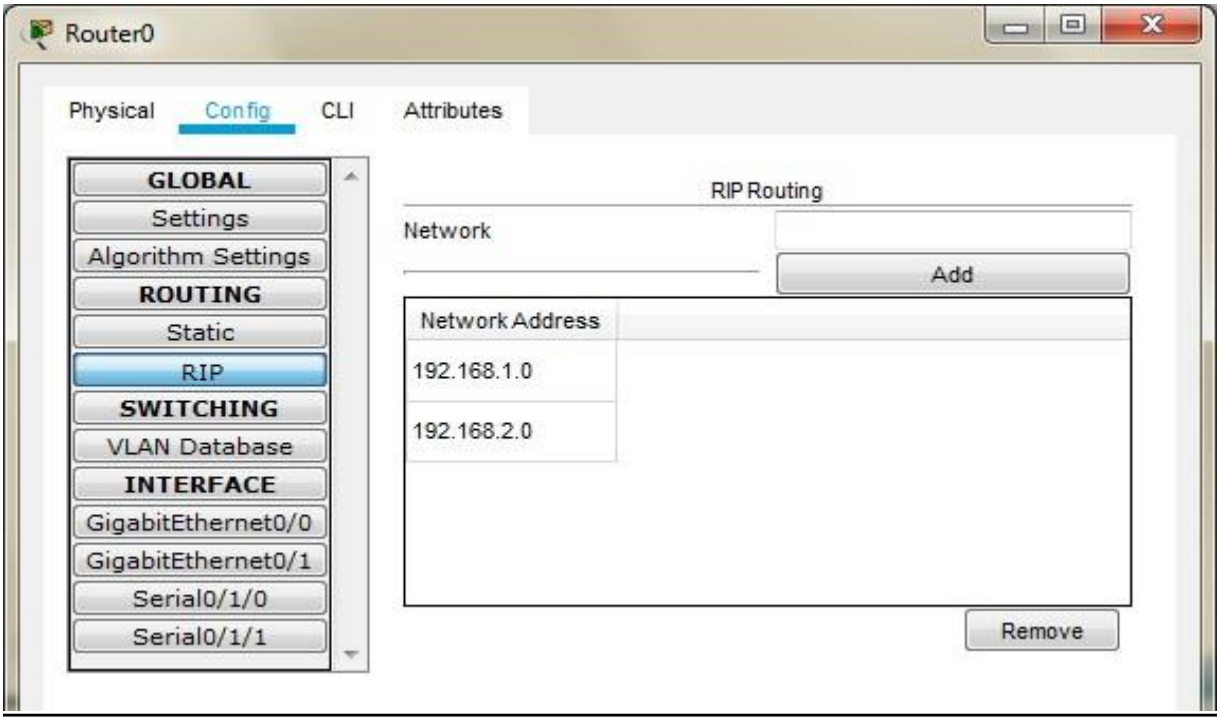

Router2
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0
GigabitEthernet0/1
Serial0/1/0
Serial0/1/1
Serial0/1/1
Port Status
On
Duplex
Full Duplex
Clock Rate
2000000
IP Configuration
IP Address
192.168.3.2
Subnet Mask
255.255.255.0
Tx Ring Limit
10


Router2
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0
GigabitEthernet0/1
Serial0/1/0
Serial0/1/1
GigabitEthernet0/0
Port Status
On
Bandwidth
1000 Mbps
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
0000.0C0D.A101
IP Configuration
IP Address
192.168.4.1
Subnet Mask
255.255.255.0
Tx Ring Limit
10

SIC JOURNAL TYIT

**Configuring Router2**


Router0
Physical
Config
CLI
Attributes
MODULES
HWIC-2T
HWIC-8A
WIC-Cover
GLC-LH-SMD
Physical Device View
Zoom In
Original Size
Zoom Out
Customize Icon in Physical View
Customize Icon in Logical View
The HWIC-1GE-SFP is a single-wide HWIC with one Small Form-Factor Pluggable (SFP) slot. The SFP slot can be populated with Cisco copper and optical Gigabit Ethernet SFPs to provide 1-port Gigabit Ethernet connectivity on all Cisco Integrated Services
Top

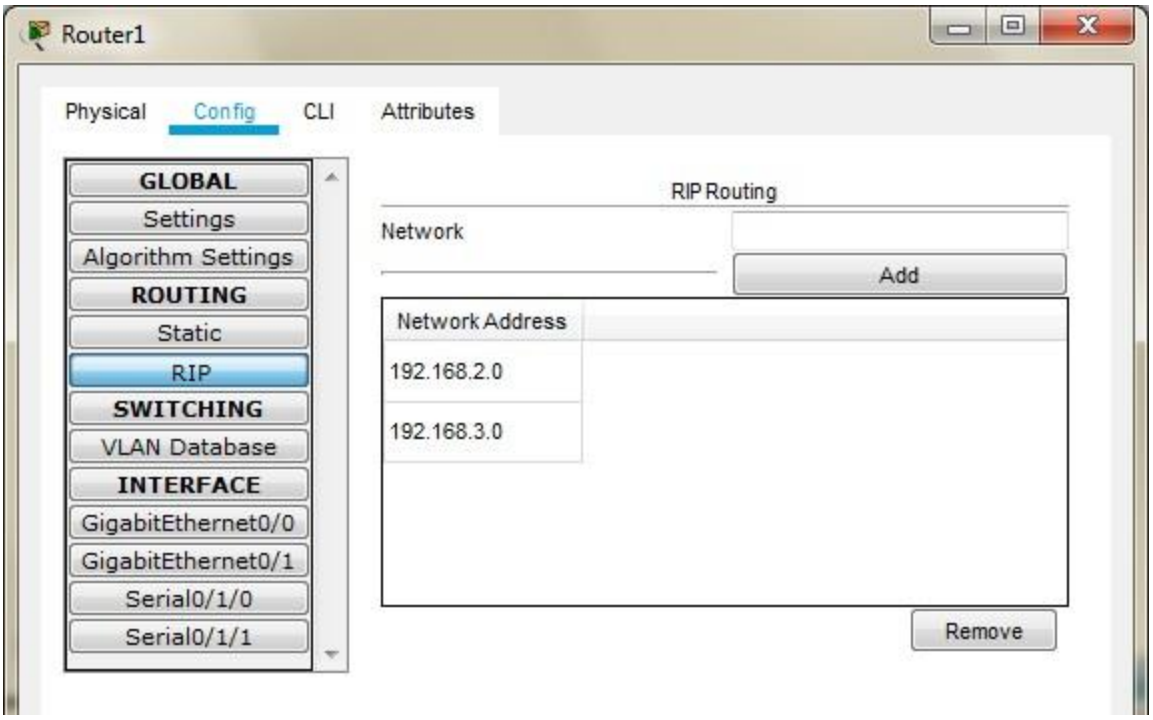

Router0
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0
GigabitEthernet0/1
Serial0/1/0
Serial0/1/1
RIP Routing
Network
Add
Network Address
192.168.1.0
192.168.2.0
Remove

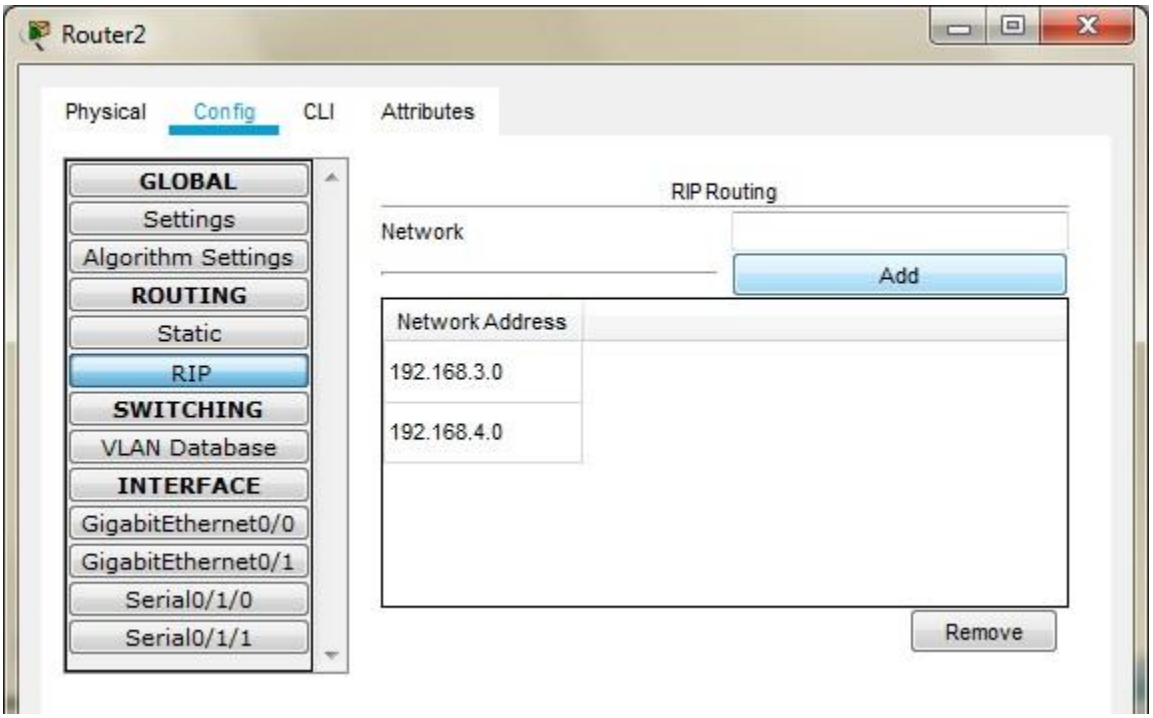
SIC JOURNAL TYIT

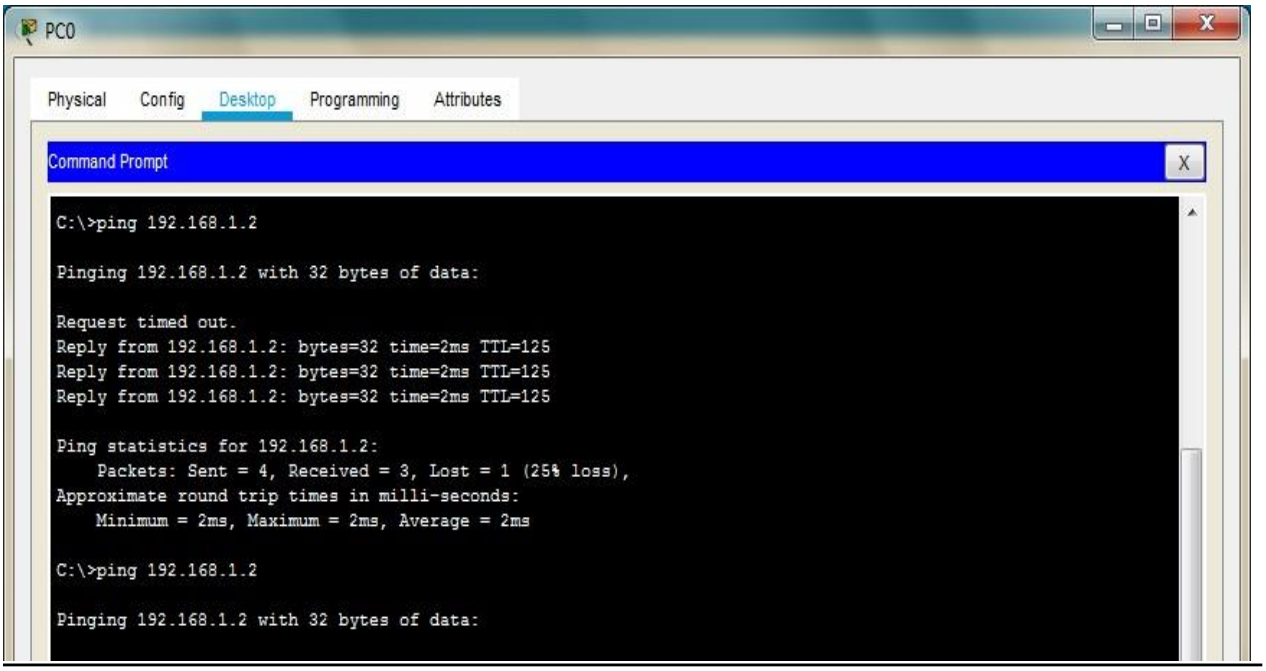
**The serial interface in each Router are added as follows**

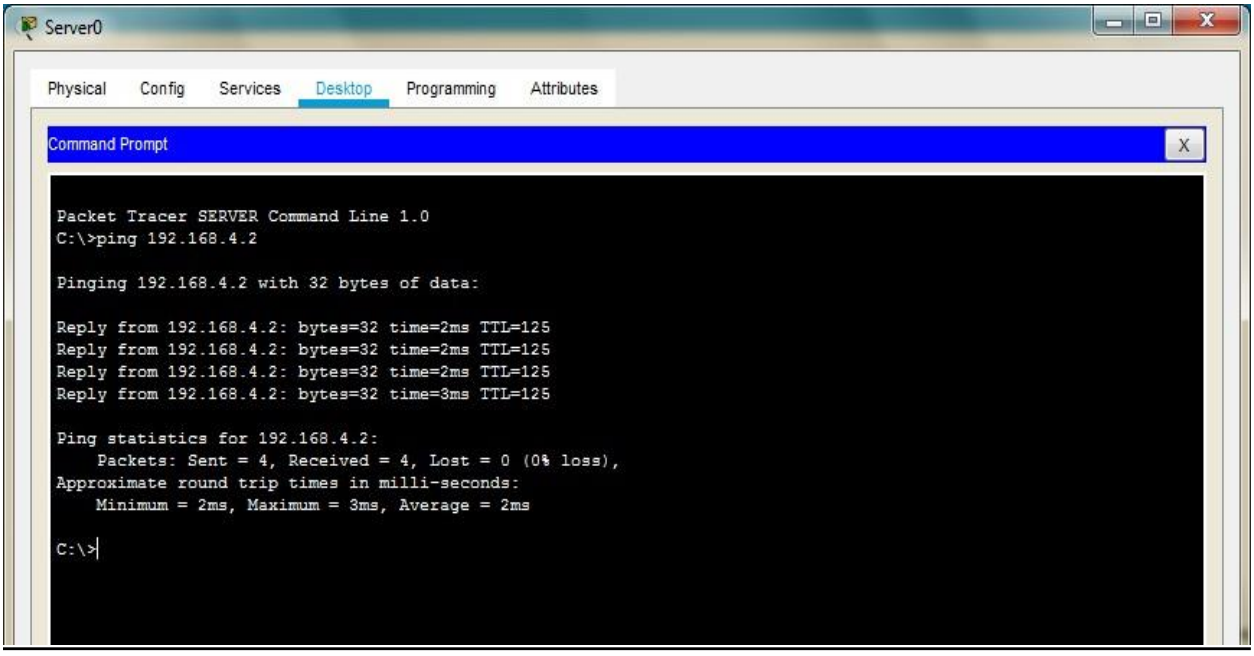
**Set the RIP on each Router**

SIC JOURNAL TYIT




PC0
Physical
Config
Desktop
Programming
Attributes
Command Prompt
C:\>ping 192.168.1.2
Pinging 192.168.1.2 with 32 bytes of data:
Request timed out.
Reply from 192.168.1.2: bytes=32 time=2ms TTL=125
Reply from 192.168.1.2: bytes=32 time=2ms TTL=125
Reply from 192.168.1.2: bytes=32 time=2ms TTL=125
Ping statistics for 192.168.1.2:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 2ms, Maximum = 2ms, Average = 2ms
C:\>ping 192.168.1.2
Pinging 192.168.1.2 with 32 bytes of data:


Server0
Physical
Config
Services
Desktop
Programming
Attributes
Command Prompt
Packet Tracer SERVER Command Line 1.0
C:\>ping 192.168.4.2
Pinging 192.168.4.2 with 32 bytes of data:
Reply from 192.168.4.2: bytes=32 time=2ms TTL=125
Reply from 192.168.4.2: bytes=32 time=2ms TTL=125
Reply from 192.168.4.2: bytes=32 time=2ms TTL=125
Reply from 192.168.4.2: bytes=32 time=3ms TTL=125
Ping statistics for 192.168.4.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 2ms, Maximum = 3ms, Average = 2ms
C:\>

SIC JOURNAL TYIT

## Part 1: Verify Basic Connectivity

**We can now verify the connectivity by pinging Server from PC**

**We can now verify the connecticity by pinging PC from Server**

SIC JOURNAL TYIT

## Part 2: Secure Access to Routers

We configure ACL 10 to block all remote access to the Routers and allow remote access only from PC. We type the following commands in all the Routers (Router0, Router1, and Router2). This part is divided in 2 subparts

## Part a) Set up the SSH protocol

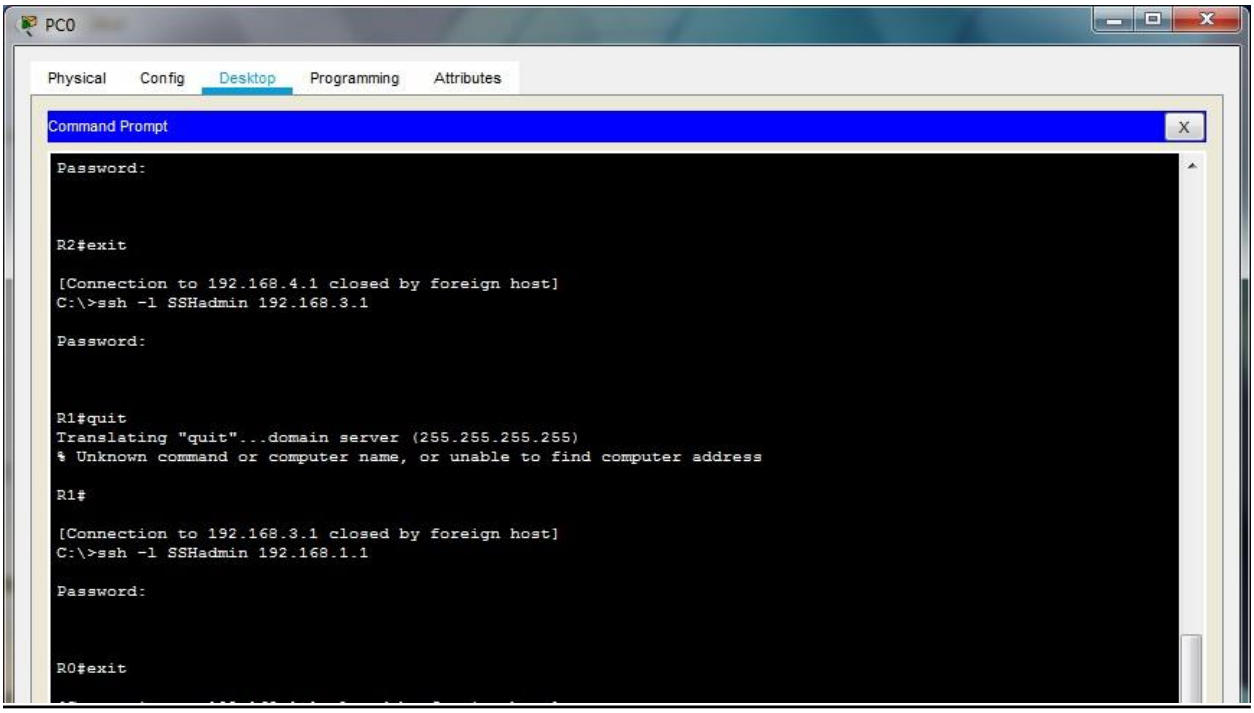
Enter the following commands in CLI mode of all Routers

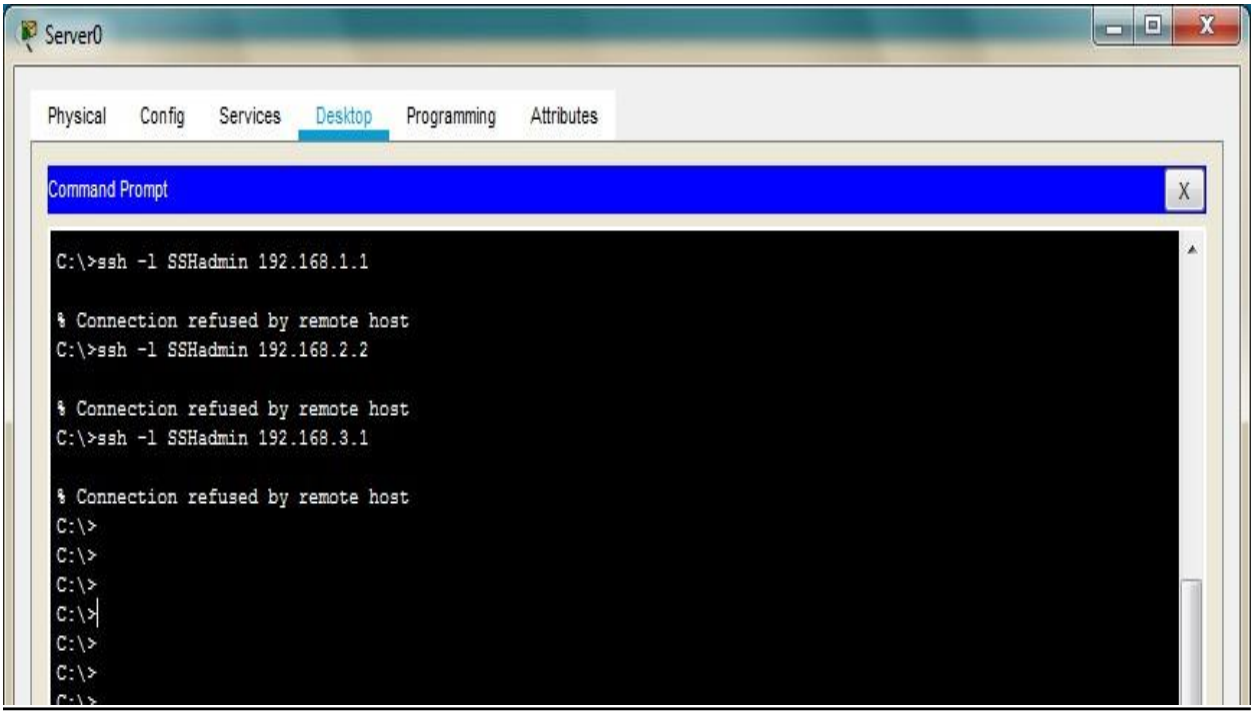
```
Router>enable
Router#configure t
Router(config)#ip domain-name ismail.com
Router(config)#hostname R0
R0(config)#
R0(config)#crypto key generate rsa
R0(config)#line vty 0 4
R0(config-line)#transport input
ssh R0(config-line)#login local
R0(config-line)#exit
R0(config)#username SSHadmin privilege 15 password ismail
R0(config)#exit
R0#
```

## Part b) Create an ACL 10 to permit remote access to PC only

Enter the following commands in CLI mode of all Routers

```
Router>enable
Router#configure terminal
Router(config)#access-list 10 permit host 192.168.4.2
Router(config)#line vty 0 4
Router(config-line)#access-class 10 in
```


PC0
Physical
Config
Desktop
Programming
Attributes
Command Prompt
Password:
R2#exit
[Connection to 192.168.4.1 closed by foreign host]
C:\>ssh -l SSHadmin 192.168.3.1
Password:
R1#quit
Translating "quit"...domain server (255.255.255.255)
% Unknown command or computer name, or unable to find computer address
R1#
[Connection to 192.168.3.1 closed by foreign host]
C:\>ssh -l SSHadmin 192.168.1.1
Password:
R0#exit


Server0
Physical
Config
Services
Desktop
Programming
Attributes
Command Prompt
C:\>ssh -l SSHadmin 192.168.1.1
% Connection refused by remote host
C:\>ssh -l SSHadmin 192.168.2.2
% Connection refused by remote host
C:\>ssh -l SSHadmin 192.168.3.1
% Connection refused by remote host
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>

SIC JOURNAL TYIT

**Now we verify the remote access from PC using the following and find it to be successful**

**Now we verify the remote access from Server using the following and find it to be failure**

SIC JOURNAL TYIT

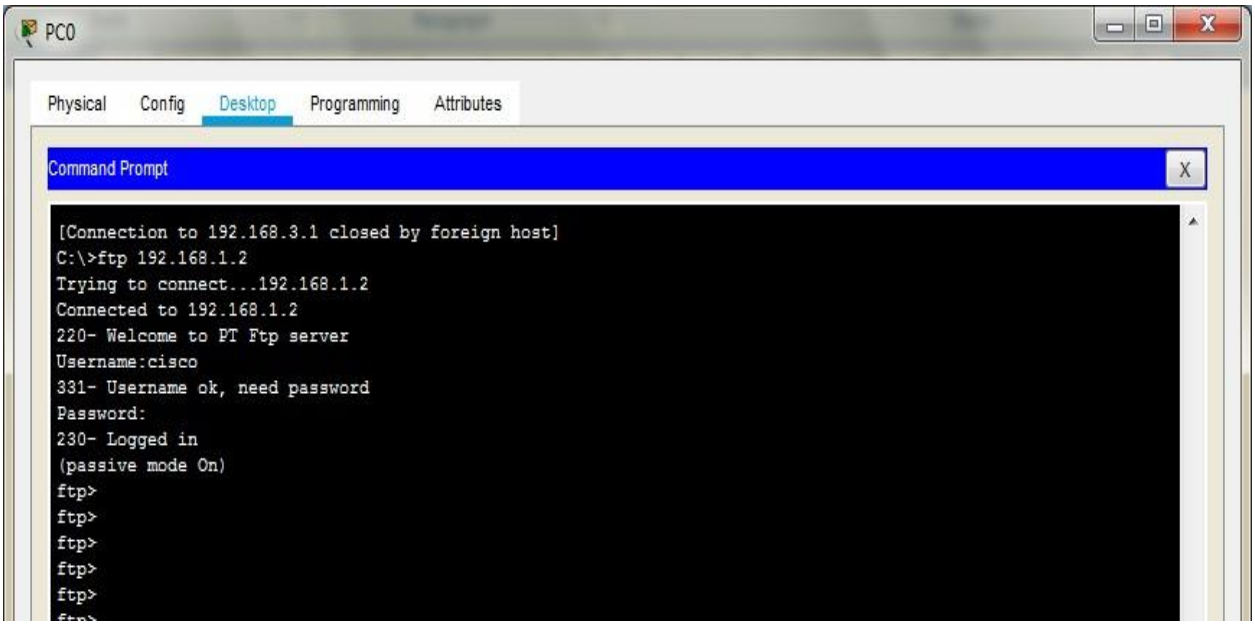
## Part 3: Create a Numbered IP ACL 120 on R1

We need to perform the following in this part

1) Create an IP ACL numbered 120 on R1 using the following rules
2) Permit any outside host to access DNS, SMTP, and FTP services on server
3) Deny any outside host access to HTTPS services on **server**
4) Permit **PC to** access **R1** via SSH. (done in previous part)

**Enter the following commands in the CLI mode of Router1**

R1>enable
R1#
R1#configure terminal
R1(config)#access-list 120 permit udp any host 192.168.1.2 eq domain
R1(config)#access-list 120 permit tcp any host 192.168.1.2
eq smtp R1(config)#access-list 120 permit tcp any host
192.168.1.2 eq ftp R1(config)#access-list 120 deny tcp any
host 192.168.1.2 eq 443
R1(config)#exit
R1#configure terminal
R1(config)#interface Serial0/1/1
R1(config-if)#ip access-group 120 in
Verify the above entering the following commands in the PC




Hence we have applied and verified all the required ACLs