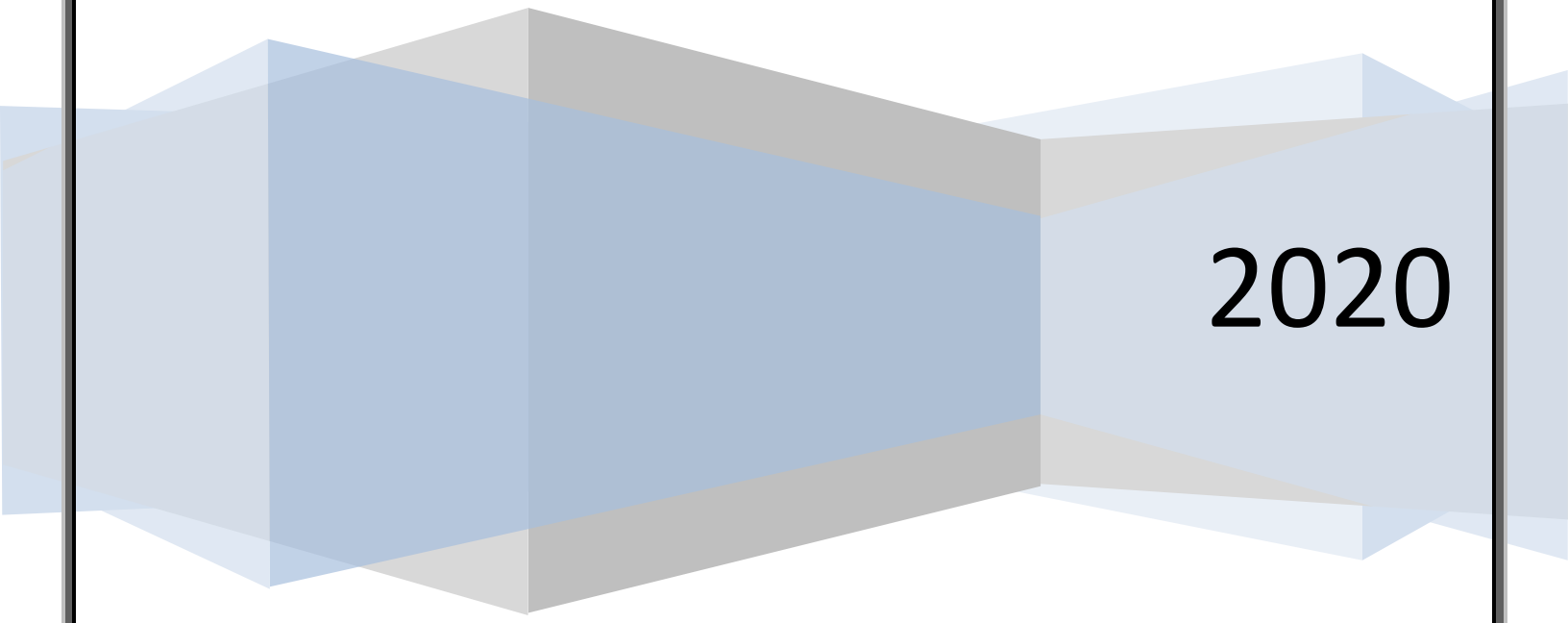
Maharashtra College

SECURITY IN COMPUTING

JOURNAL

TYIT



2020

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 get there.
- When many OSPF routers are part of the same network, information about all of the 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 go on).
- Each OSPF router passes along information about the routes and costs they've heard about to all of their adjacent OSPF routers, called **neighbors**.
- OSPF routers rely on **cost** to compute the shortest path through the network between themselves and a remote router or network destination.
- The shortest path computation is done using Djikstra's algorithm. This algorithm isn't unique to OSPF. Rather, it's a mathematical algorithm that happens to have an obvious application to networking.

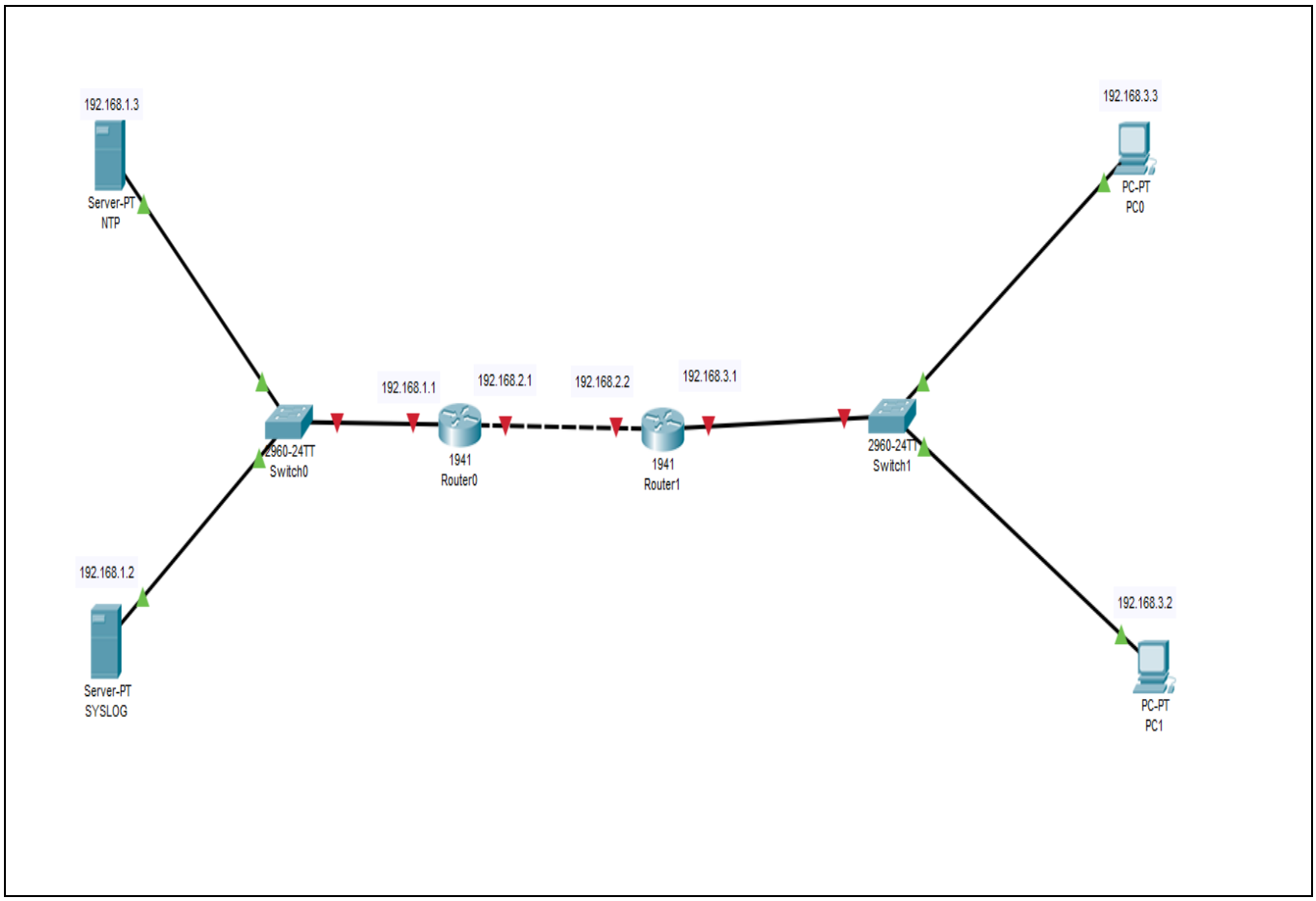
MD5 Authentication

- MD5 authentication provides higher security than plain text authentication.
- This method uses the MD5 algorithm to compute a hash value from the contents of the OSPF packet and a password (or key).
- This hash value is transmitted in the packet, along with a key ID and a non-decreasing sequence number.
- The receiver, which knows the same password, calculates its own hash value.
- If nothing in the message changes, the hash value of the receiver should match the hash value of the sender which is transmitted with the message.
- The key ID allows the routers to reference multiple passwords.
- This makes password migration easier and more secure.

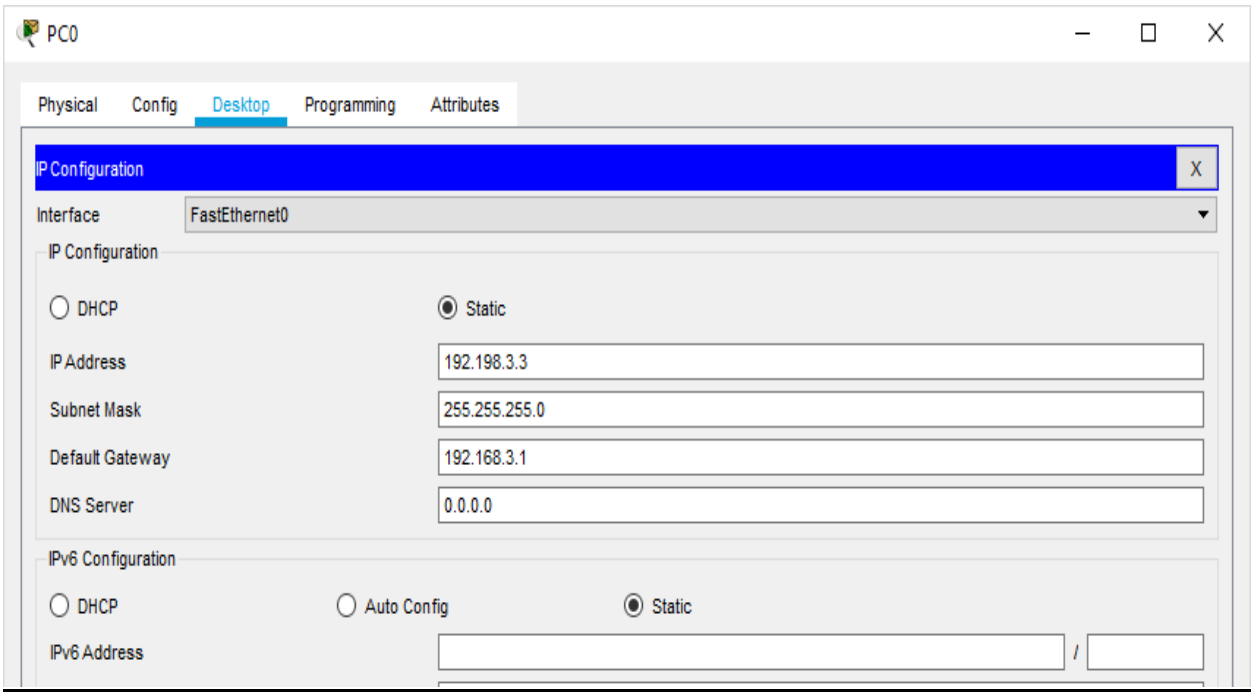
- For example, to migrate from one password to another, configure a password under a different key ID and remove the first key.
- The sequence number prevents replay attacks, in which OSPF packets are captured, modified, and retransmitted to a router.
- As with plain text authentication, MD5 authentication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

Example

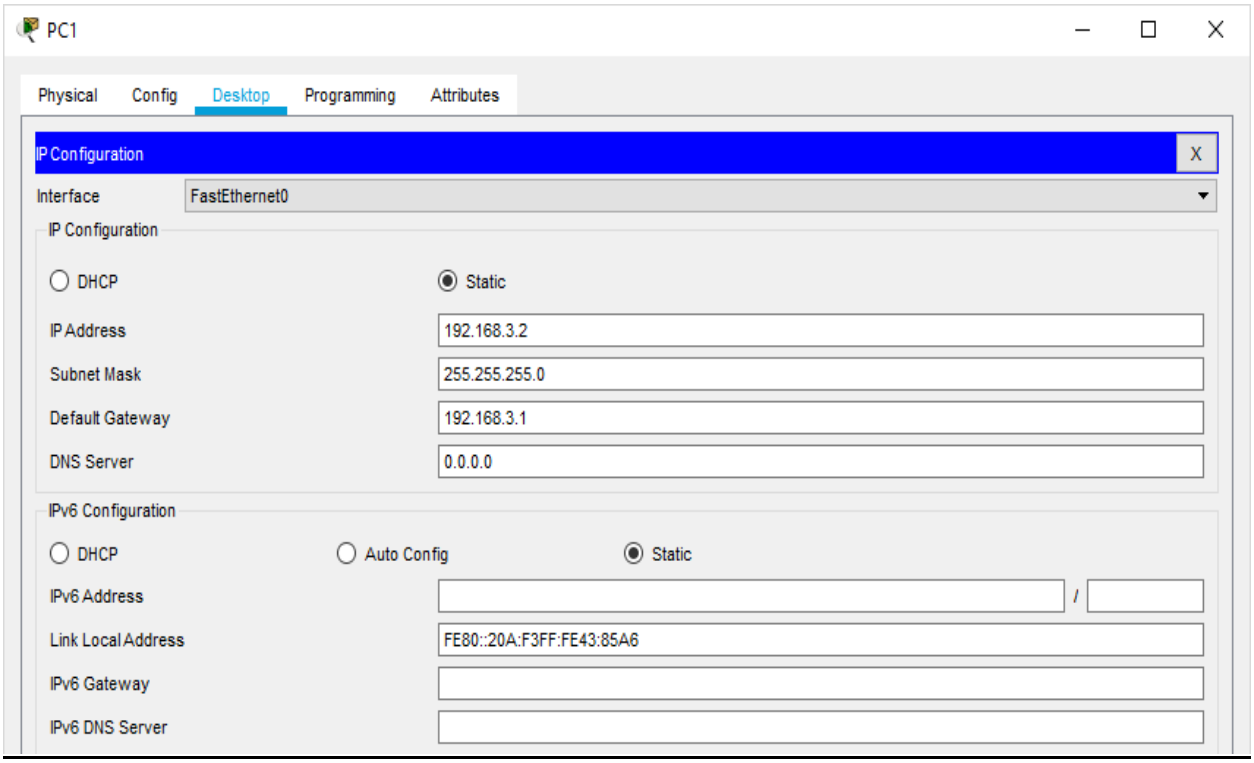
Consider the following topology



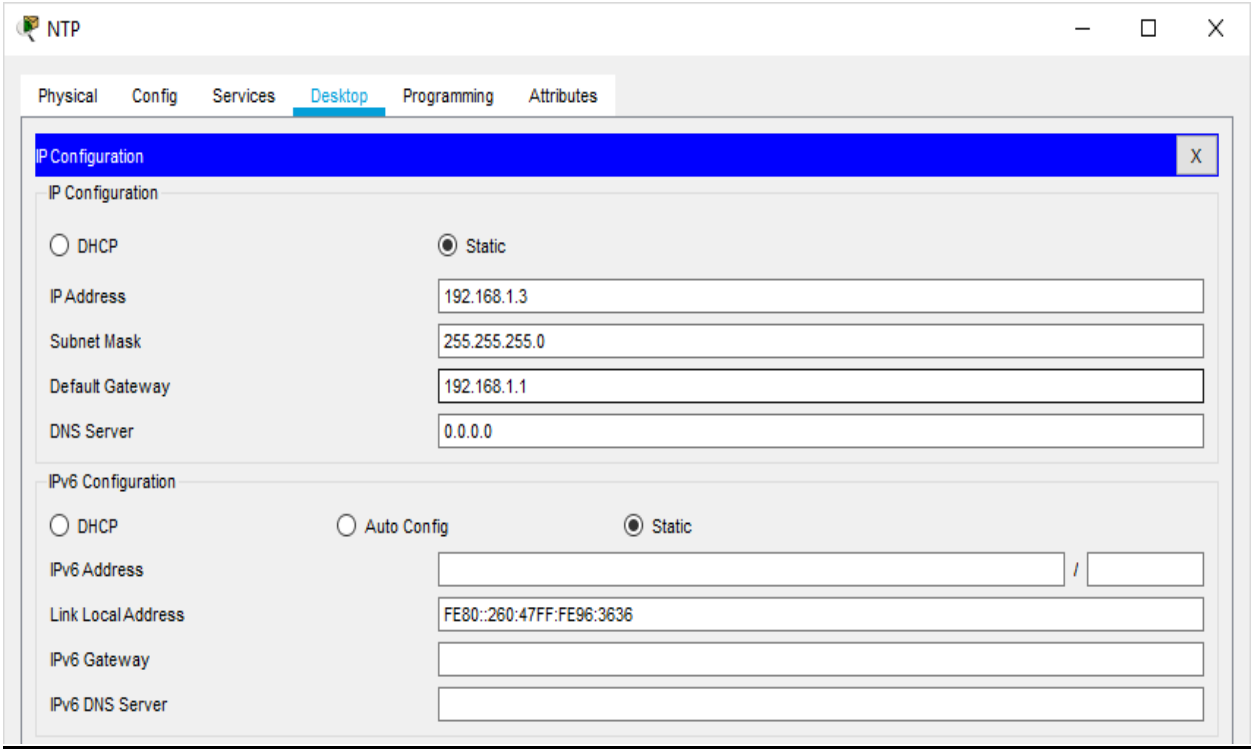
Configuring PC0



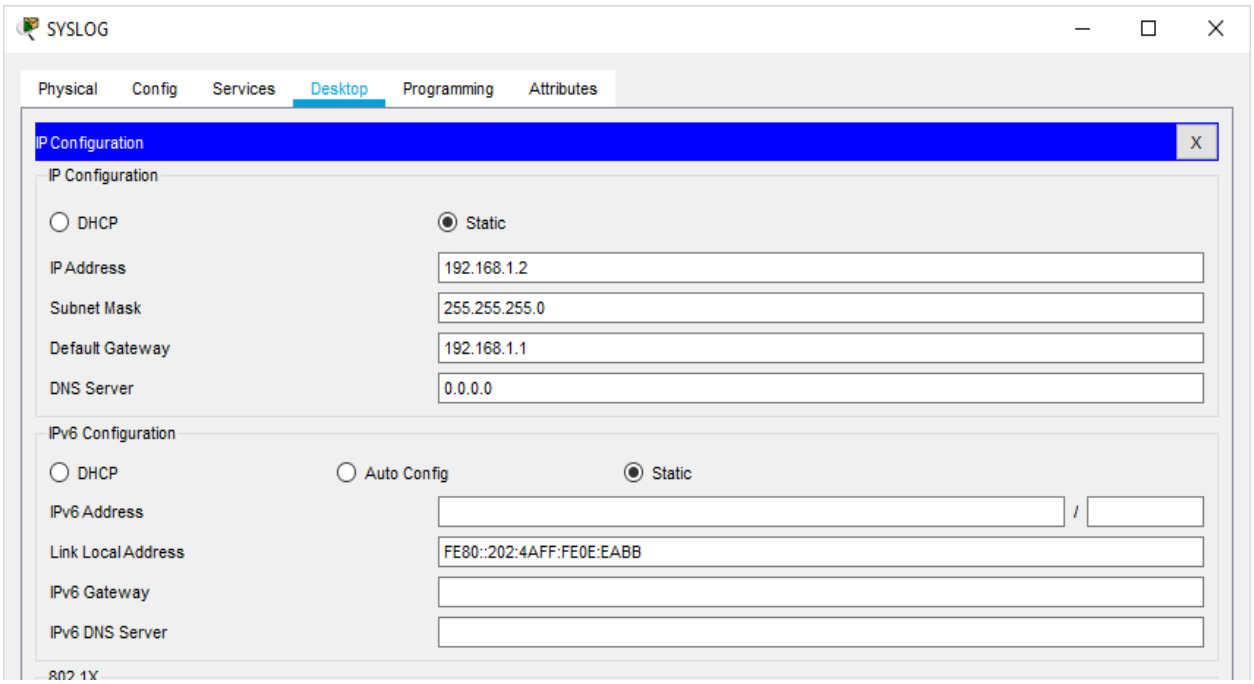
Configuring PC1



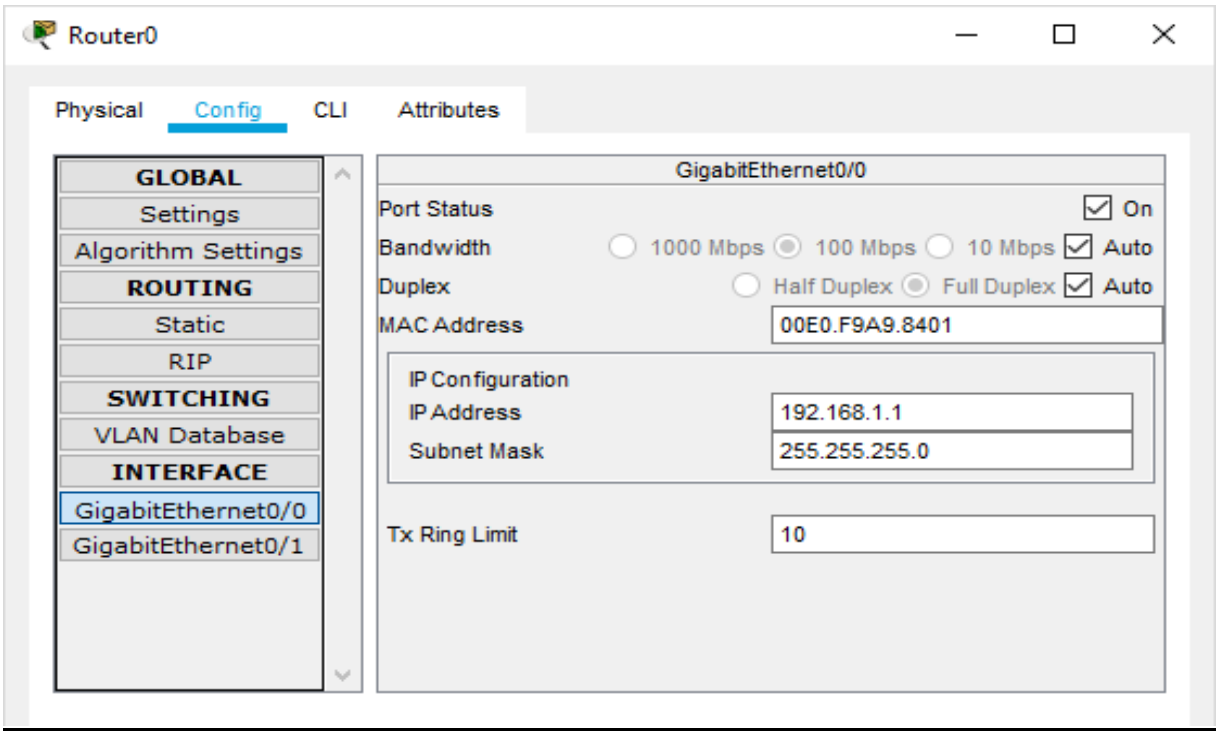
Configuring NTP Server

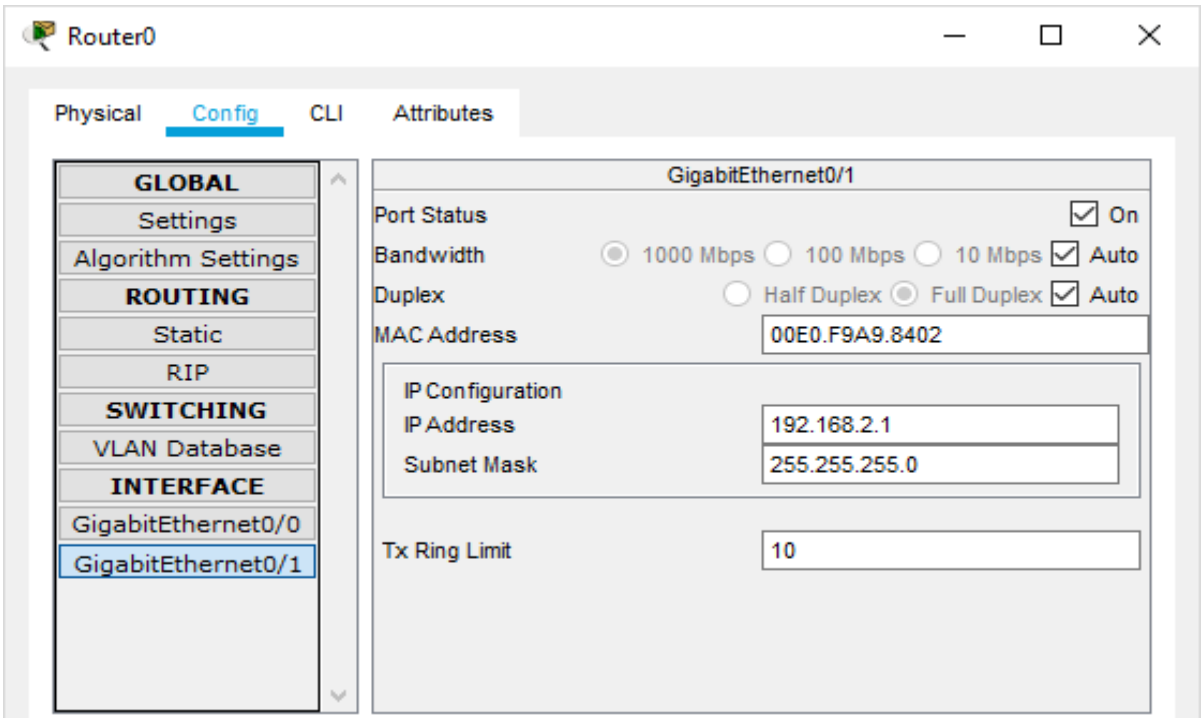


Configuring SYSLOG Server

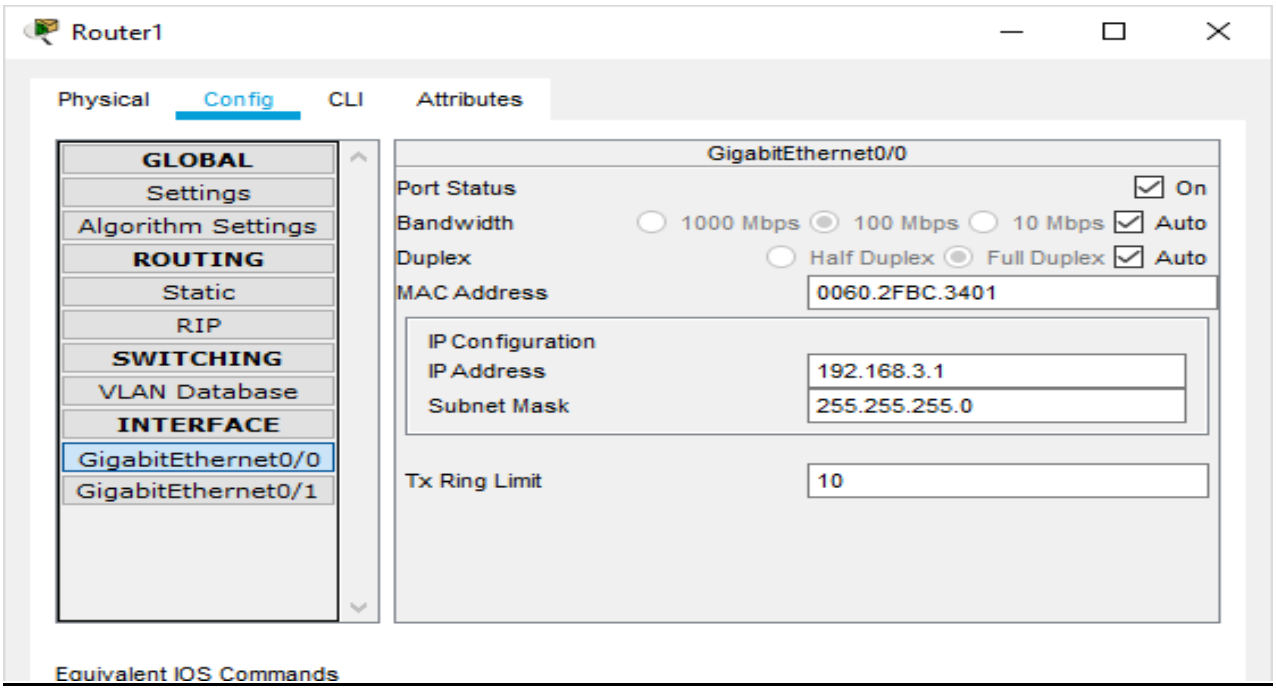


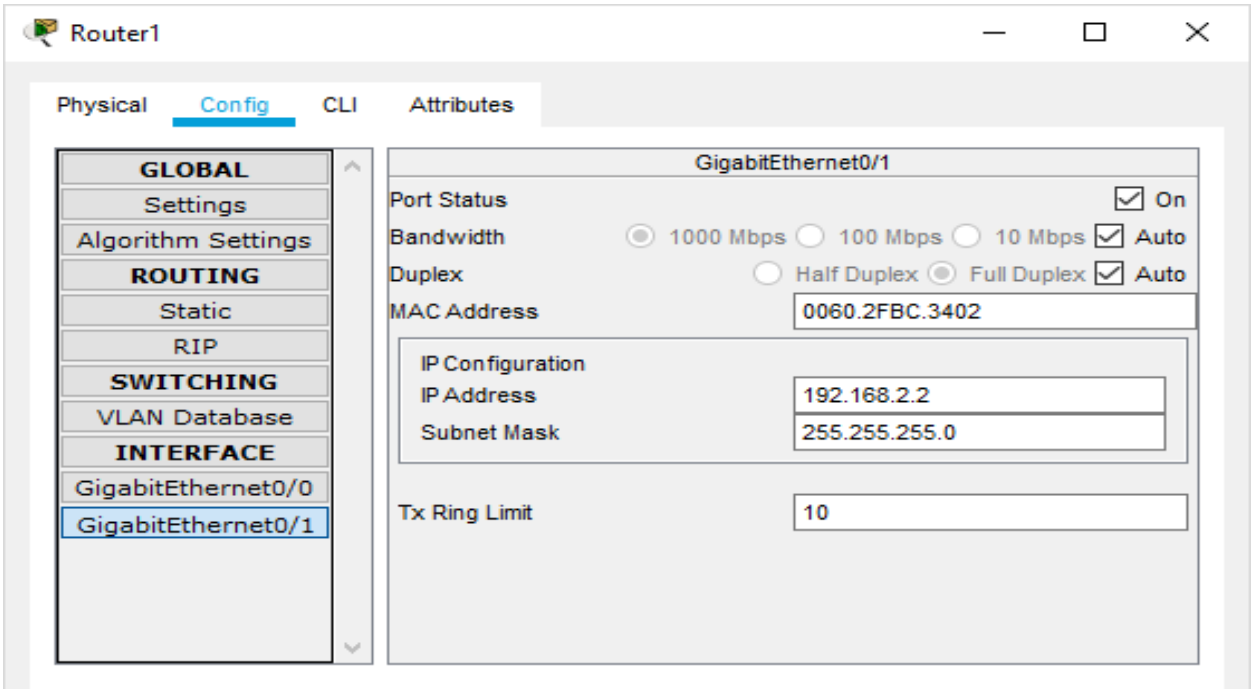
Configuring Router0





Configuring Router1





Part 1: Configure OSPF MD5 Authentication

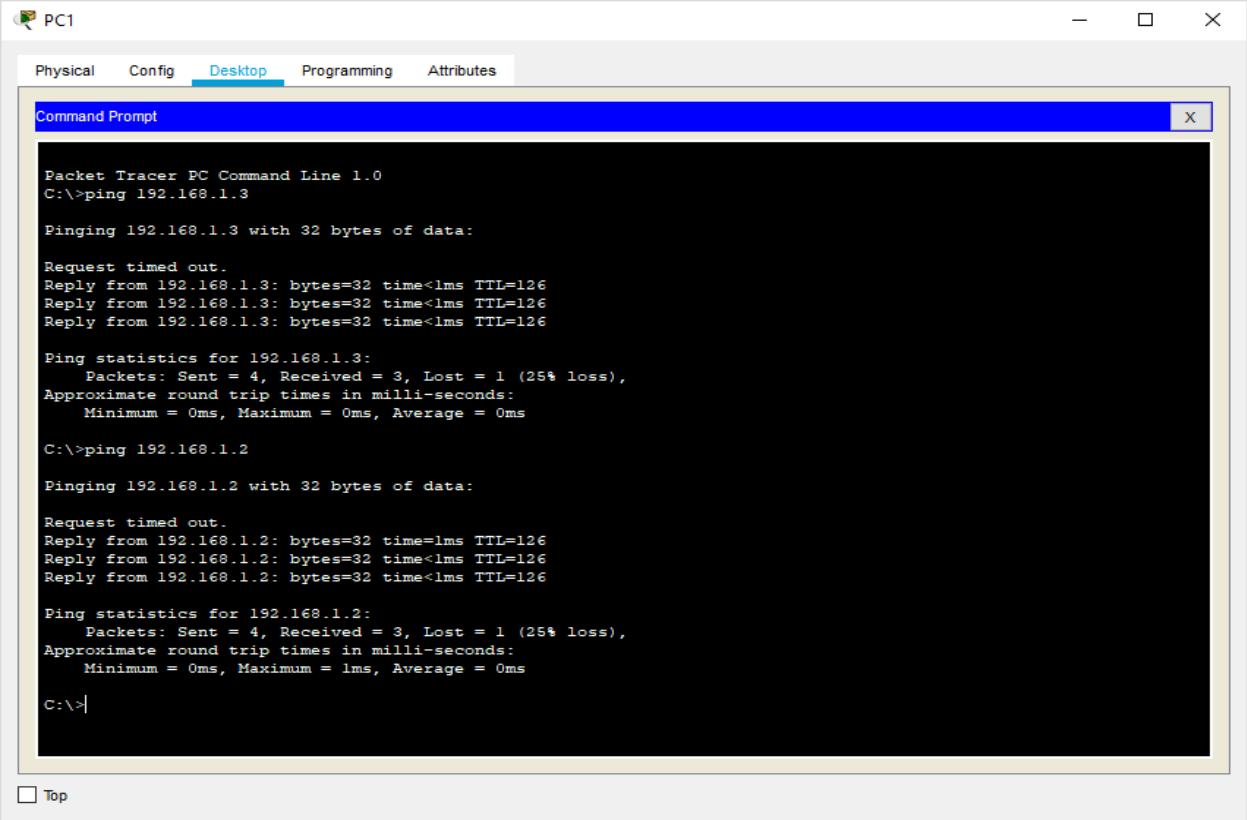
ROUTER 0: Type the following command in the CLI mode

```
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

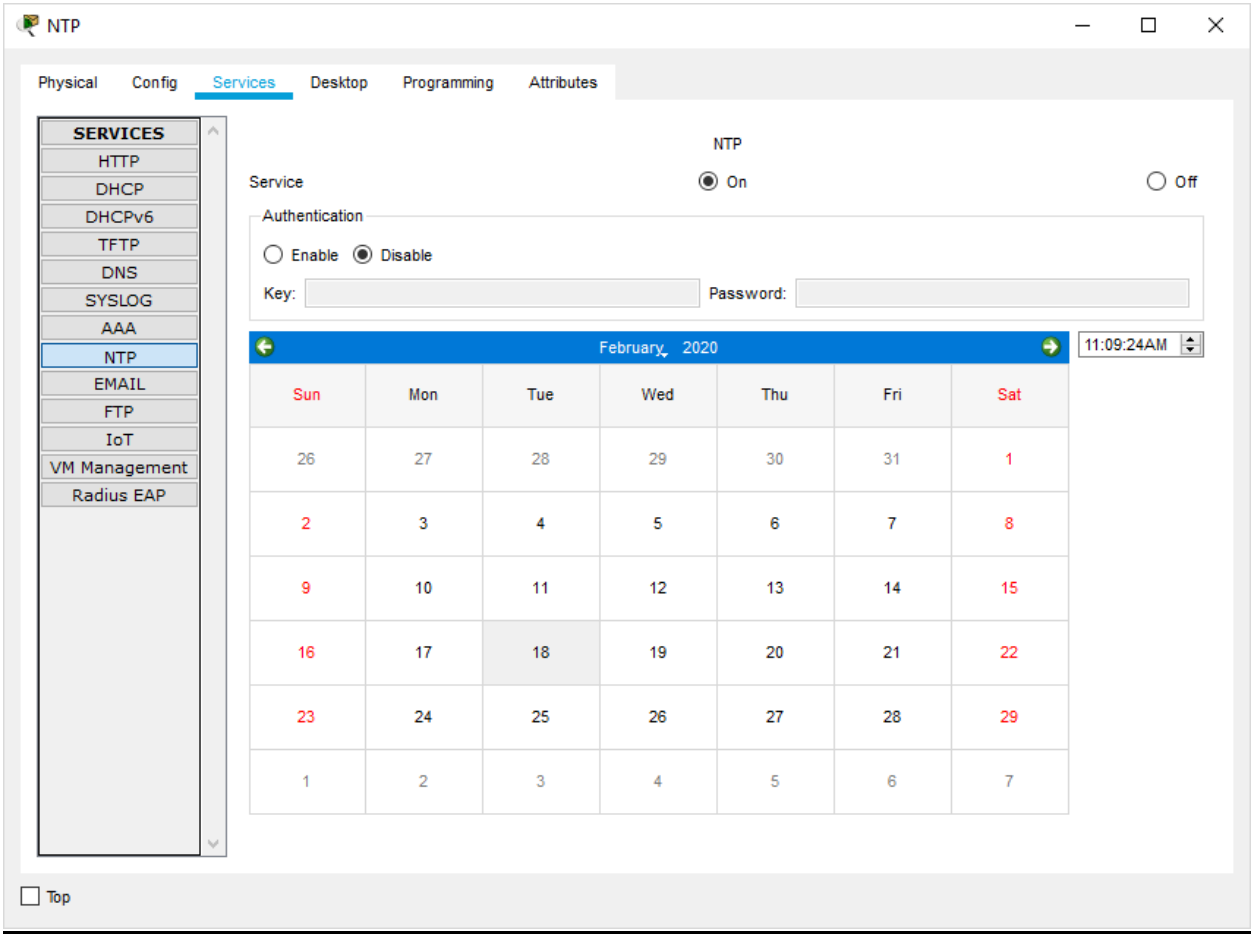
MD5 Authentication has been verified

b) NTP

- Network Time Protocol (NTP) is a TCP/IP protocol used to synchronize computer clocks across data networks.
- 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 effects of variable latency over packet-switched data networks through a jitter buffer.

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 the Routers

```
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

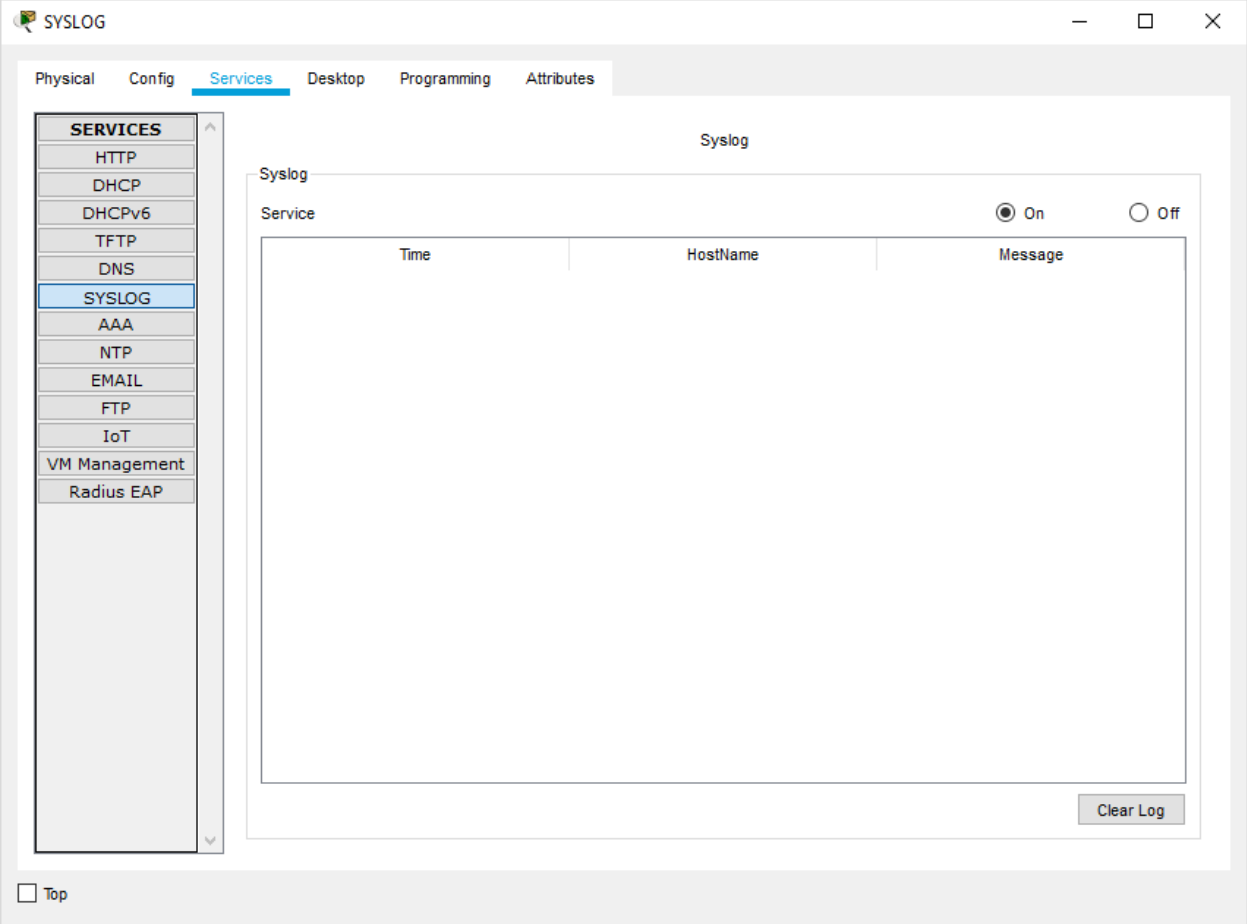
```
Router#show clock
11:14:58.985 UTC Tue Feb 18 2020
Router#
```

c) SYSLOG server

Configure SYSLOG Server and enable the service

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

Turn ON the SYSLOG service on the server

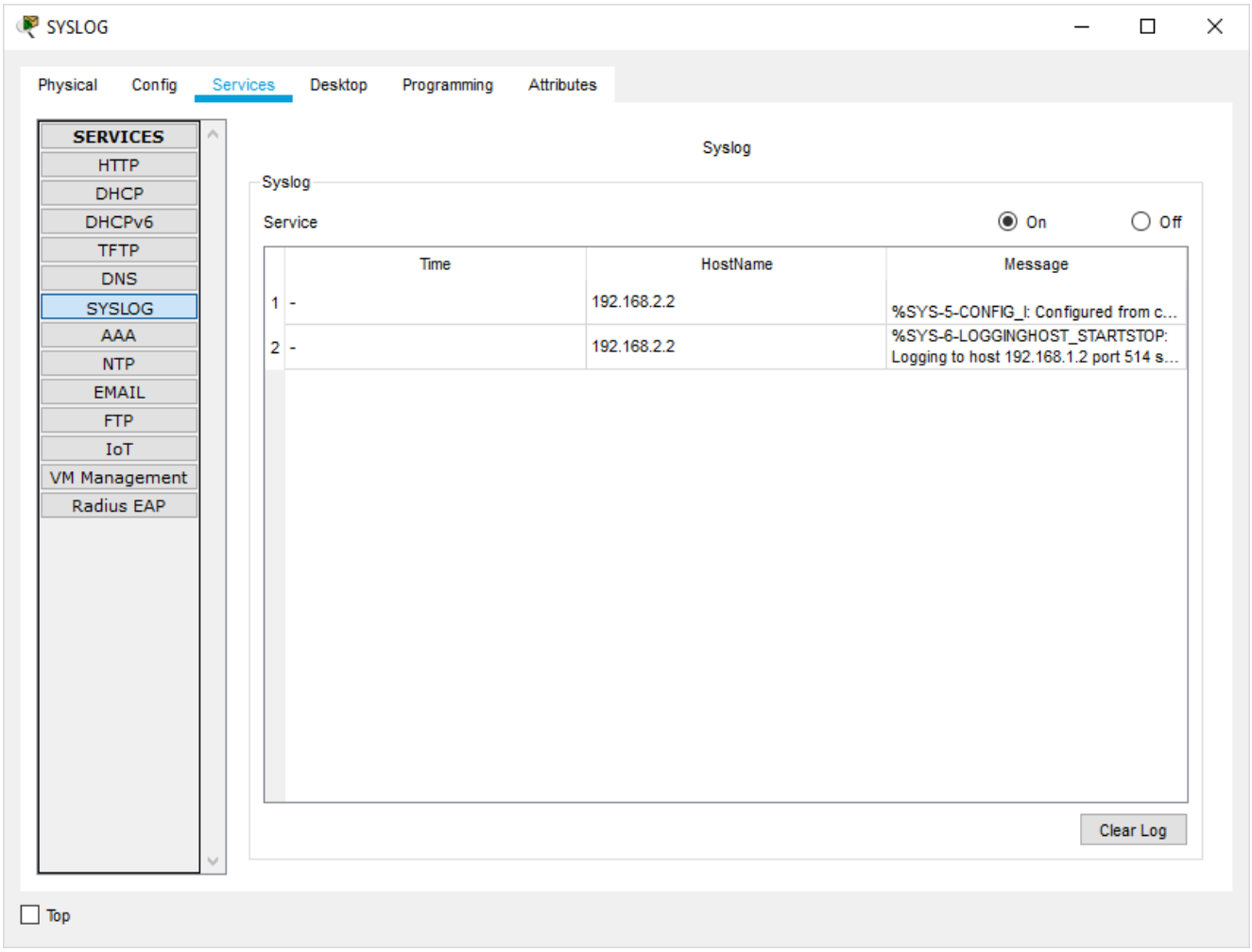


And Turn OFF on all other Servers

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

```
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 remote computers.
- 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 between them.
- It organizes the secure connection by authenticating the client and opening the correct shell environment if the verification is successful.

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

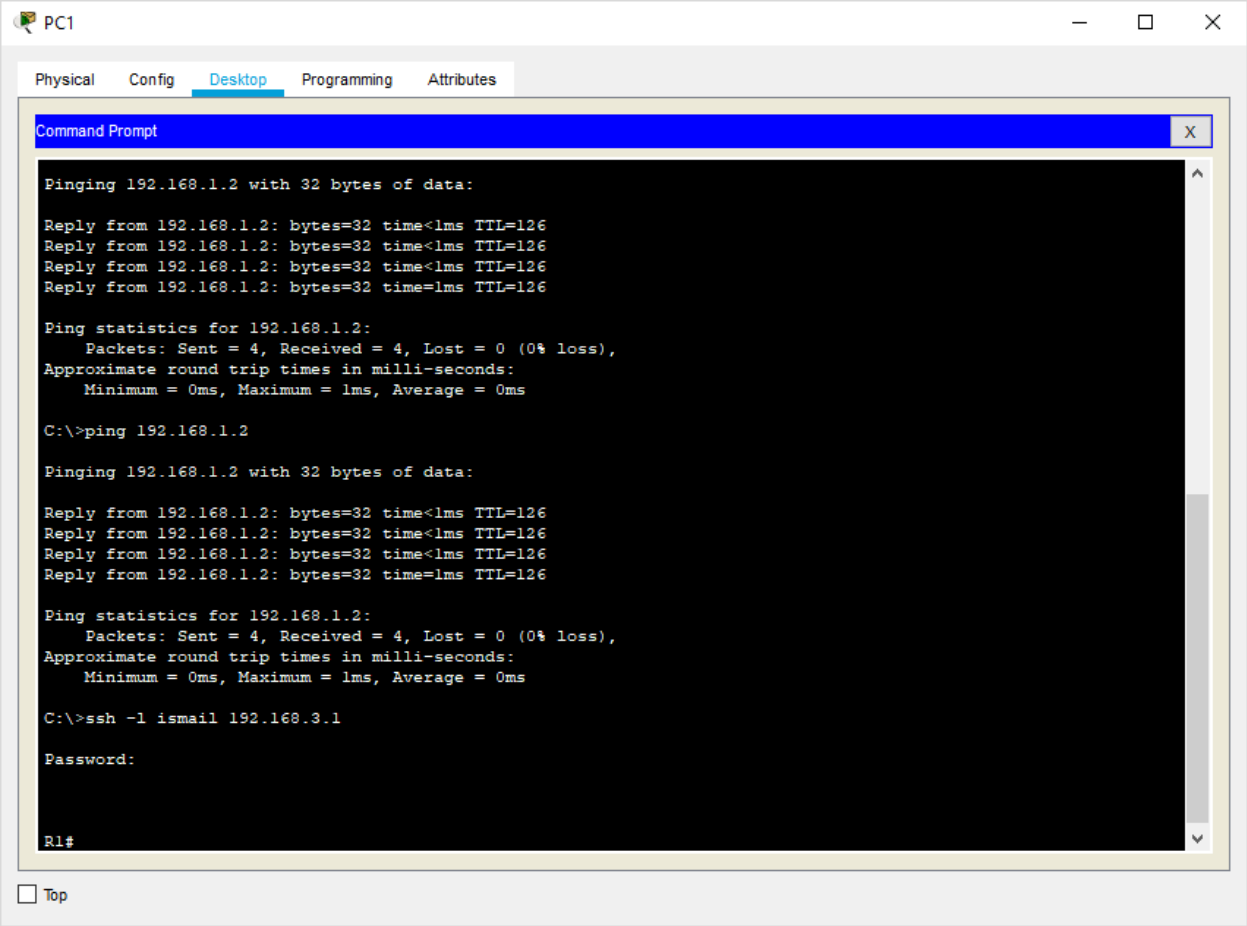
```
Router#configure terminal
Router(config)#ip domain-name ismail.com
Router(config)#hostname R1
R1(config)#
R1(config)#crypto key generate rsa


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