
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 Dijkstra'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

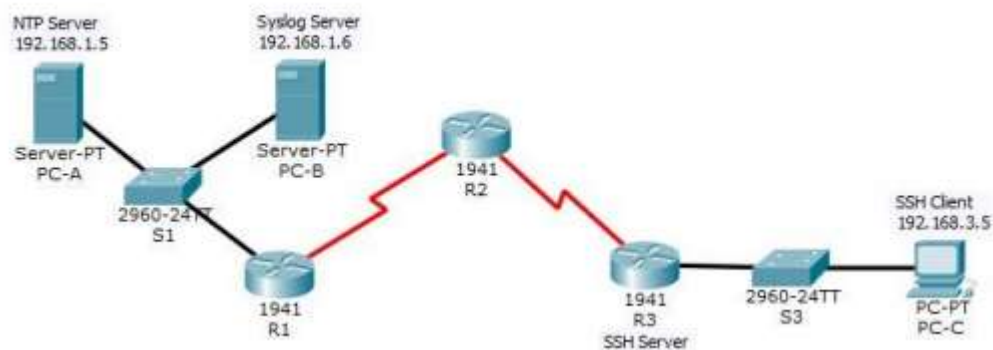
- MD5 authentication provides higher security than plain text authentication.
- This method uses the MD5 algorithm to compute a hash value from the contents of the OSPF packet and a password (or key).
- This hash value is transmitted in the packet, along with a key ID and a non-decreasing sequence number.
- 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

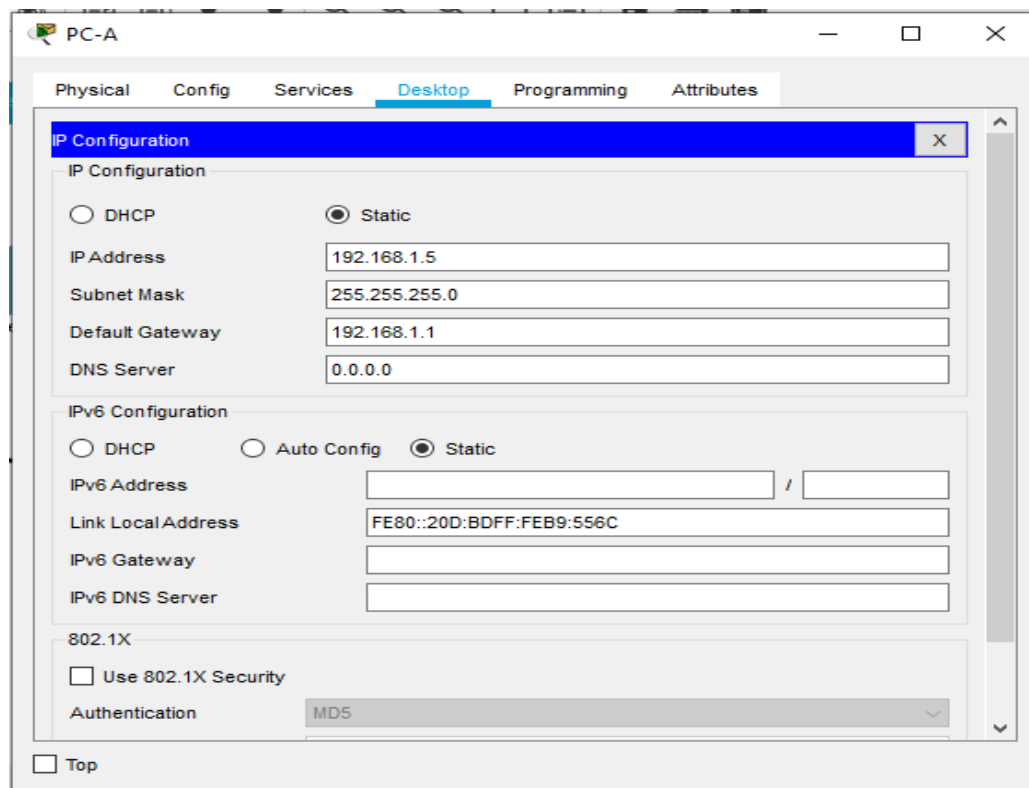
Consider the following topology

Topology



Addressing Table

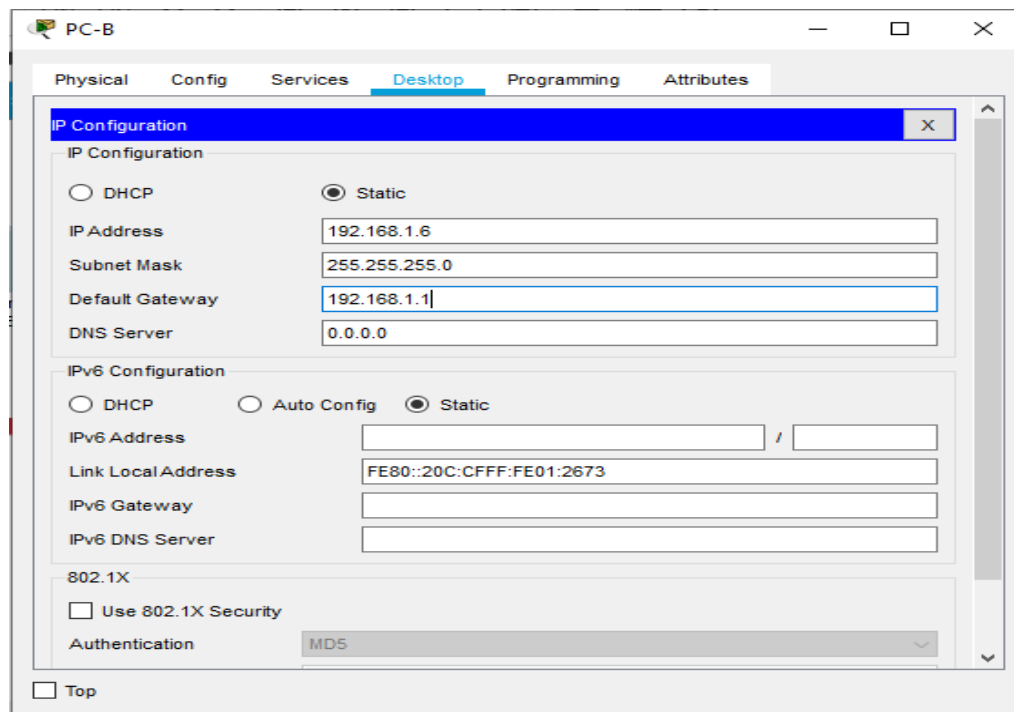
Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	G0/1	192.168.1.1	255.255.255.0	N/A	S1 F0/5
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A	N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A	N/A
	S0/0/1 (DCE)	100.2.2.2	255.255.255.252	N/A	N/A
R3	G0/1	192.168.3.1	255.255.255.0	N/A	S3 F0/5
	S0/0/1	100.2.2.1	255.255.255.252	N/A	N/A
PC-A	NIC	192.168.1.5	255.255.255.0	192.168.1.1	S1 F0/6
PC-B	NIC	192.168.1.6	255.255.255.0	192.168.1.1	S1 F0/18
PC-C	NIC	192.168.3.5	255.255.255.0	192.168.3.1	S3 F0/18

Configuring PC-A

The screenshot shows the 'PC-A' configuration window with the 'Desktop' tab selected. The 'IP Configuration' section is expanded, showing the following settings:

- IP Configuration:**
 - ☐ DHCP
 - ☒ Static
 - IP Address: 192.168.1.5
 - 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: (empty)
 - Link Local Address: FE80::20D:BDFF:FEB9:556C
 - IPv6 Gateway: (empty)
 - IPv6 DNS Server: (empty)
- 802.1X:**
 - ☐ Use 802.1X Security
 - Authentication: MD5

At the bottom, there is a 'Top' button.

Configuring PC-B

The screenshot shows the 'PC-B' configuration window with the 'Desktop' tab selected. The 'IP Configuration' section is expanded, showing the following settings:

- IP Configuration:**
 - ☐ DHCP
 - ☒ Static
 - IP Address: 192.168.1.6
 - 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: (empty)
 - Link Local Address: FE80::20C:CFFF:FE01:2673
 - IPv6 Gateway: (empty)
 - IPv6 DNS Server: (empty)
- 802.1X:**
 - ☐ Use 802.1X Security
 - Authentication: MD5

At the bottom, there is a 'Top' button.

Configuring PC-C

PC-C

Physical Config **Desktop** Programming Attributes

IP Configuration

Interface: FastEthernet0

IP Configuration

☐ DHCP ☒ Static

IP Address: 192.168.3.5

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::2D0:FFFF:FEA1:1819

IPv6 Gateway:

IPv6 DNS Server:

802.1X

☐ Use 802.1X Security

☐ Top

Configuring R1

R1

Physical Config **CLI** Attributes

GLOBAL

Settings

Algorithm Settings

ROUTING

Static

RIP

SWITCHING

VLAN Database

INTERFACE

GigabitEthernet0/0

GigabitEthernet0/1

Serial0/0/0

Serial0/0/1

Serial0/1/0

Serial0/1/1

GigabitEthernet0/1

Port Status: ☒ On

Bandwidth: 1000 Mbps ☐ 100 Mbps ☐ 10 Mbps ☒ Auto

Duplex: ☒ Half Duplex ☐ Full Duplex ☒ Auto

MAC Address: 0030.A3E7.1802

IP Configuration

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

Tx Ring Limit: 10

Equivalent IOS Commands

```
%LINK-S-CHANGED: Interface GigabitEthernet0/1, changed state to up
%LINEPROTO-S-UPDOWN: Line protocol on Interface GigabitEthernet0/1,
changed state to up
```

☐ Top

R1

Physical Config **CLI** Attributes

GLOBAL

Settings

Algorithm Settings

ROUTING

Static

RIP

SWITCHING

VLAN Database

INTERFACE

GigabitEthernet0/0

GigabitEthernet0/1

Serial0/0/0

Serial0/0/1

Serial0/1/0

Serial0/1/1

Serial0/0/0

Port Status: ☒ On

Duplex: Full Duplex

Clock Rate: 64000

IP Configuration

IP Address: 10.1.1.1

Subnet Mask: 255.0.0.0

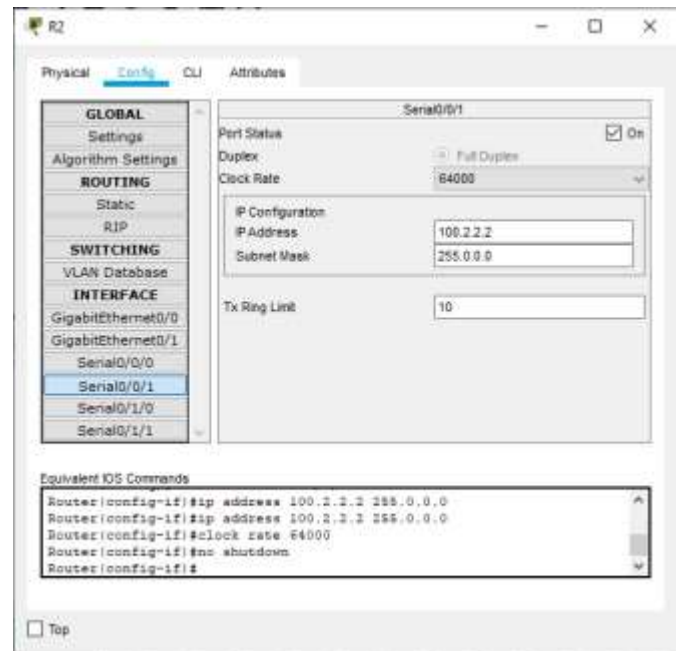
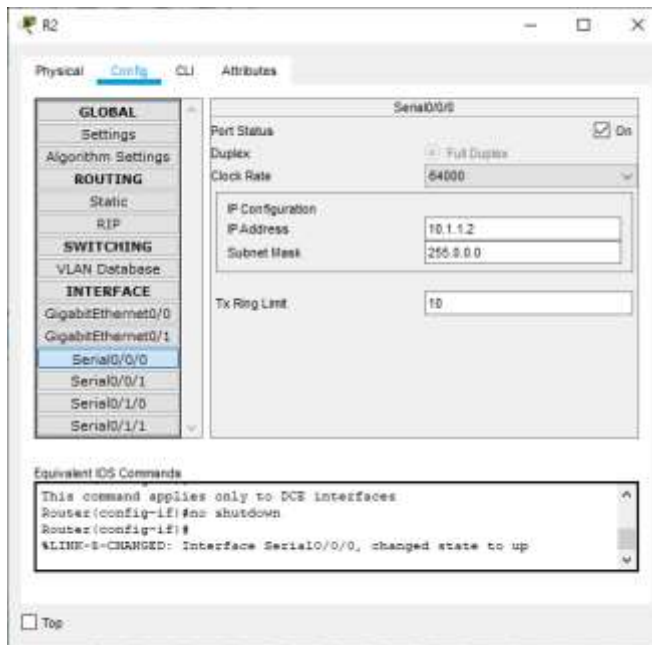
Tx Ring Limit: 10

Equivalent IOS Commands

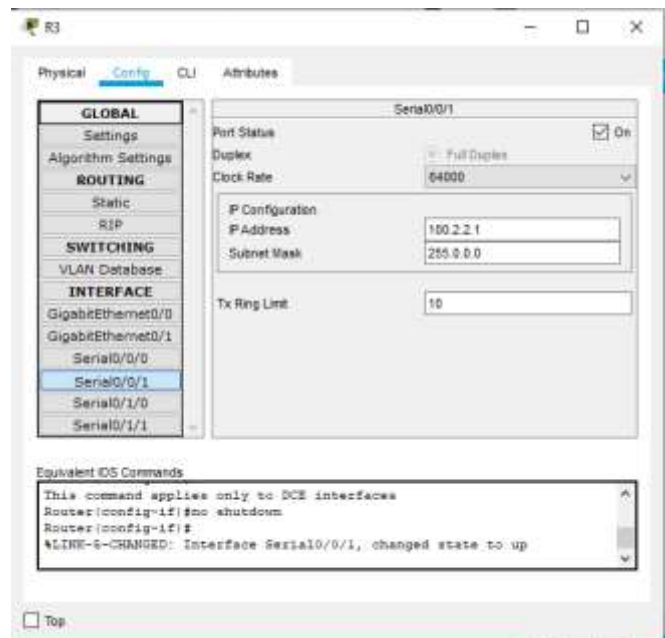
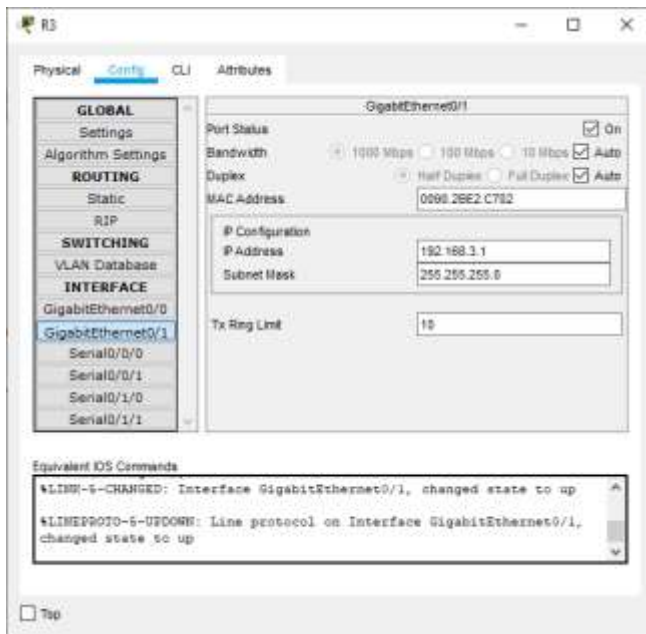
```
Router(config-if)#ip address 10.1.1.1 255.0.0.0
Router(config-if)#ip address 10.1.1.1 255.0.0.0
Router(config-if)#clock rate 64000
Router(config-if)#no shutdown
Router(config-if)#
```

☐ Top

Configuring R2



Configuring R3



Part 1: Configure OSPF MD5 Authentication

ROUTER 1: Type the following command in the CLI mode

```
Router>enable
Router#configure terminal
Router(config)#router ospf 1
Router(config-router)#network 192.168.1.0 0.255.255.255 area 1
Router(config-router)#network 10.1.1.0 0.255.255.255 area 1
Router(config-router)#exit
Router(config)#exit
Router#
```

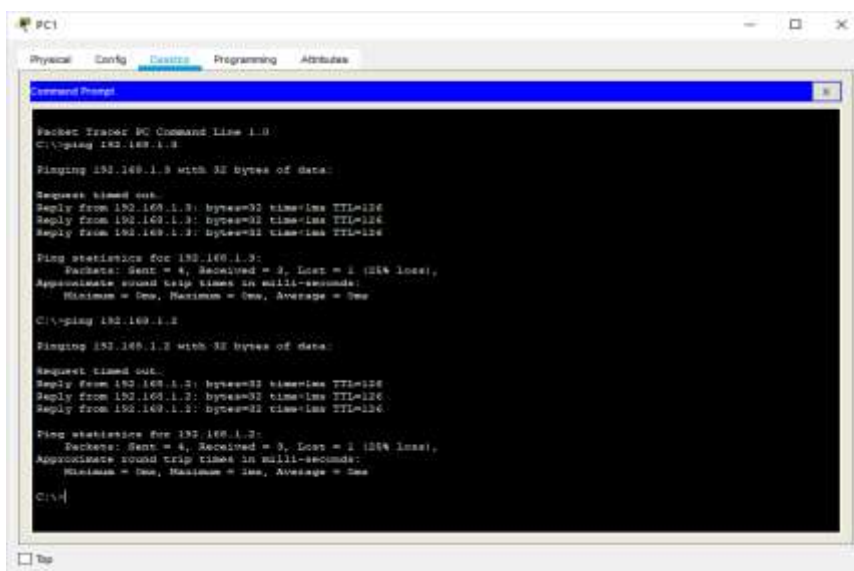
ROUTER 2: Type the following command in the CLI mode

```
Router>enable
Router#configure terminal
Router(config)#router ospf 1
Router(config-router)#network 10.1.1.0 0.255.255.255 area 1
Router(config-router)#network 100.2.2.0 0.255.255.255 area 1
Router(config-router)#exit
Router(config)#exit
Router#
```

ROUTER 3: 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 100.2.2.0 0.255.255.255 area 1
Router(config-router)#exit
Router(config)#exit
Router#
```

Now we verify the connectivity by using the following



```
PC1
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
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=1ms TTL=124
Reply from 192.168.1.2: bytes=32 time=1ms TTL=124
Reply from 192.168.1.2: bytes=32 time=1ms TTL=124

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.3: bytes=32 time=1ms TTL=124
Reply from 192.168.1.3: bytes=32 time=1ms TTL=124
Reply from 192.168.1.3: bytes=32 time=1ms TTL=124

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Hence OSPF has been verified

MD5 Authentication

ROUTER 1: Type the following command in the CLI mode

```
Router>enable
Router#
Router#configure terminal
Router(config)#interface Serial0/0/0
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 2: Type the following command in the CLI mode

```
Router>enable
Router#
Router#configure terminal
Router(config)#interface Serial0/0/0
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 Router1

```
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

The screenshot displays the NTP configuration window. On the left, a list of services includes HTTP, DHCP, DHCPv6, TFTP, DNS, SYSLOG, AAA, NTP (selected), EMAIL, FTP, IoT, VM Management, and Radius EAP. The main area shows the NTP service configuration. The 'Service' is set to 'On'. The 'Authentication' section has 'Enable' and 'Disable' radio buttons, with 'Disable' selected. There are input fields for 'Key' and 'Password'. Below this is a calendar for February 2020, with dates 1 through 29. The current time is 11:09:24AM. A 'Top' button is located at the bottom left.

Now Go to CLI Mode of Router1 and type the following commands on both the Routers

```
Router#enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ntp server 192.168.1.5
Router(config)#ntp update-calendar
Router(config)#exit
Router#
```

To verify the Output we use the following command

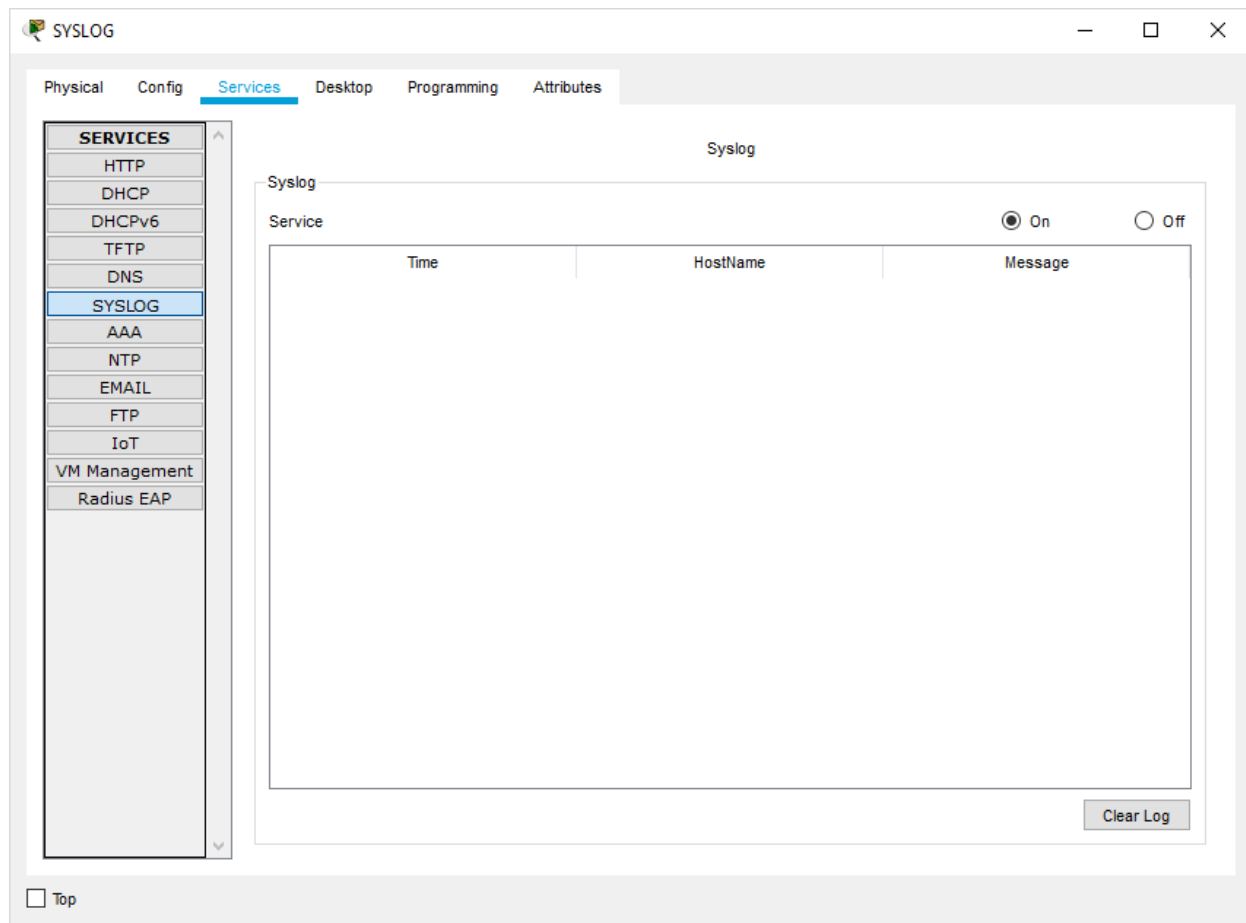
```
Router#show clock
18:12:43.760 UTC Fri Jan 14 2022
Router#
```

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

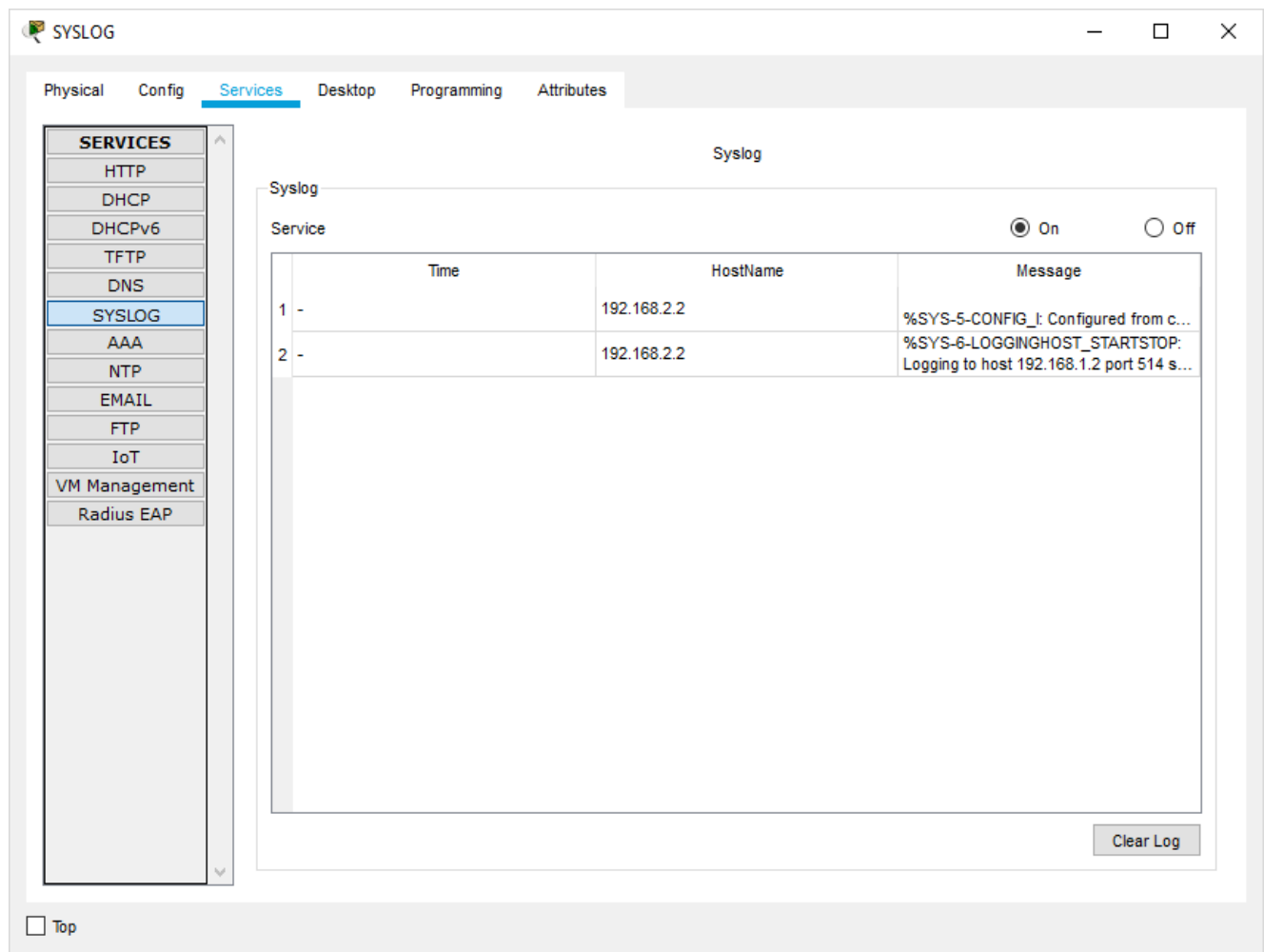


And Turn OFF on all other Servers

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

```
Router#  
Router#configure terminal  
Router(config)#logging 192.168.1.6  
Router(config)#exit  
Router#
```

Output:



The screenshot shows the Syslog configuration window with the 'Services' tab selected. The 'Syslog' service is turned 'On'. A table displays the log entries:

Service	Time	HostName	Message
1 -		192.168.2.2	%SYS-5-CONFIG_I: Configured from c...
2 -		192.168.2.2	%SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 192.168.1.2 port 514 s...

At the bottom right of the log table is a 'Clear Log' button. The left sidebar lists various services, with 'SYSLOG' highlighted. The bottom left has a 'Top' link.

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 Router3 and type the following commands.

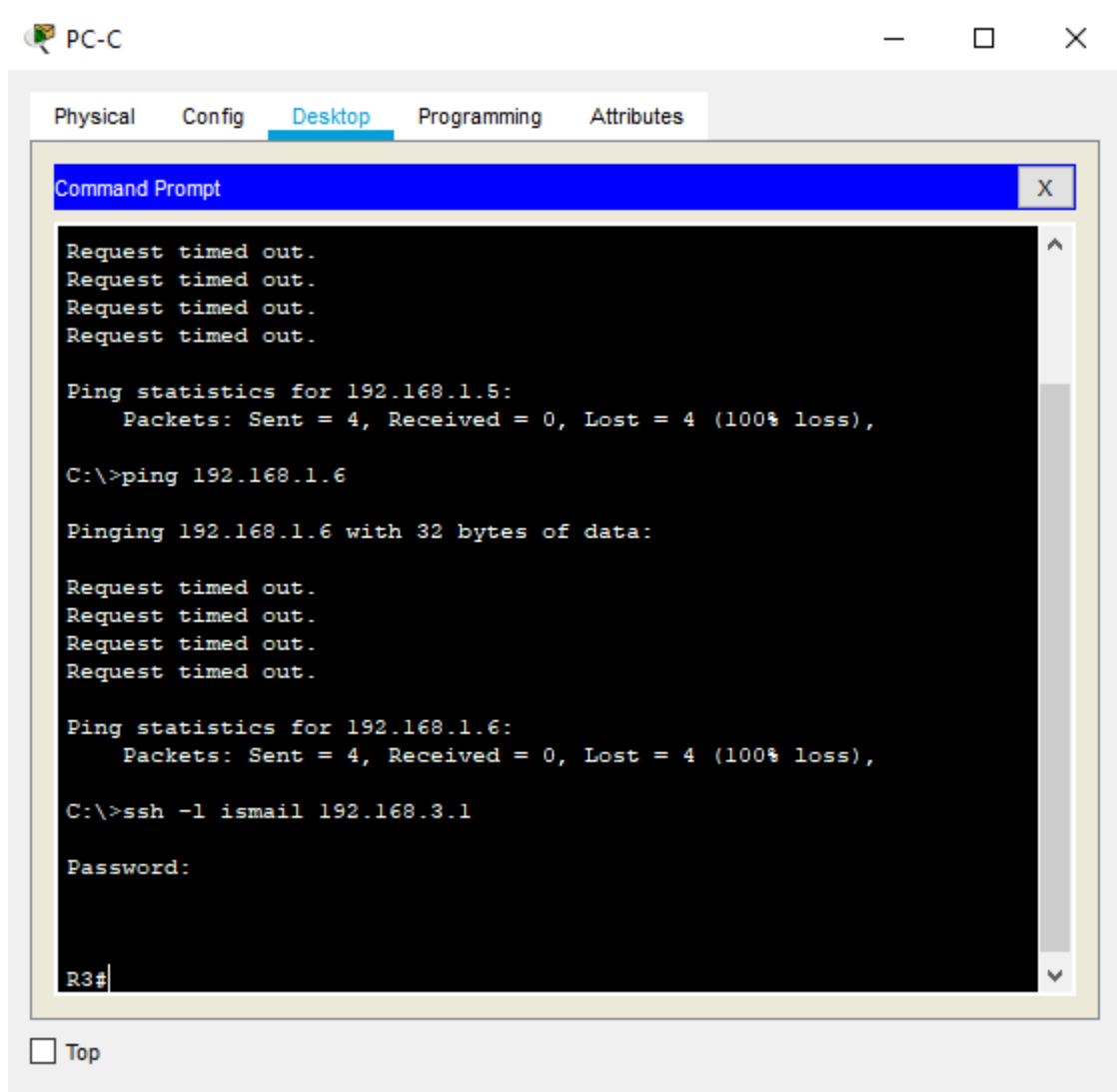
```
Router#configure terminal
Router(config)#ip domain-name ismail.com
Router(config)#hostname R3
R3(config)#
R3(config)#crypto key generate rsa
```

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.

```
R3(config)#line vty 0 4
R3(config-line)#transport input ssh
R3(config-line)#login local
R3(config-line)#exit
R3(config)#username ismail privilege 15 password cisco
R3(config)#
```

Output: Go to cmd of PC-C and type the command

ssh -l ismail 192.168.3.1 and type the password cisco



The screenshot shows a window titled "PC-C" with a tabbed interface. The "Desktop" tab is active, displaying a "Command Prompt" window. The Command Prompt shows the following text:

```
Request timed out.
Request timed out.
Request timed out.
Request timed out.

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

C:\>ping 192.168.1.6

Pinging 192.168.1.6 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.6:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ssh -l ismail 192.168.3.1

Password:

R3#
```

At the bottom of the Command Prompt window, there is a checkbox labeled "Top".

Hence SSH is also verified