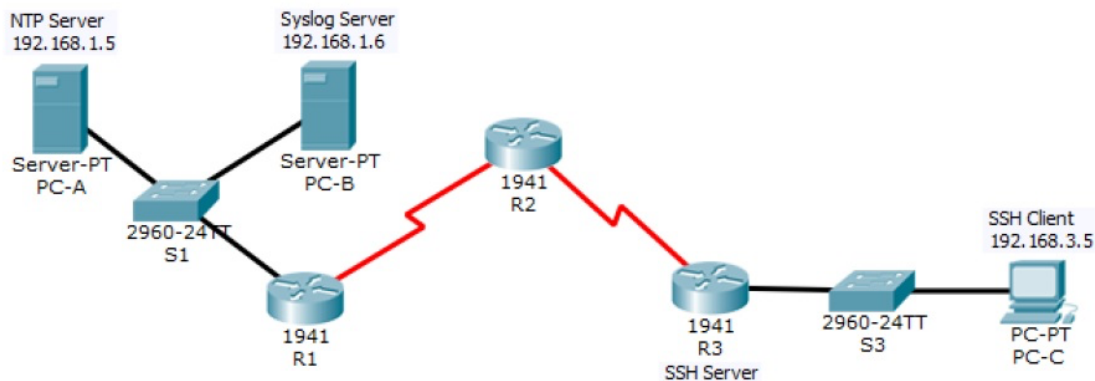


Name	Sanjeev Gupta	Roll Number	21302B0023
Class	TYBsc IT	Division	C
Subject/Course	Security in Computing		
Topic	Configure Cisco Routers for Syslog, NTP, and SSH Operations		

Topology and Addressing Table

Use the pre-configured topology shared as an attachment with this worksheet. Configure this topology for Syslog, NTP, and SSH Operations

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)	10.2.2.2	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	10.2.2.1	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	S2 F0/18
PC-C	NIC	192.168.3.5	255.255.255.0	192.168.3.1	S3 F0/18

Part 1: Configure OSPF MD5 Authentication

Step 1: Test connectivity. All devices should be able to ping all other IP addresses.

Step 2: Configure OSPF MD5 authentication for all the routers in area 0.

Configure OSPF MD5 authentication for all the routers in area 0.

R1(config)# router ospf 1

R1(config-router)# area 0 authentication message-digest

R2(config)# router ospf 1

R2(config-router)# area 0 authentication message-digest

```

R3(config)# router ospf 1
R3(config-router)# area 0 authentication message-digest
Step 3: Configure the MD5 key for all the routers in area 0.
Configure an MD5 key on the serial interfaces on R1, R2 and R3. Use the password MD5pa55 for key 1.
R1(config)# interface s0/0/0
R1(config-if)# ip ospf message-digest-key 1 md5 MD5pa55
R2(config)# interface s0/0/0
R2(config-if)# ip ospf message-digest-key 1 md5 MD5pa55
R3(config)# interface s0/0/1
R3(config-if)# ip ospf message-digest-key 1 md5 MD5pa55
Step 4: Verify configurations.
a. Verify the MD5 authentication configurations using the commands show ip ospf interface.
b. Verify end-to-end connectivity.

```

Insert screenshots here

R1:

```

R1>en
R1#ping 10.1.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/10/19 ms

R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#router ospf 1
R1(config-router)#network 192.168.1.0 0.0.0.255 area 0
R1(config-router)#network 10.1.1.0 0.0.0.3 area 0
R1(config-router)#area 0 authentication message-digest
R1(config-router)#exit
R1(config)#interface s0/1/0
R1(config-if)#ip ospf message-digest-key 1 md5 MD5pa55
R1(config-if)#exit

R1#show ip ospf interface

GigabitEthernet0/0 is up, line protocol is up
Internet address is 192.168.1.1/24, Area 0
Process ID 1, Router ID 192.168.1.1, Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State DR, Priority 1
Designated Router (ID) 192.168.1.1, Interface address 192.168.1.1
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:03
Index 1/1, 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 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)
Message digest authentication enabled
No key configured, using default key id 0
Serial0/1/0 is up, line protocol is up
Internet address is 10.1.1.1/30, Area 0
Process ID 1, Router ID 192.168.1.1, Network Type POINT-TO-POINT, Cost: 64
Transmit Delay is 1 sec, State POINT-TO-POINT,
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:02
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
Suppress hello for 0 neighbor(s)
Message digest authentication enabled
Youngest key id is 1

```

R2:

```
R2>
R2>en
R2#ping 10.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/15/23 ms

R2#ping 10.2.2.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.2.1, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/8/21 ms

R2(config)#router ospf 1
R2(config-router)#network 10.1.1.0 0.0.0.3 area 0
R2(config-router)#network 10.2.2.0 0.0.0.3 area 0
R2(config-router)#area 0 authentication message-digest
R2(config-router)#exit
R2(config)#interface s0/1/0
R2(config-if)#ip ospf message-digest-key 1 md5 MD5pa55
R2(config-if)#exit

R2(config)#interface s0/1/1
R2(config-if)#ip ospf message-digest-key 1 md5 MD5pa55
R2(config-if)#exit

R2#show ip ospf interface

Serial0/1/0 is up, line protocol is up
  Internet address is 10.1.1.2/30, Area 0
  Process ID 1, Router ID 10.2.2.2, Network Type POINT-TO-POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT-TO-POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:05
  Index 1/1, 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 192.168.1.1
  Suppress hello for 0 neighbor(s)
  Message digest authentication enabled
    Youngest key id is 1
Serial0/1/1 is up, line protocol is up
  Internet address is 10.2.2.2/30, Area 0
  Process ID 1, Router ID 10.2.2.2, Network Type POINT-TO-POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT-TO-POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:09
  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
  Suppress hello for 0 neighbor(s)
  Message digest authentication enabled
    Youngest key id is 1
```

R3:

```
R3>
R3>en
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#do ping 10.2.2.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.2.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/13/24 ms
```

```
R3(config)#router ospf 1
R3(config-router)#network 192.168.3.0 0.0.0.255 area 0
R3(config-router)#network 10.2.2.0 0.0.0.3 area 0
R3(config-router)#exit
R3(config)#interface s0/1/0
R3(config-if)#exit
R3(config)#router ospf 1
R3(config-router)#area 0 authentication message-digest
R3(config-router)#exit
R3(config)#interface s0/1/0
R3(config-if)#ip ospf message-digest-key 1 md5 MD5pa55
R3(config-if)#exit
```

```
R3#show ip ospf interface
```

```
GigabitEthernet0/0 is up, line protocol is up
  Internet address is 192.168.3.1/24, Area 0
  Process ID 1, Router ID 192.168.3.1, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 192.168.3.1, Interface address 192.168.3.1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:04
  Index 1/1, 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 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
  Message digest authentication enabled
    No key configured, using default key id 0
Serial0/1/0 is up, line protocol is up
  Internet address is 10.2.2.1/30, Area 0
  Process ID 1, Router ID 192.168.3.1, Network Type POINT-TO-POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT-TO-POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:02
  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 10.2.2.2
  Suppress hello for 0 neighbor(s)
  Message digest authentication enabled
    Youngest key id is 1
```

Part 2: Configure NTP

Step 1: Enable NTP authentication on PC-A.

a. On PC-A, click NTP under the Services tab to verify NTP service is enabled.

b. To configure NTP authentication, click Enable under Authentication. Use key 1 and password NTPpa55 for authentication

Step 2: Configure R1, R2, and R3 as NTP clients.

```
R1(config)# ntp server 192.168.1.5
```

```
R2(config)# ntp server 192.168.1.5
```

```
R3(config)# ntp server 192.168.1.5
```

Verify client configuration using the command show ntp status.

Step 3: Configure routers to update hardware clock.

Configure R1, R2, and R3 to periodically update the hardware clock with the time learned from NTP.

```
R1(config)# ntp update-calendar
```

```
R2(config)# ntp update-calendar
```

```
R3(config)# ntp update-calendar
```

Exit global configuration and verify that the hardware clock was updated using the command show clock.

Step 4: Configure NTP authentication on the routers.

Configure NTP authentication on R1, R2, and R3 using key 1 and password NTPpa55.

```
R1(config)# ntp authenticate
```

```
R1(config)# ntp trusted-key 1
```

```
R1(config)# ntp authentication-key 1 md5 NTPpa55
```

```
R2(config)# ntp authenticate
```

```
R2(config)# ntp trusted-key 1
```

```
R2(config)# ntp authentication-key 1 md5 NTPpa55
```

```
R3(config)# ntp authenticate
```

```
R3(config)# ntp trusted-key 1
```

```
R3(config)# ntp authentication-key 1 md5 NTPpa55
```

Step 5: Configure routers to timestamp log messages.

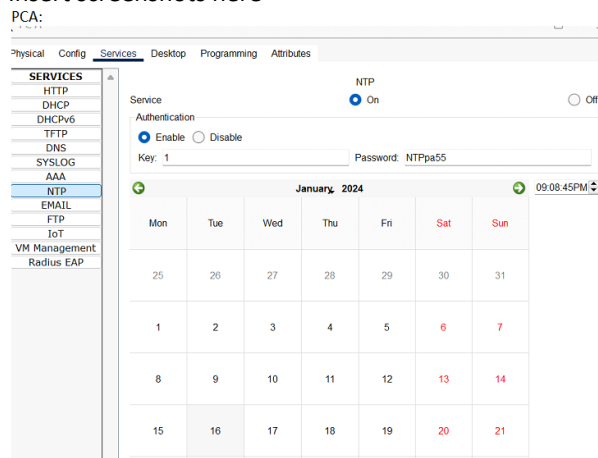
Configure timestamp service for logging on the routers.

```
R1(config)# service timestamps log datetime msec
```

```
R2(config)# service timestamps log datetime msec
```

```
R3(config)# service timestamps log datetime msec
```

Insert screenshots here



R1:

```
R1>en
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ntp server 192.168.1.5
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#show ntp status
Clock is unsynchronized, stratum 16, no reference clock
nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision is 2**24
reference time is 00000000.00000000 (00:00:00.000 UTC Mon Jan 1 1990)
clock offset is 0.00 msec, root delay is 0.00 msec
root dispersion is 0.00 msec, peer dispersion is 0.00 msec.
loopfilter state is 'FSET' (Drift set from file), drift is - 0.000001193 s/s system poll
interval is 4, never updated.
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ntp update-calendar
R1(config)#ntp authenticate
R1(config)#ntp trusted-key 1
R1(config)#ntp authentication-key 1 md5 NTPpa55
R1(config)#service timestamps log datetime msec
R1(config)#exit
R1#
*Jan 16, 21:07:35.077: SYS-5-CONFIG_I: Configured from console by console
R1#show clock
21:7:43.114 UTC Tue Jan 16 2024
R1#
```

R3:

```
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ntp server 192.168.1.5
R2(config)#exit
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#show ntp status
Clock is unsynchronized, stratum 16, no reference clock
nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision is 2**24
reference time is 00000000.00000000 (00:00:00.000 UTC Mon Jan 1 1990)
clock offset is 0.00 msec, root delay is 0.00 msec
root dispersion is 0.00 msec, peer dispersion is 0.00 msec.
loopfilter state is 'FSET' (Drift set from file), drift is - 0.000001193 s/s sys
interval is 4, never updated.
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ntp update-calendar
R2(config)#ntp authenticate
R2(config)#ntp trusted-key 1
R2(config)#ntp authentication-key 1 md5 NTPpa55
R2(config)#service timestamps log datetime msec
R2(config)#exit
R2>
R2>en
R2#show clock
21:42:0.271 UTC Tue Jan 16 2024
R2#
```

R3:

```
R3>
R3>en
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#ntp server 192.168.1.5
R3(config)#ntp update-calendar
R3(config)#ntp authenticate
R3(config)#ntp trusted-key 1
R3(config)#ntp authentication-key 1 md5 NTPpa55
R3(config)#service timestamps log datetime msec
R3(config)#exit

R3(config)#exit
R3#
*Jan 16, 21:40:40.4040: SYS-5-CONFIG_I: Configured from console by console
R3#show clock
21:41:1.265 UTC Tue Jan 16 2024
R3#
```

Part 3: Configure Routers to Log Messages to the Syslog Server

Step 1: Configure the routers to identify the remote host (Syslog Server) that will receive logging messages.

```
R1(config)# logging host 192.168.1.6
```

```
R2(config)# logging host 192.168.1.6
```

```
R3(config)# logging host 192.168.1.6
```

The router console will display a message that logging has started.

Step 2: Verify logging configuration.

Use the command show logging to verify logging has been enabled.

Step 3: Examine logs of the Syslog Server.

From the Services tab of the Syslog Server's dialogue box, select the Syslog services button. Observe the logging messages received from the routers.

Insert screenshots here

R1:

```
R1#conf t
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
R1(config)#logging host 192.168.1.6
```

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

```
R1#
```

```
*Jan 16, 21:26:55.2626: SYS-5-CONFIG_I: Configured from console by console
```

```
*Jan 16, 21:26:55.2626: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 192.168.1.6 port 514  
started - CLI initiatedshow logging
```

```
Syslog logging: enabled (0 messages dropped, 0 messages rate-limited,  
0 flushes, 0 overruns, xml disabled, filtering disabled)
```

```
No Active Message Discriminator.
```

```
No Inactive Message Discriminator.
```

```
Console logging: level debugging, 18 messages logged, xml disabled,  
filtering disabled
```

```
Monitor logging: level debugging, 18 messages logged, xml disabled,  
filtering disabled
```

```
Buffer logging: disabled, xml disabled,  
filtering disabled
```

```
Logging Exception size (4096 bytes)  
Count and timestamp logging messages: disabled  
Persistent logging: disabled
```

```
No active filter modules.
```

```
ESM: 0 messages dropped
```

```
Trap logging: level informational, 18 message lines logged  
Logging to 192.168.1.6 (udp port 514, audit disabled,
```

R2:

```
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#logging host 192.168.1.6
R2(config)#
R2(config)#exit
R2#
*Jan 16, 21:28:13.2828: SYS-5-CONFIG_I: Configured from console by console
*Jan 16, 21:28:13.2828: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 192.168.1.6 port 514
started - CLI initiated
R2#show logging
Syslog logging: enabled (0 messages dropped, 0 messages rate-limited,
                  0 flushes, 0 overruns, xml disabled, filtering disabled)
```

No Active Message Discriminator.

No Inactive Message Discriminator.

```
Console logging: level debugging, 22 messages logged, xml disabled,
                  filtering disabled
Monitor logging: level debugging, 22 messages logged, xml disabled,
                  filtering disabled
Buffer logging: disabled, xml disabled,
                  filtering disabled
```

```
Logging Exception size (4096 bytes)
Count and timestamp logging messages: disabled
Persistent logging: disabled
```

No active filter modules.

```
ESM: 0 messages dropped
Trap logging: level informational, 22 message lines logged
Logging to 192.168.1.6 (udp port 514, audit disabled,
authentication disabled, encryption disabled, link up),
2 message lines logged,
0 message lines rate-limited,
0 message lines dropped-by-MD,
xml disabled, sequence number disabled
filtering disabled
```

R3:

```
R3#
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#logging host 192.168.1.6
R3(config)#exit
R3#
*Jan 16, 21:28:58.2828: SYS-5-CONFIG_I: Configured from console by console
*Jan 16, 21:28:58.2828: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 192.168.1.6 port
started - CLI initiated
R3#show logging
Syslog logging: enabled (0 messages dropped, 0 messages rate-limited,
                  0 flushes, 0 overruns, xml disabled, filtering disabled)
```

No Active Message Discriminator.

No Inactive Message Discriminator.

```
Console logging: level debugging, 16 messages logged, xml disabled,
                  filtering disabled
Monitor logging: level debugging, 16 messages logged, xml disabled,
                  filtering disabled
Buffer logging: disabled, xml disabled,
                  filtering disabled
```

```
Logging Exception size (4096 bytes)
Count and timestamp logging messages: disabled
Persistent logging: disabled
```

No active filter modules.

```
ESM: 0 messages dropped
Trap logging: level informational, 16 message lines logged
Logging to 192.168.1.6 (udp port 514, audit disabled,
authentication disabled, encryption disabled, link up),
2 message lines logged,
0 message lines rate-limited,
0 message lines dropped-by-MD,
xml disabled, sequence number disabled
filtering disabled
```


Part 4: Configure R3 to Support SSH Connections

Step 1: Configure a domain name.

Configure a domain name of ccnasecurity.com on R3.

```
R3(config)# ip domain-name ccnasecurity.com
```

Step 2: Configure users for login to the SSH server on R3.

Create a user ID of SSHadmin with the highest possible privilege level and a secret password of ciscosshpa55.

```
R3(config)# username SSHadmin privilege 15 secret ciscosshpa55
```

Step 3: Configure the incoming vty lines on R3.

Use the local user accounts for mandatory login and validation. Accept only SSH connections.

```
R3(config)# line vty 0 4
```

```
R3(config-line)# login local
```

```
R3(config-line)# transport input ssh
```

Step 4 Erase existing key pairs on R3.

Any existing RSA key pairs should be erased on the router.

```
R3(config)# crypto key zeroize rsa
```

Note: If no keys exist, you might receive this message: % No Signature RSA Keys found in configuration.

Step 5: Generate the RSA encryption key pair for R3.

The router uses the RSA key pair for authentication and encryption of transmitted SSH data. Configure the RSA keys with a modulus of 1024. The default is 512, and the range is from 360 to 2048.

```
R3(config)# crypto key generate rsa
```

The name for the keys will be: R3.ccnasecurity.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.

How many bits in the modulus [512]: 1024

% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

Note: The command to generate RSA encryption key pairs for R3 in Packet Tracer differs from those used in the lab.

Step 6: Verify the SSH configuration.

Use the show ip ssh command to see the current settings. Verify that the authentication timeout and retries are at their default values of 120 and 3.

Step 7: Configure SSH timeouts and authentication parameters.

The default SSH timeouts and authentication parameters can be altered to be more restrictive. Set the timeout to 90 seconds, the number of authentication retries to 2, and the version to 2.

```
R3(config)# ip ssh time-out 90
```

```
R3(config)# ip ssh authentication-retries 2
```

```
R3(config)# ip ssh version 2
```

Issue the show ip ssh command again to confirm that the values have been changed.

Step 8: Attempt to connect to R3 via Telnet from PC-C.

Open the Desktop of PC-C. Select the Command Prompt icon. From PC-C, enter the command to connect to R3 via Telnet.

```
PC> telnet 192.168.3.1
```

This connection should fail because R3 has been configured to accept only SSH connections on the virtual terminal lines.

Step 9: Connect to R3 using SSH on PC-C.

Open the Desktop of PC-C. Select the Command Prompt icon. From PC-C, enter the command to connect to R3 via SSH. When prompted for the password, enter the password configured for the administrator ciscosshpa55.

```
PC> ssh -l SSHadmin 192.168.3.1
```

Step 10: Connect to R3 using SSH on R2.

To troubleshoot and maintain R3, the administrator at the ISP must use SSH to access the router CLI. From the CLI of R2, enter the command to connect to R3 via SSH version 2 using the SSHadmin user account. When prompted for the password, enter the password configured for the administrator: ciscosshpa55.
R2# ssh -v 2 -l SSHadmin 10.2.2.1

Insert screenshots here

R3:

```
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#ip domain-name arati.com
R3(config)#username SSHadmin privilege 15 secret sshpa55
^
% Invalid input detected at '^' marker.

R3(config)#username SSHadmin privilege 15 secret sshpa55
R3(config)#line vty 0 4
R3(config-line)#login local
R3(config-line)#transport input ssh
R3(config-line)#crypto key zeroize rsa
^
% Invalid input detected at '^' marker.

R3(config-line)#crypto key zeroize rsa
% No Signature RSA Keys found in configuration.

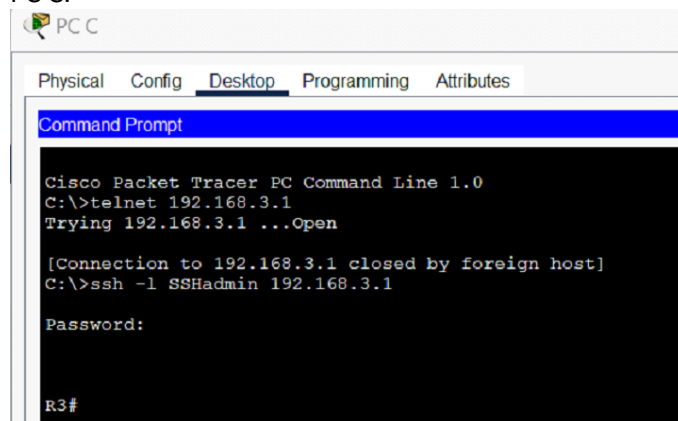
R3(config)#crypto key generate rsa
The name for the keys will be: R3.arati.com
Choose the size of the key modulus in the range of 360 to 4096 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

R3(config)#show ip ssh
*Jan 16 21:46:19.445: %SSH-5-ENABLED: SSH 1.99 has been enabled
^
% Invalid input detected at '^' marker.

R3(config)#ip ssh time-out 90
R3(config)#ip ssh authentication-retries 2
R3(config)#ip ssh version 2
R3(config)#exit
R3#
*Jan 16, 21:48:13.4848: SYS-5-CONFIG_I: Configured from console by console
R3#show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 90 secs; Authentication retries: 2
R3#
```

PC C:



R2:

```
R2#ssh -l SSHadmin 10.2.2.1
```

Password:

R3#