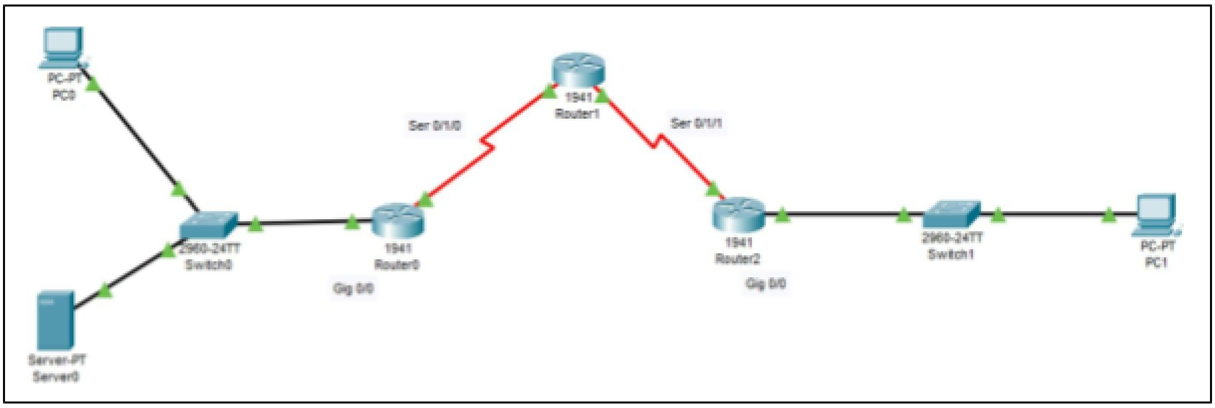
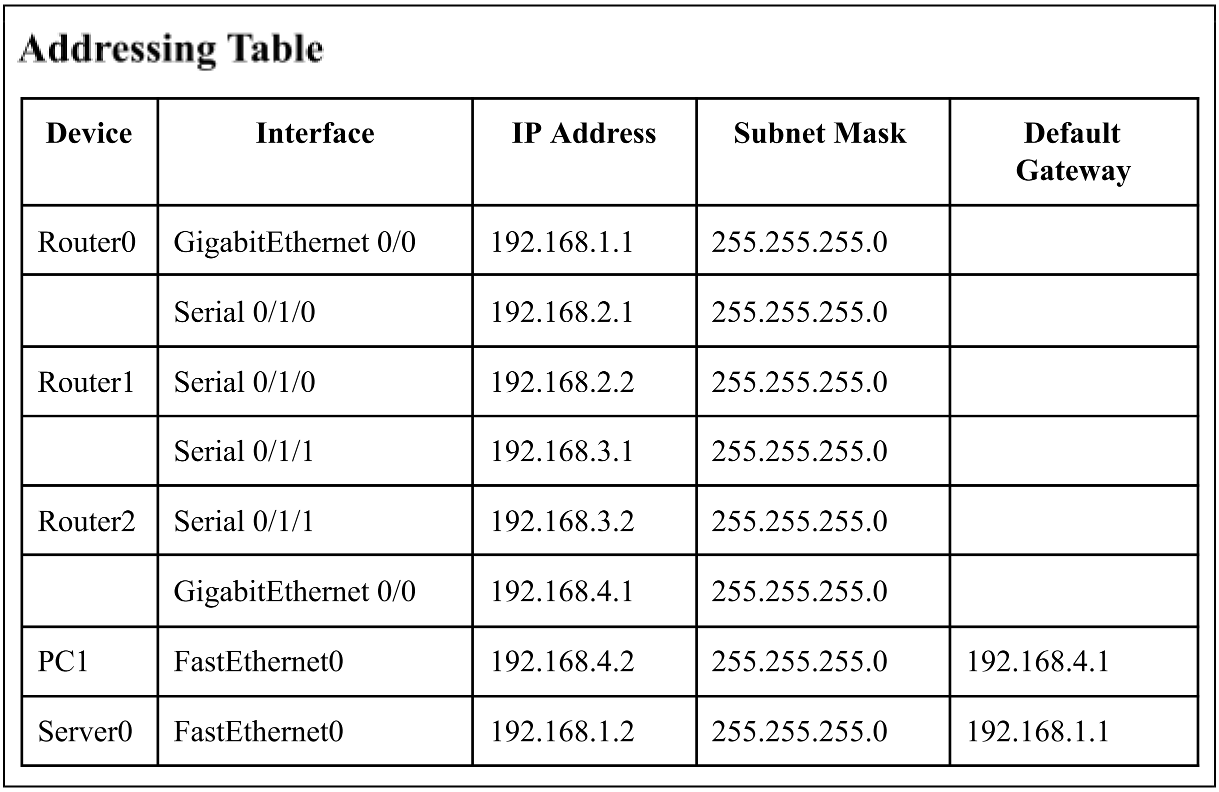
Name :Harsh Kadu Roll No : 33

Practical 6

Configure IOS Intrusion Prevention System (IPS) using CLI

Topology:





Addressing Table

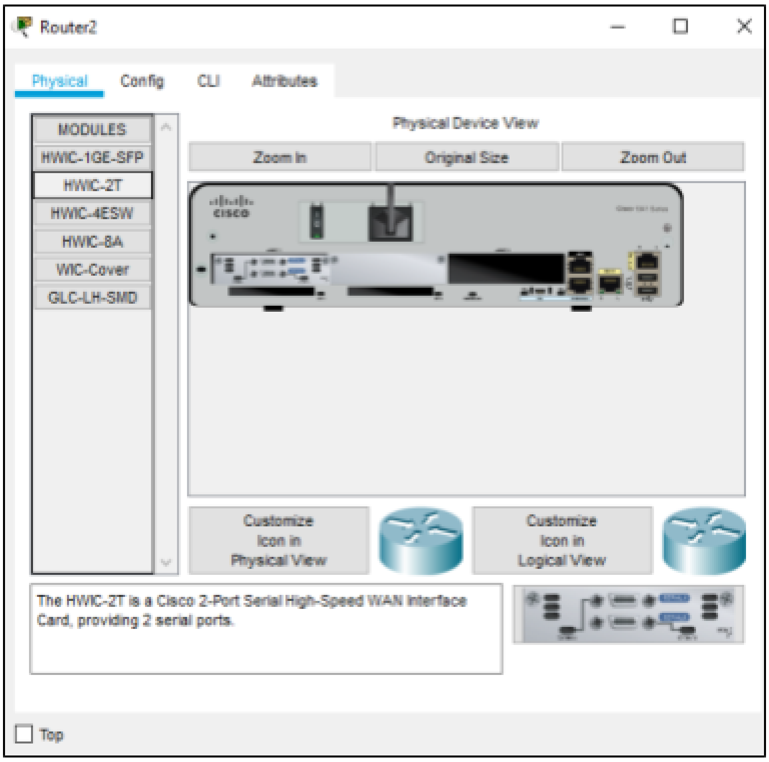
Device	Interface	IP Address	Subnet Mask	Default Gateway
Router0	GigabitEthernet 0/0	192.168.1.1	255.255.255.0	
	Serial 0/1/0	192.168.2.1	255.255.255.0	
Router1	Serial 0/1/0	192.168.2.2	255.255.255.0	
	Serial 0/1/1	192.168.3.1	255.255.255.0	
Router2	Serial 0/1/1	192.168.3.2	255.255.255.0	
	GigabitEthernet 0/0	192.168.4.1	255.255.255.0	
PC1	FastEthernet0	192.168.4.2	255.255.255.0	192.168.4.1
Server0	FastEthernet0	192.168.1.2	255.255.255.0	192.168.1.1

Procedure:

Step 1: Add Serial Interface to each Router before connecting component:

i) Click on Router2 ➜ Physical Tab ➜ Switch off the switch first ➜ Select H2WIC-2T ➜ Drag it and place it on Interface ➜ Make Switch On. Repeat

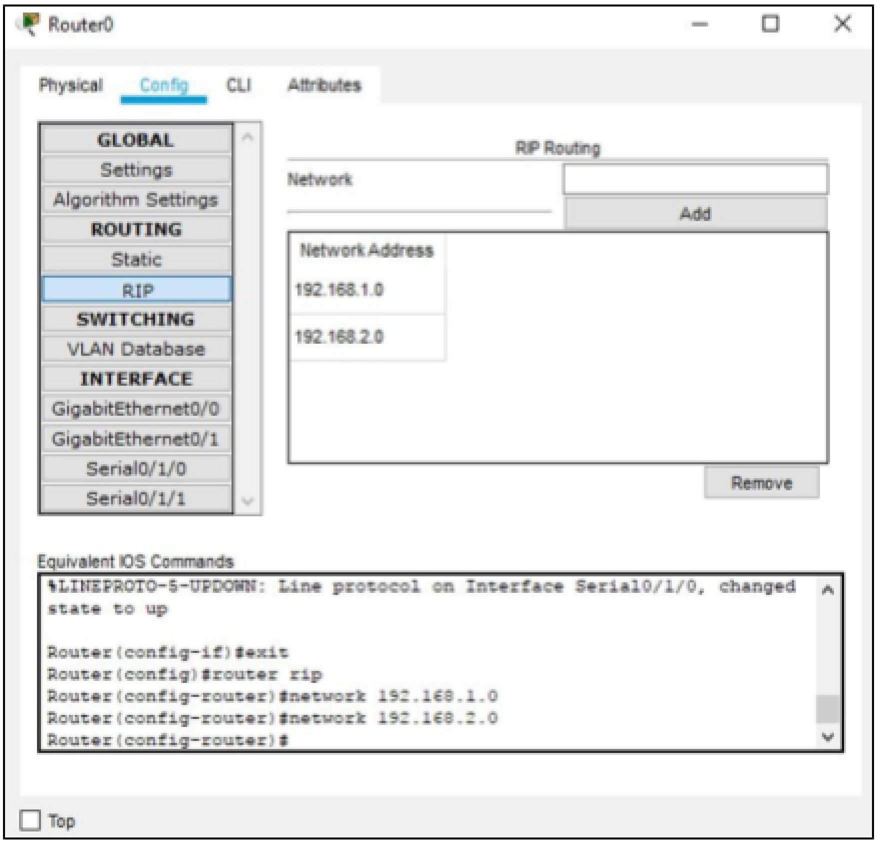
the same procedure on Router0 and Router1.



The HWIC-2T is a Cisco 2-Port Serial High-Speed WAN Interface Card, providing 2 serial ports.

Step 2: Set Routing Path using RIP:

i) Click on Router0 ➜ Click on Config Tab ➜ Click on RIP ➜ Add the Network Addresses ➜ Click on Add.

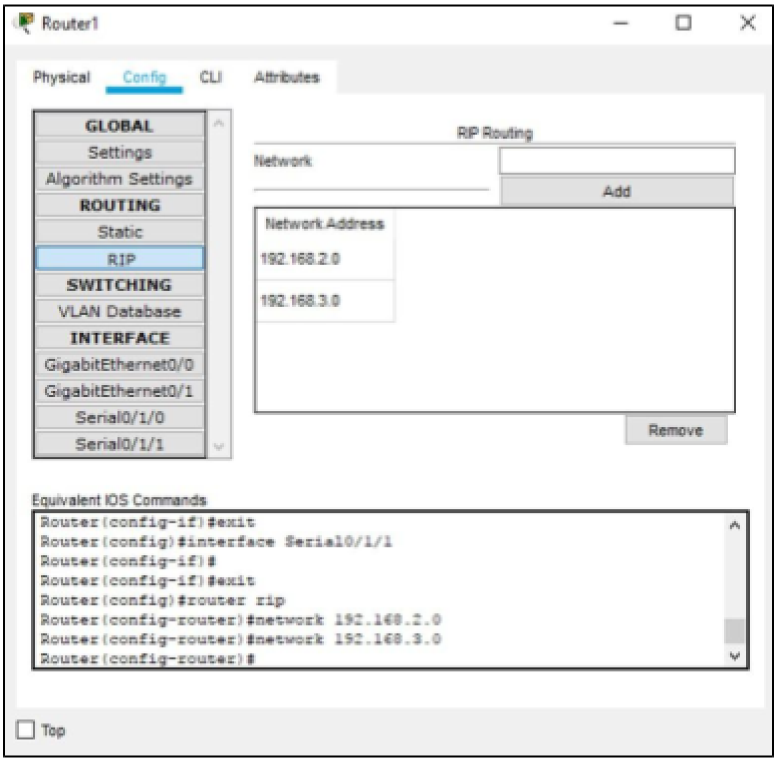


Network Address
192.168.1.0
192.168.2.0

Equivalent IOS Commands

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed
state to up

Router(config-if)#exit
Router(config)#router rip
Router(config-router)#network 192.168.1.0
Router(config-router)#network 192.168.2.0
Router(config-router)#
```

ii) Click on Router1 ➜ Click on Config Tab ➜ Click on RIP ➜ Add the Network Addresses ➜ Click on Add.

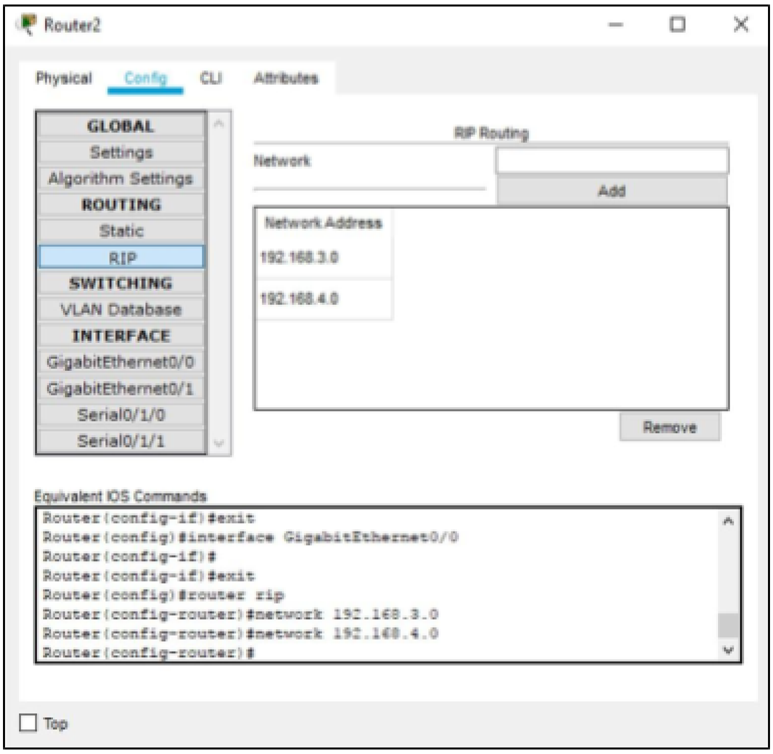


Network Address
192.168.2.0
192.168.3.0

Equivalent IOS Commands

```
Router(config-if)#exit
Router(config)#interface Serial0/1/1
Router(config-if)#
Router(config-if)#exit
Router(config)#router rip
Router(config-router)#network 192.168.2.0
Router(config-router)#network 192.168.3.0
Router(config-router)#
```

iii) Click on Router2 ➜ Click on Config Tab ➜ Click on RIP ➜ Add the Network Addresses ➜ Click on Add.



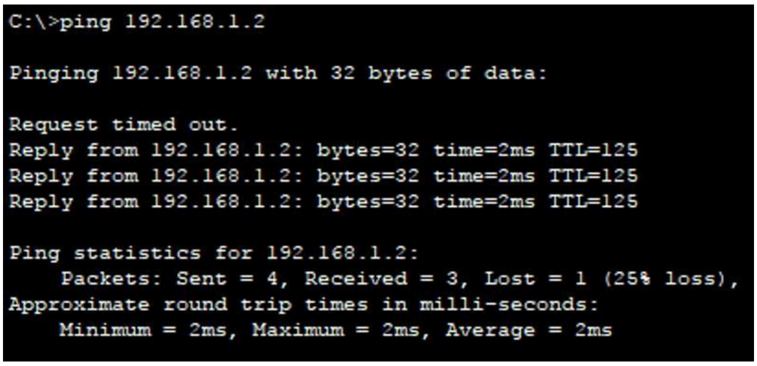
Network Address
192.168.3.0
192.168.4.0

Equivalent IOS Commands

```
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#router rip
Router(config-router)#network 192.168.3.0
Router(config-router)#network 192.168.4.0
Router(config-router)#
```

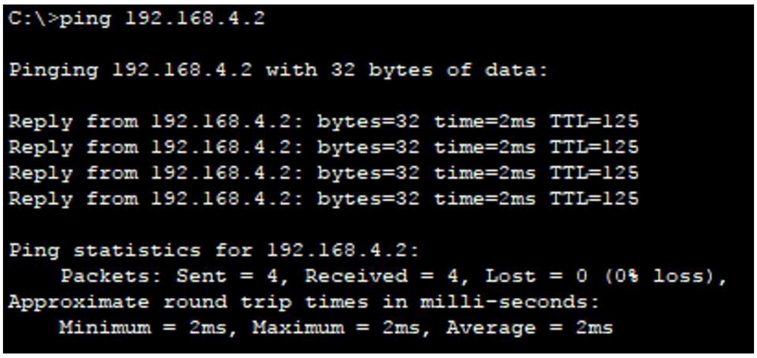
Step 3: Check Connectivity:

i) Click on PC1 ➜ Desktop ➜ Command Prompt ➜ Type the following Command:



```
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
```

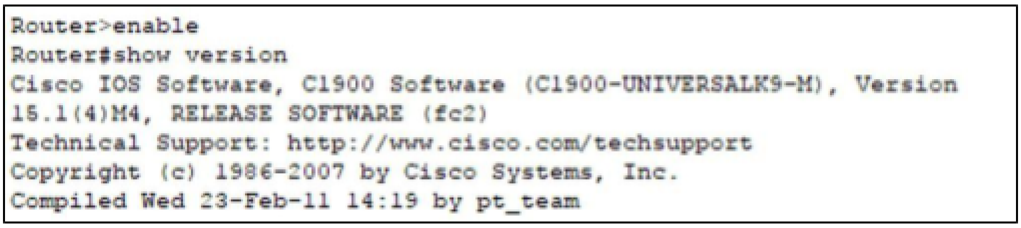
ii) Click on PC0 ➜ Desktop ➜ Command Prompt ➜ Type the following Command:



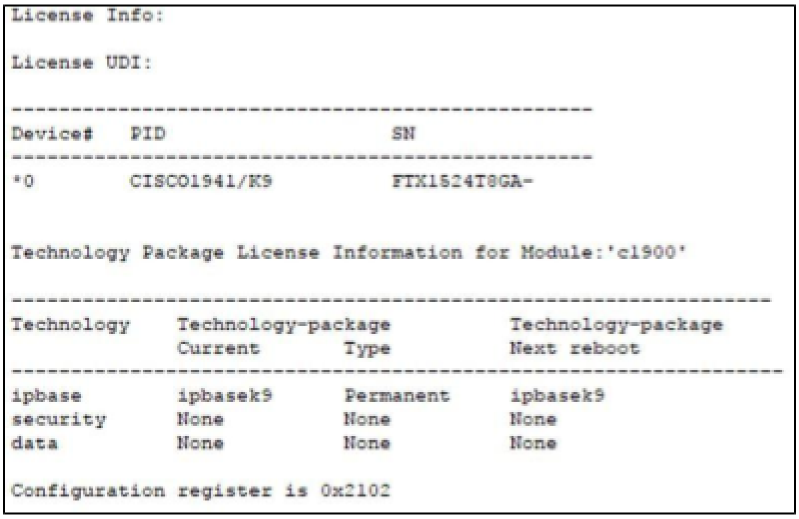
```
C:\>ping 192.168.4.2

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=2ms 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 = 2ms, Average = 2ms
```

Step 4: Enable the IOS IPS on Router1:

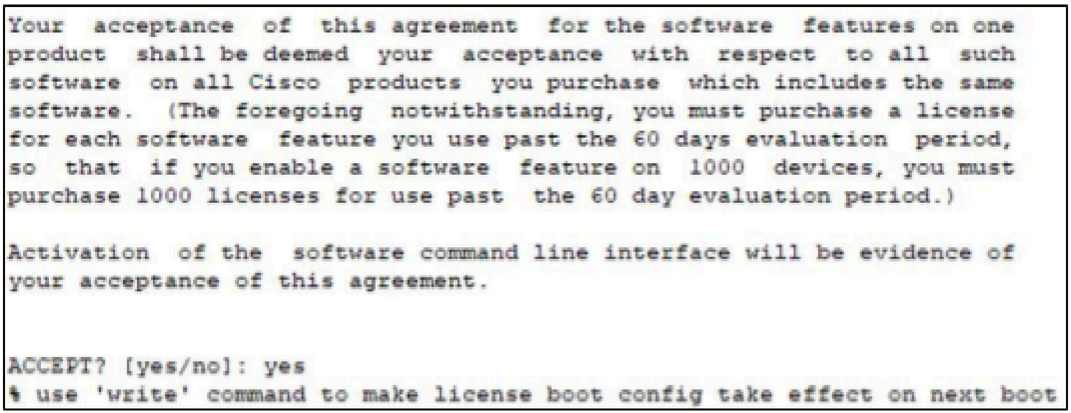
i) Click on Router1 ➜ CLI Tab ➜ Type following command:



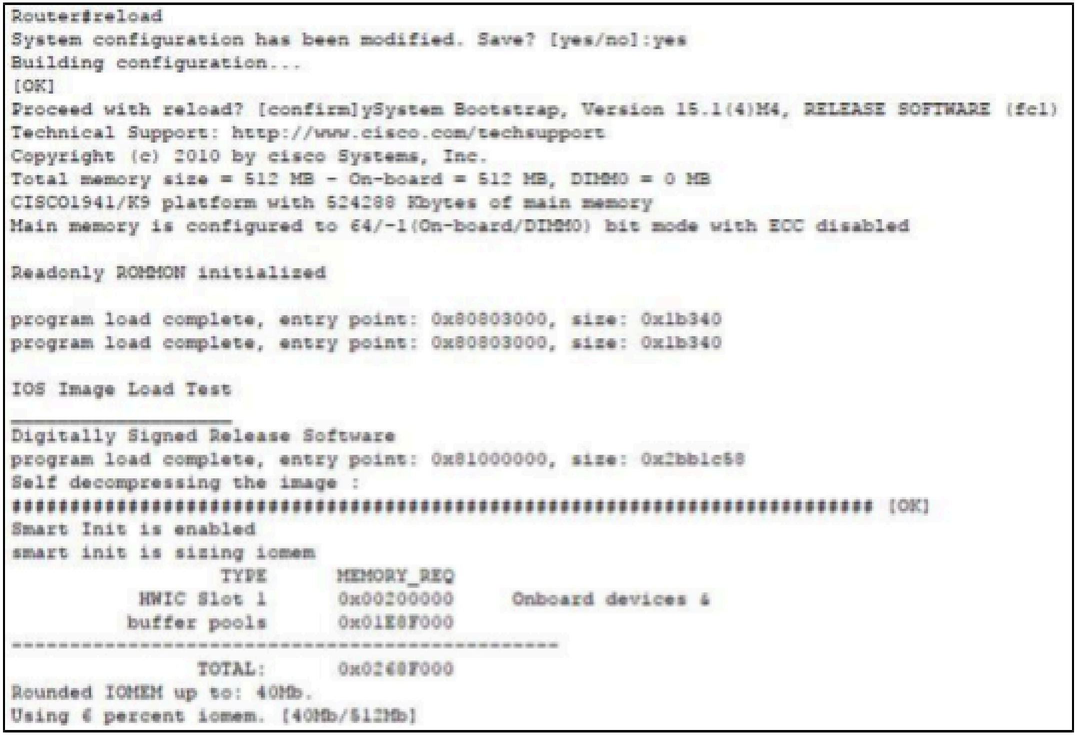
```
Router>enable
Router#show version
Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version
15.1(4)M4, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 23-Feb-11 14:19 by pt_team
```



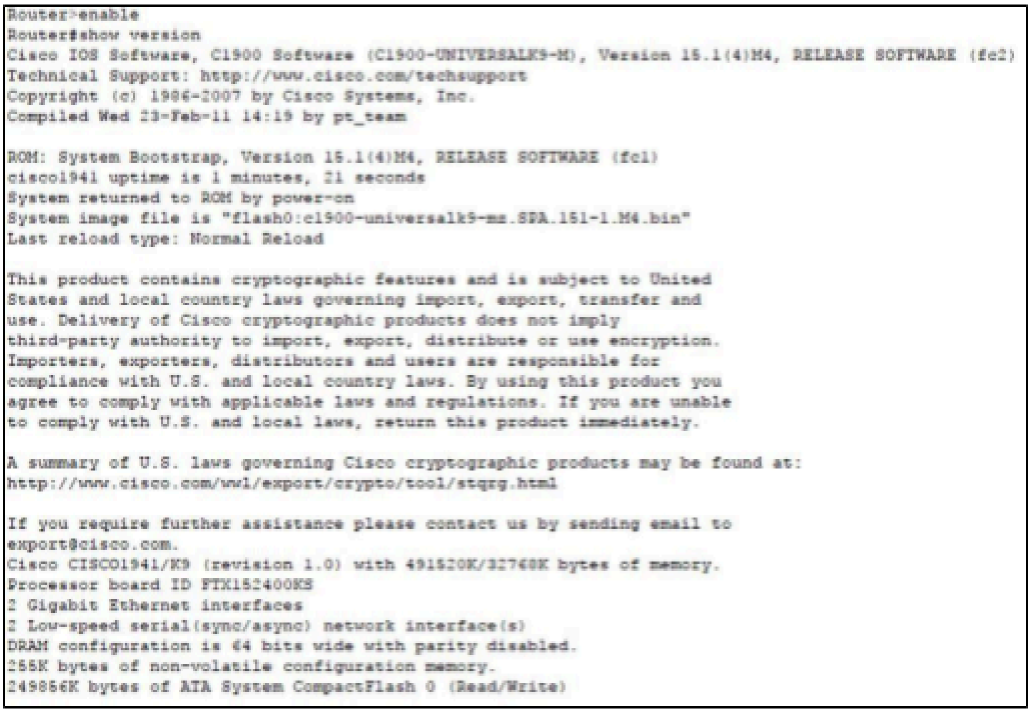
```
License Info:

License UDI:

-------------------------------------------------
Device#   PID                      SN
-------------------------------------------------
*0        CISCO1941/K9             FTX1524T8GA-


Technology Package License Information for Module:'c1900'

-----------------------------------------------------------------
Technology    Technology-package           Technology-package
              Current       Type           Next reboot
------------------------------------------------------------------
ipbase        ipbasek9      Permanent      ipbasek9
security      None          None           None
data          None          None           None

Configuration register is 0x2102
```



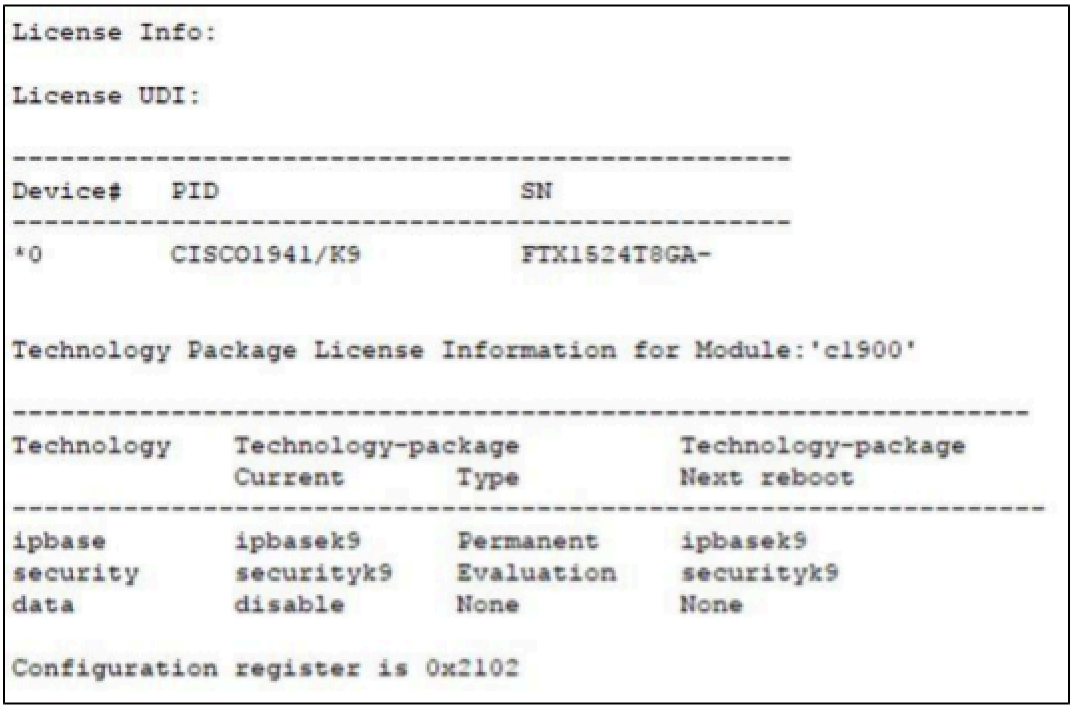
```
Your  acceptance  of  this agreement  for the software  features on one
product  shall be deemed  your  acceptance  with  respect  to all  such
software  on all Cisco  products  you purchase  which includes the same
software.  (The foregoing  notwithstanding, you must purchase a license
for each software  feature you use past the 60 days evaluation  period,
so  that  if you enable a software  feature on  1000  devices, you must
purchase 1000 licenses for use past  the 60 day evaluation period.)

Activation  of the  software command line interface will be evidence of
your acceptance of this agreement.


ACCEPT? [yes/no]: yes
% use 'write' command to make license boot config take effect on next boot
```



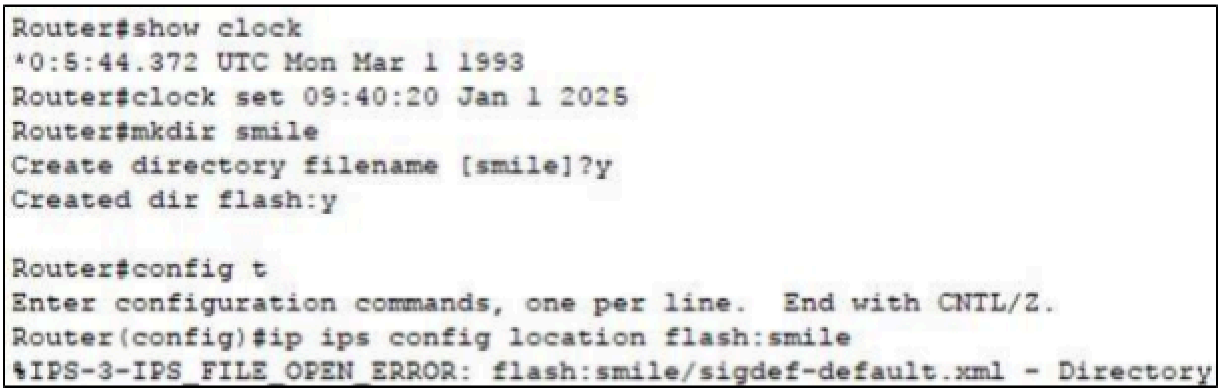
```
Router#reload
System configuration has been modified. Save? [yes/no]:yes
Building configuration...
[OK]
Proceed with reload? [confirm]ySystem Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2010 by cisco Systems, Inc.
Total memory size = 512 MB - On-board = 512 MB, DIMM0 = 0 MB
CISCO1941/K9 platform with 524288 Kbytes of main memory
Main memory is configured to 64/-1(On-board/DIMM0) bit mode with ECC disabled

Readonly ROMMON initialized

program load complete, entry point: 0x80803000, size: 0x1b340
program load complete, entry point: 0x80803000, size: 0x1b340

IOS Image Load Test
___________________
Digitally Signed Release Software
program load complete, entry point: 0x81000000, size: 0x2bb1c58
Self decompressing the image :
########################################################################## [OK]
Smart Init is enabled
smart init is sizing iomem
                TYPE      MEMORY_REQ
           HWIC Slot 1      0x00200000     Onboard devices &
          buffer pools      0x01E8F000
-----------------------------------------------
              TOTAL:        0x0268F000
Rounded IOMEM up to: 40Mb.
Using 6 percent iomem. [40Mb/512Mb]
```



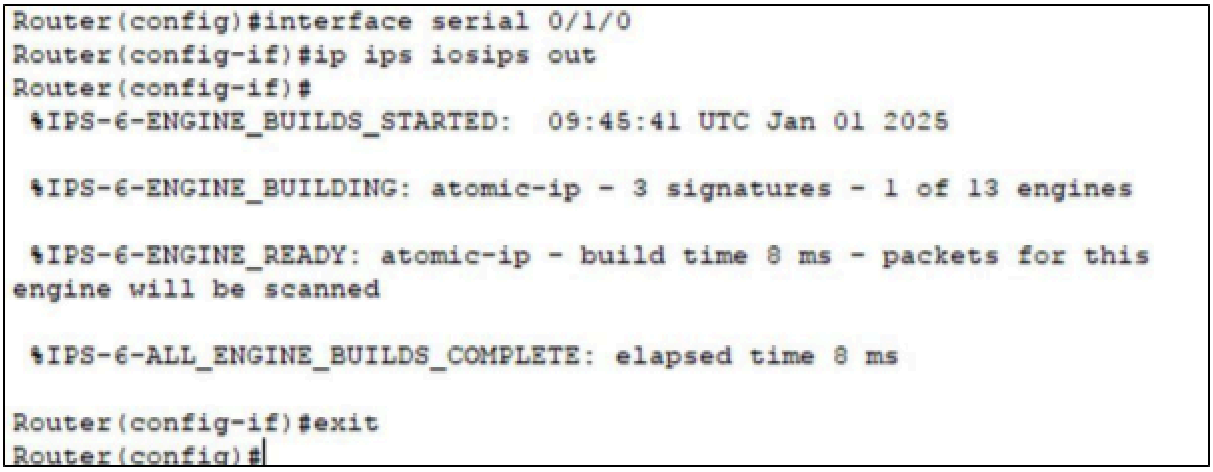
```
Router>enable
Router#show version
Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version 15.1(4)M4, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 23-Feb-11 14:19 by pt_team

ROM: System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
cisco1941 uptime is 1 minutes, 21 seconds
System returned to ROM by power-on
System image file is "flash0:c1900-universalk9-mz.SPA.151-1.M4.bin"
Last reload type: Normal Reload

This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.
Cisco CISCO1941/K9 (revision 1.0) with 491520K/32768K bytes of memory.
Processor board ID FTX152400KS
2 Gigabit Ethernet interfaces
2 Low-speed serial(sync/async) network interface(s)
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)
```



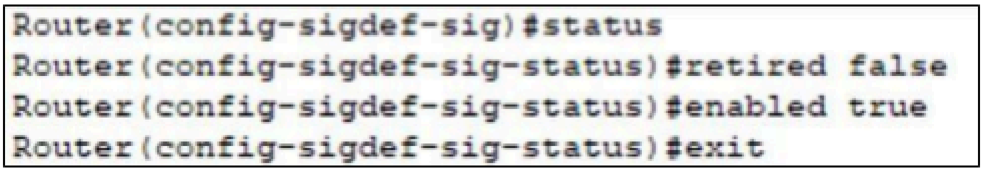
```
License Info:

License UDI:

-------------------------------------------------
Device#   PID                    SN
-------------------------------------------------
*0        CISCO1941/K9           FTX1524T8GA-


Technology Package License Information for Module:'c1900'

-----------------------------------------------------------------
Technology    Technology-package           Technology-package
              Current       Type           Next reboot
------------------------------------------------------------------
ipbase        ipbasek9      Permanent      ipbasek9
security      securityk9    Evaluation     securityk9
data          disable       None           None

Configuration register is 0x2102
```



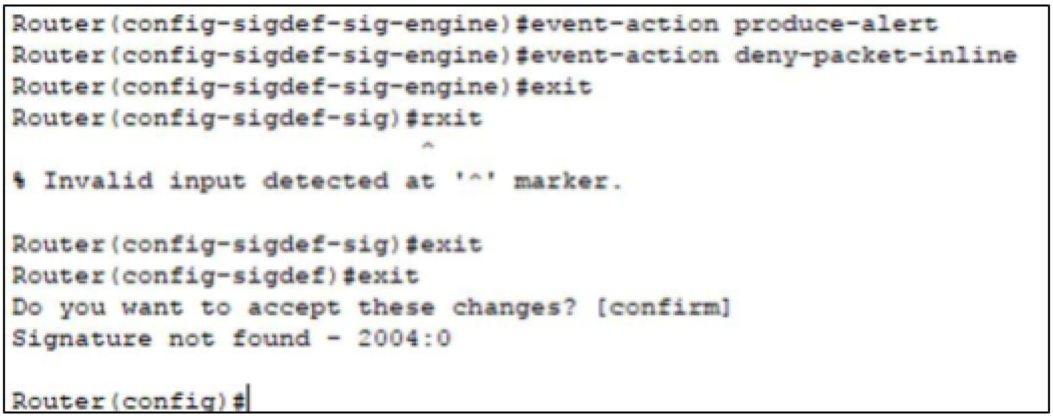
```
Router#show clock
*0:5:44.372 UTC Mon Mar 1 1993
Router#clock set 09:40:20 Jan 1 2025
Router#mkdir smile
Create directory filename [smile]?y
Created dir flash:y

Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip ips config location flash:smile
%IPS-3-IPS_FILE_OPEN_ERROR: flash:smile/sigdef-default.xml - Directory
```



```
Router(config)#interface serial 0/1/0
Router(config-if)#ip ips iosips out
Router(config-if)#
 %IPS-6-ENGINE_BUILDS_STARTED:  09:45:41 UTC Jan 01 2025

 %IPS-6-ENGINE_BUILDING: atomic-ip - 3 signatures - 1 of 13 engines

 %IPS-6-ENGINE_READY: atomic-ip - build time 8 ms - packets for this
engine will be scanned

 %IPS-6-ALL_ENGINE_BUILDS_COMPLETE: elapsed time 8 ms

Router(config-if)#exit
Router(config)#
```



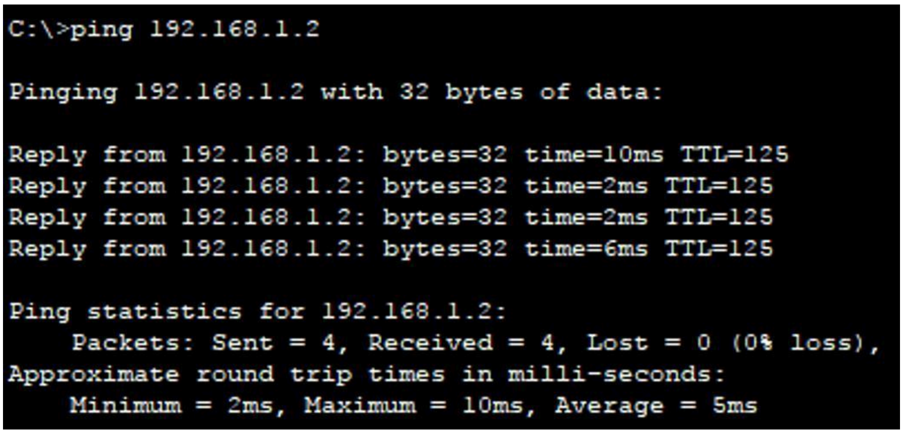
```
Router(config-sigdef-sig)#status
Router(config-sigdef-sig-status)#retired false
Router(config-sigdef-sig-status)#enabled true
Router(config-sigdef-sig-status)#exit
```



```
Router(config-sigdef-sig-engine)#event-action produce-alert
Router(config-sigdef-sig-engine)#event-action deny-packet-inline
Router(config-sigdef-sig-engine)#exit
Router(config-sigdef-sig)#rxit
                          ^
% Invalid input detected at '^' marker.

Router(config-sigdef-sig)#exit
Router(config-sigdef)#exit
Do you want to accept these changes? [confirm]
Signature not found - 2004:0

Router(config)#
```

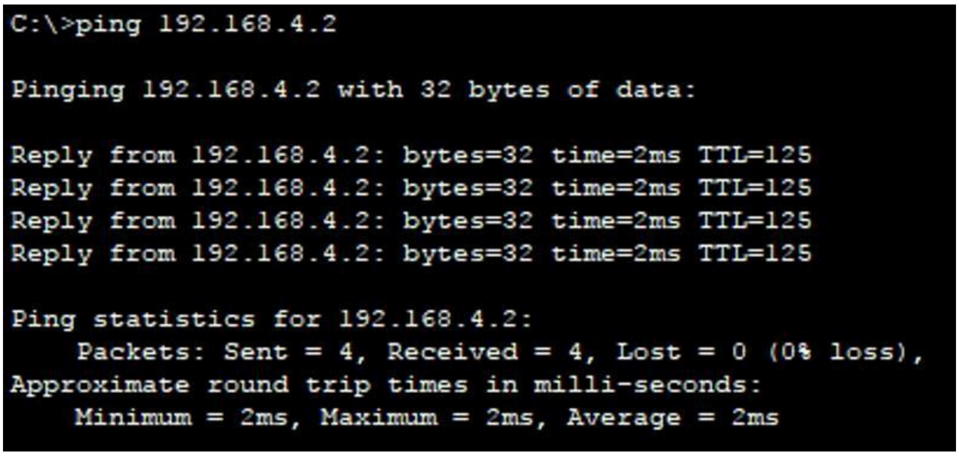
Step 5: Verify the IPS Configuration:

i) Pinging PC1 to Server ➜ Go to PC0 ➜ Desktop ➜ Command Prompt ➜ Type the following command:



```
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=10ms 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
Reply from 192.168.1.2: bytes=32 time=6ms TTL=125

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 10ms, Average = 5ms
```

ii) Pinging Server to PC1 ➜ Go to Server ➜ Desktop ➜ Command Prompt ➜ Type the following command:

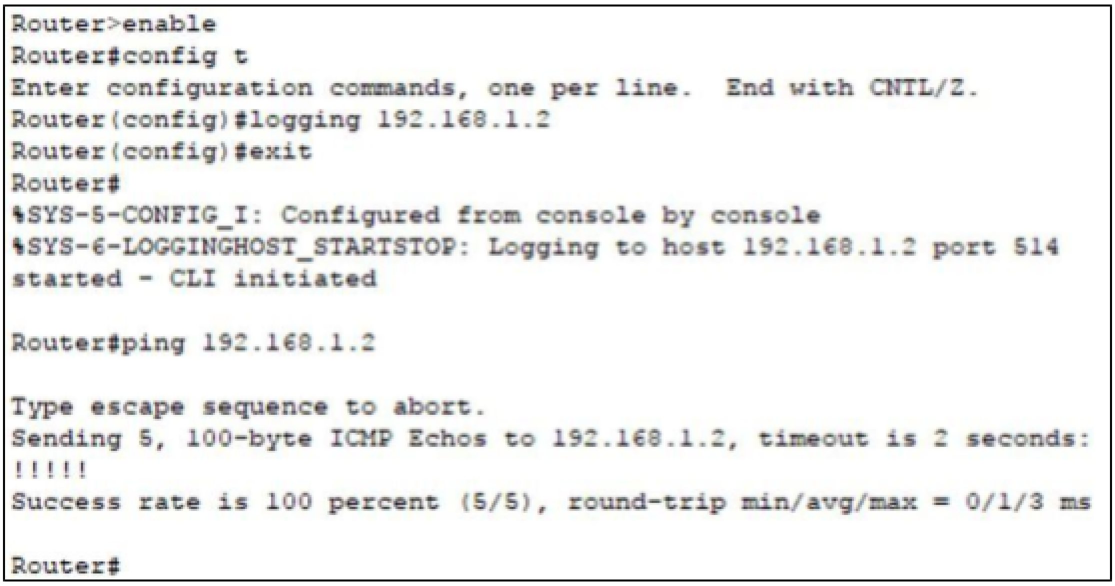


```
C:\>ping 192.168.4.2

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=2ms 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 = 2ms, Average = 2ms
```

Name :Harsh Kadu Roll No : 33

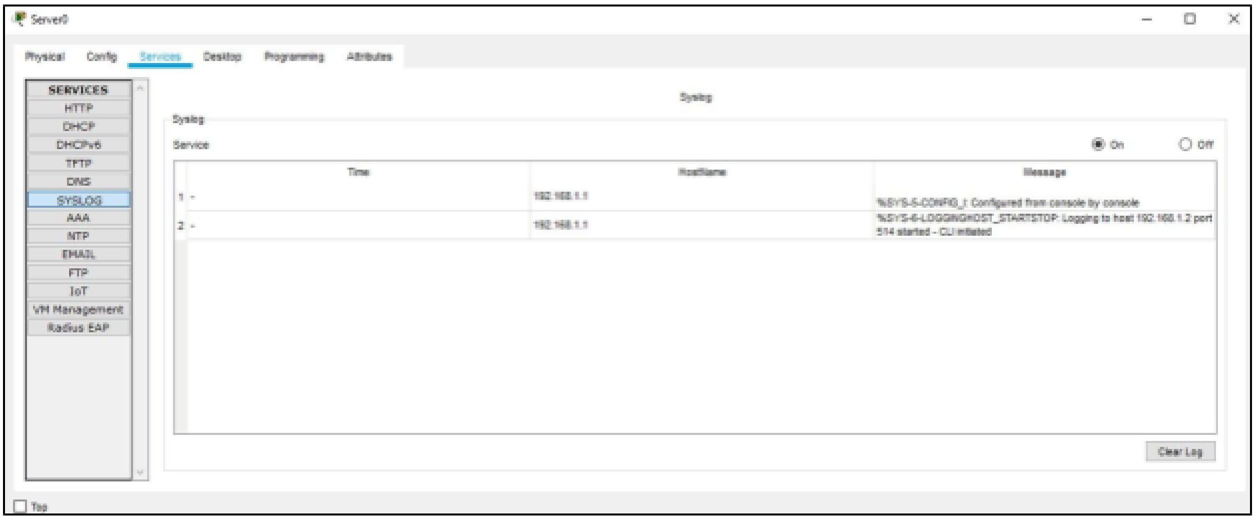
<u>Step 6:</u> To check Syslog service on the server:

i) Go to Router0 ➜ CLI Tab ➜ Type the following commands:



```
Router>enable
Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#logging 192.168.1.2
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
%SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 192.168.1.2 port 514
started - CLI initiated

Router#ping 192.168.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/1/3 ms

Router#
```

ii) Go to Server0 ➜ Service Tab ➜ SYSLOG:



Syslog

Service ● On ○ Off

	Time	HostName	Message
1	-	192.168.1.1	%SYS-5-CONFIG_I: Configured from console by console
2	-	192.168.1.1	%SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 192.168.1.2 port 514 started - CLI initiated