Roll No: IT21036 **Subject - Security in Computing** **Date: 06-03-24**
Class – TYBSCIT **Sem - VI**

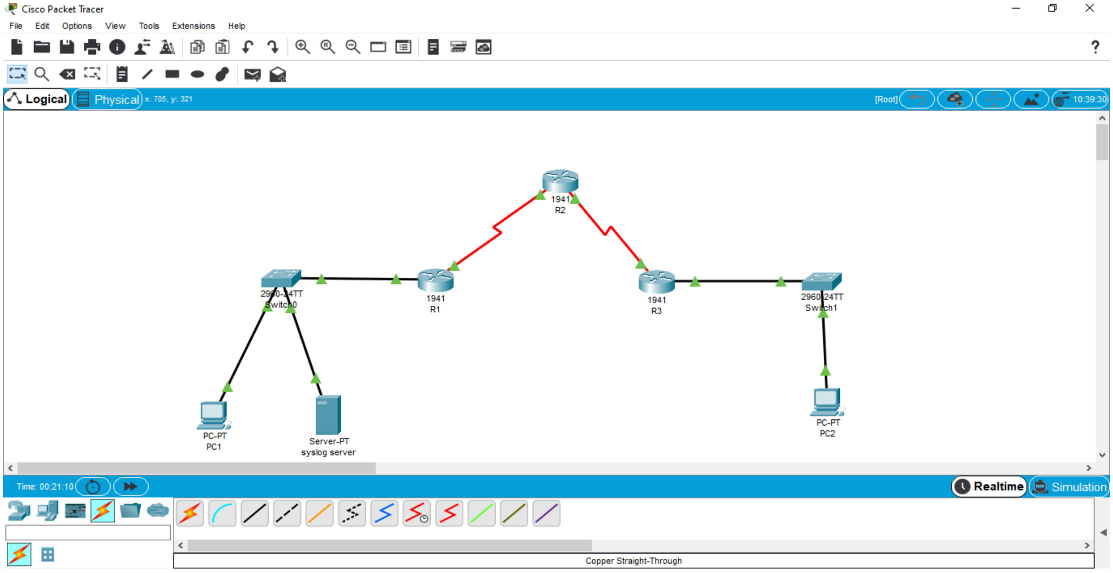
PRACTICAL NO 7

AIM: CONFIGURE IOS INTRUSION PREVENTION SYSTEM(IPS) USING THE CLI

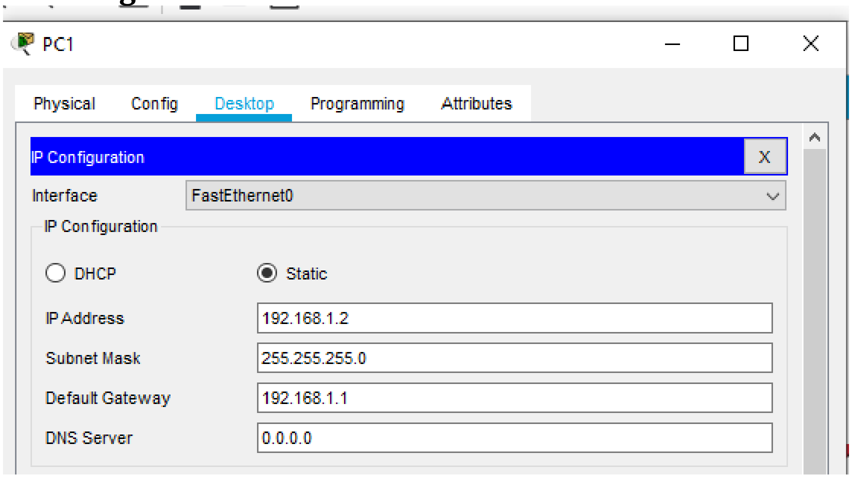
a. Enable IOS IPS

b. Modify an IPS signature

Topology Diagram



Assign IP addresses:



IP Configuration

Interface: FastEthernet0

IP Configuration

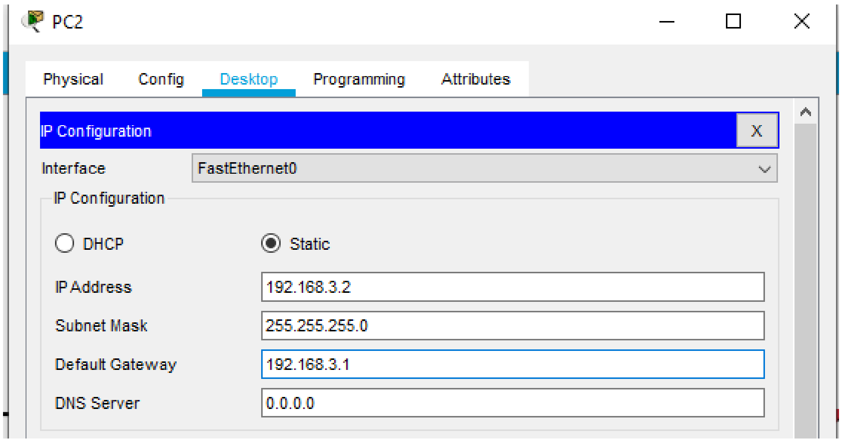
○ DHCP ● Static

IP Address: 192.168.1.2

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.1.1

DNS Server: 0.0.0.0



IP Configuration

Interface: FastEthernet0

IP Configuration

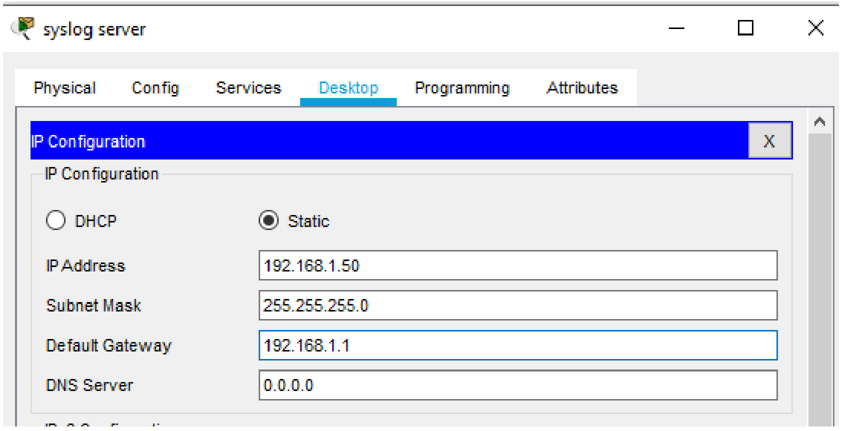
○ DHCP ● Static

IP Address: 192.168.3.2

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.3.1

DNS Server: 0.0.0.0



IP Configuration

IP Configuration

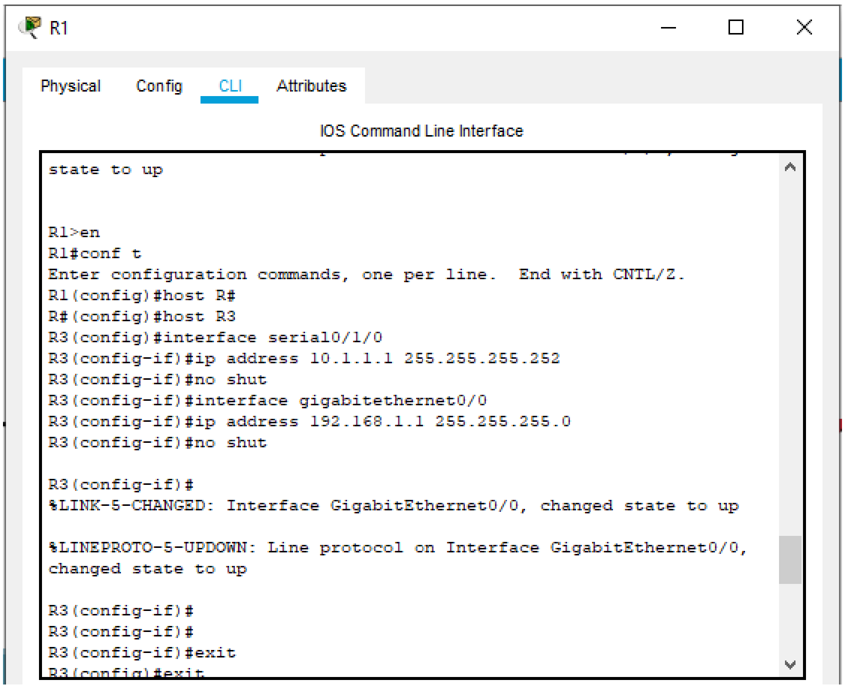
○ DHCP ● Static

IP Address 192.168.1.50

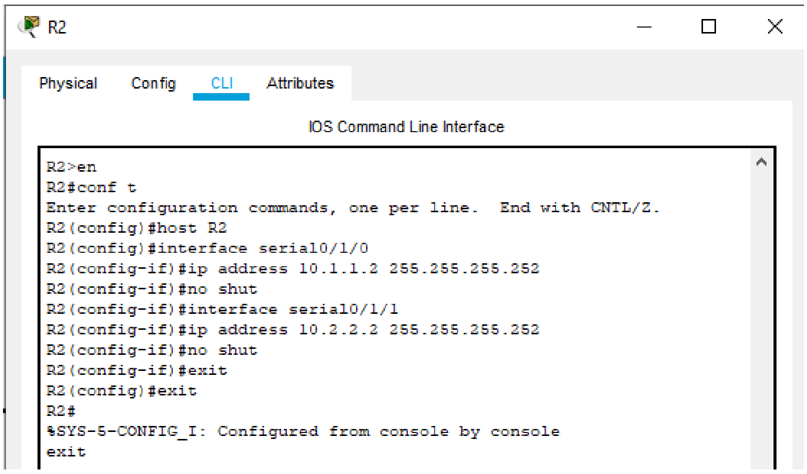
Subnet Mask 255.255.255.0

Default Gateway 192.168.1.1

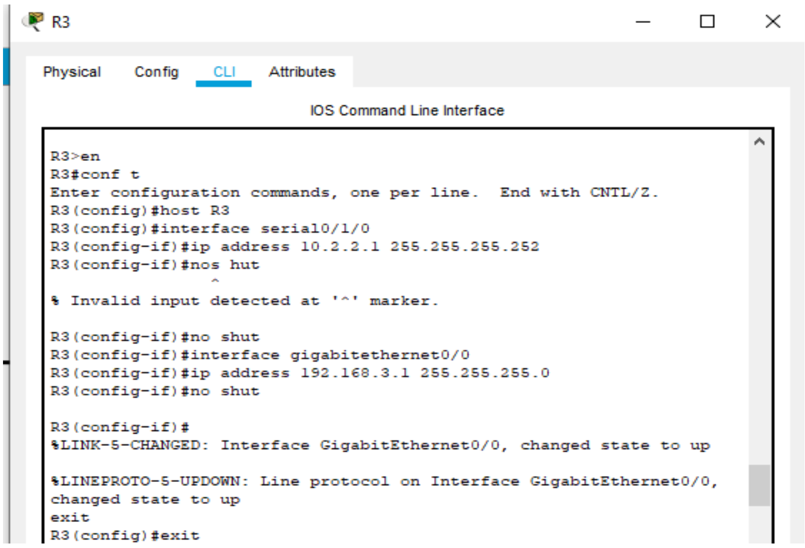
DNS Server 0.0.0.0



```
state to up


R1>en
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#host R#
R#(config)#host R3
R3(config)#interface serial0/1/0
R3(config-if)#ip address 10.1.1.1 255.255.255.252
R3(config-if)#no shut
R3(config-if)#interface gigabitethernet0/0
R3(config-if)#ip address 192.168.1.1 255.255.255.0
R3(config-if)#no shut

R3(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0,
changed state to up

R3(config-if)#
R3(config-if)#
R3(config-if)#exit
R3(config)#exit
```

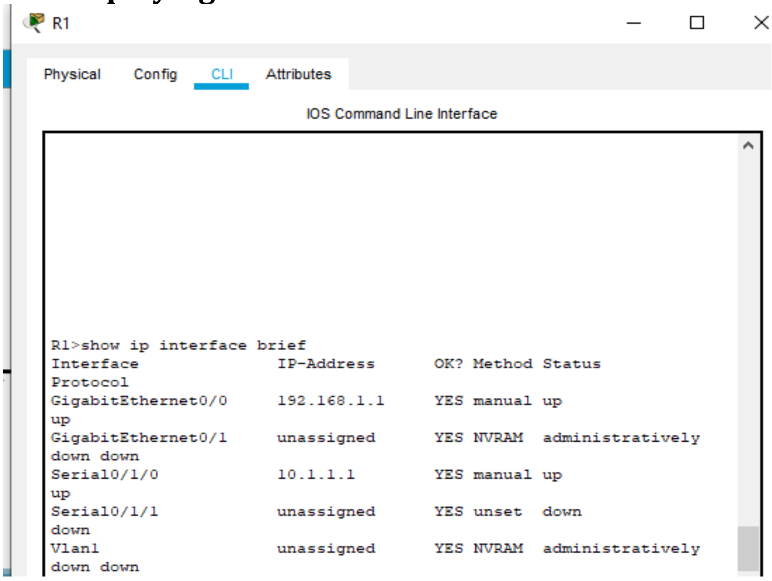


```
R2>en
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#host R2
R2(config)#interface serial0/1/0
R2(config-if)#ip address 10.1.1.2 255.255.255.252
R2(config-if)#no shut
R2(config-if)#interface serial0/1/1
R2(config-if)#ip address 10.2.2.2 255.255.255.252
R2(config-if)#no shut
R2(config-if)#exit
R2(config)#exit
R2#
%SYS-5-CONFIG_I: Configured from console by console
exit
```

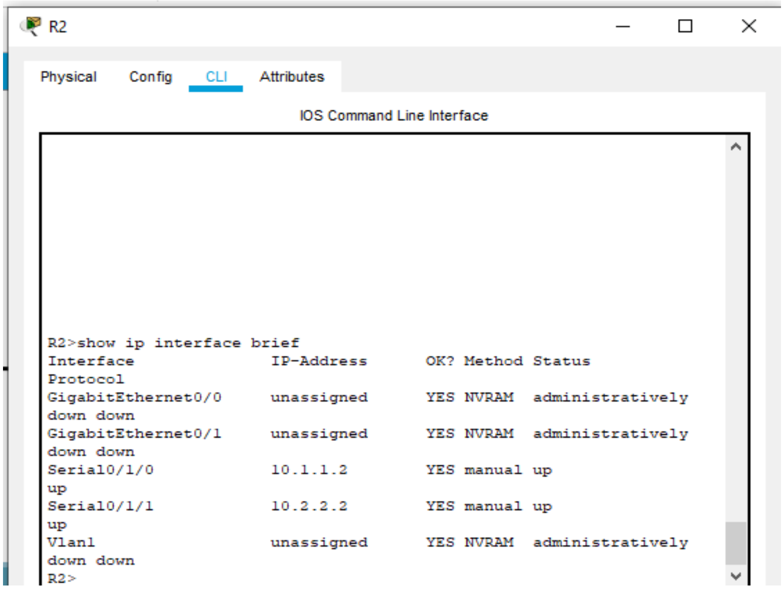


```
R3>en
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#host R3
R3(config)#interface serial0/1/0
R3(config-if)#ip address 10.2.2.1 255.255.255.252
R3(config-if)#nos hut
                ^
% Invalid input detected at '^' marker.

R3(config-if)#no shut
R3(config-if)#interface gigabitethernet0/0
R3(config-if)#ip address 192.168.3.1 255.255.255.0
R3(config-if)#no shut

R3(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0,
changed state to up
exit
R3(config)#exit
```

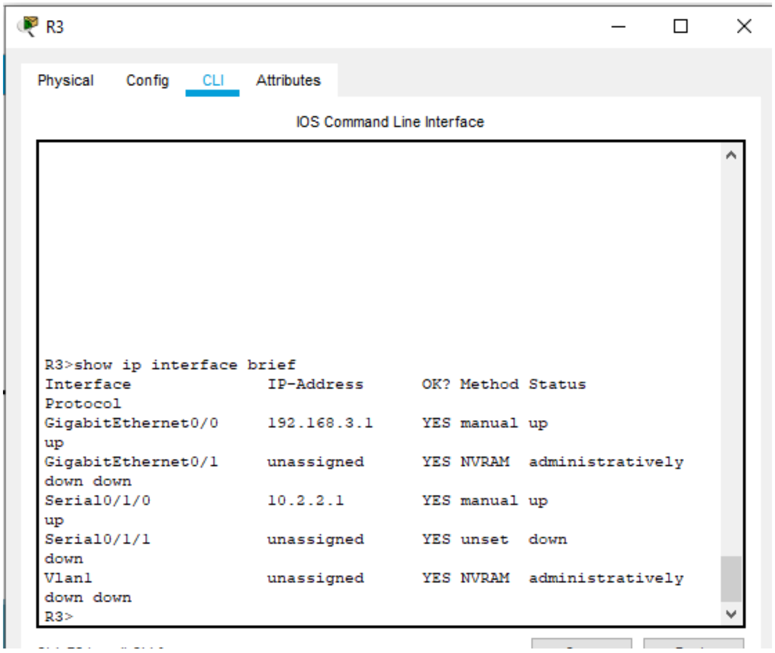
Displaying IP address Details of Routers



```
R1>show ip interface brief
Interface              IP-Address      OK? Method Status
Protocol
GigabitEthernet0/0     192.168.1.1     YES manual up
up
GigabitEthernet0/1     unassigned      YES NVRAM  administratively
down down
Serial0/1/0            10.1.1.1        YES manual up
up
Serial0/1/1            unassigned      YES unset  down
down
Vlan1                  unassigned      YES NVRAM  administratively
down down
```

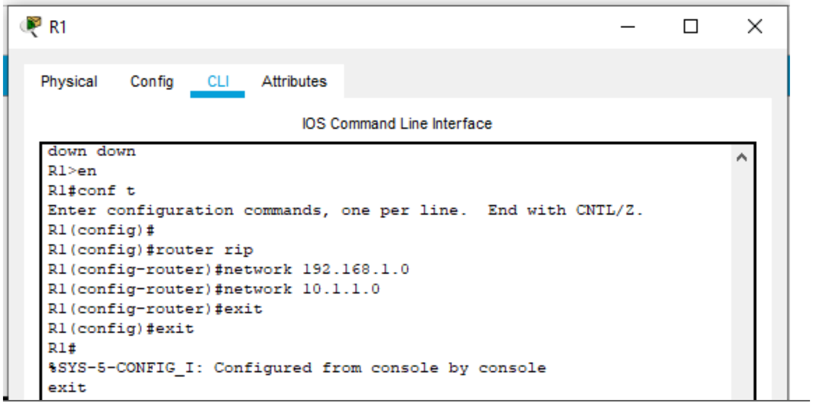


```
R2>show ip interface brief
Interface              IP-Address      OK? Method Status
Protocol
GigabitEthernet0/0     unassigned      YES NVRAM  administratively
down down
GigabitEthernet0/1     unassigned      YES NVRAM  administratively
down down
Serial0/1/0            10.1.1.2        YES manual up
up
Serial0/1/1            10.2.2.2        YES manual up
up
Vlan1                  unassigned      YES NVRAM  administratively
down down
R2>
```

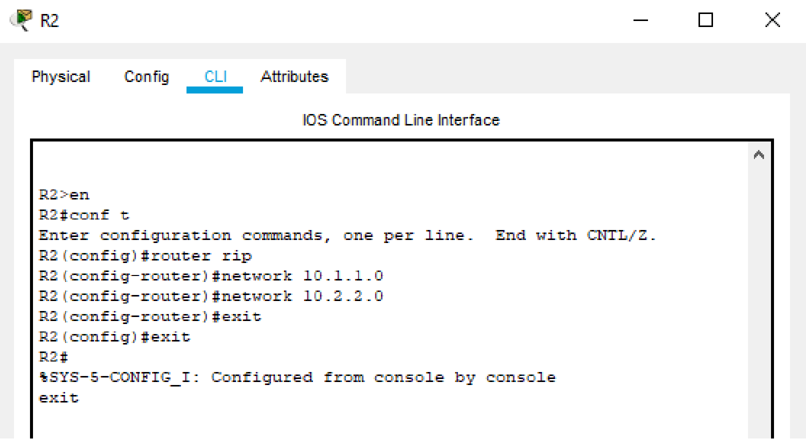


```
R3>show ip interface brief
Interface              IP-Address      OK? Method Status
Protocol
GigabitEthernet0/0     192.168.3.1     YES manual up
up
GigabitEthernet0/1     unassigned      YES NVRAM  administratively
down down
Serial0/1/0            10.2.2.1        YES manual up
up
Serial0/1/1            unassigned      YES unset  down
down
Vlan1                  unassigned      YES NVRAM  administratively
down down
R3>
```

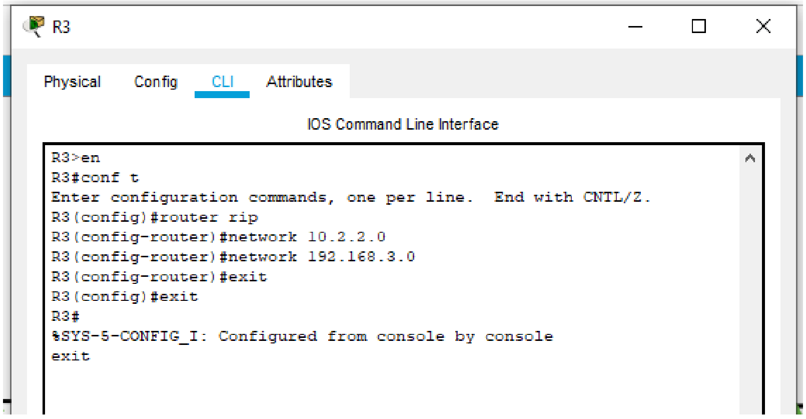
Configure RIP on routers



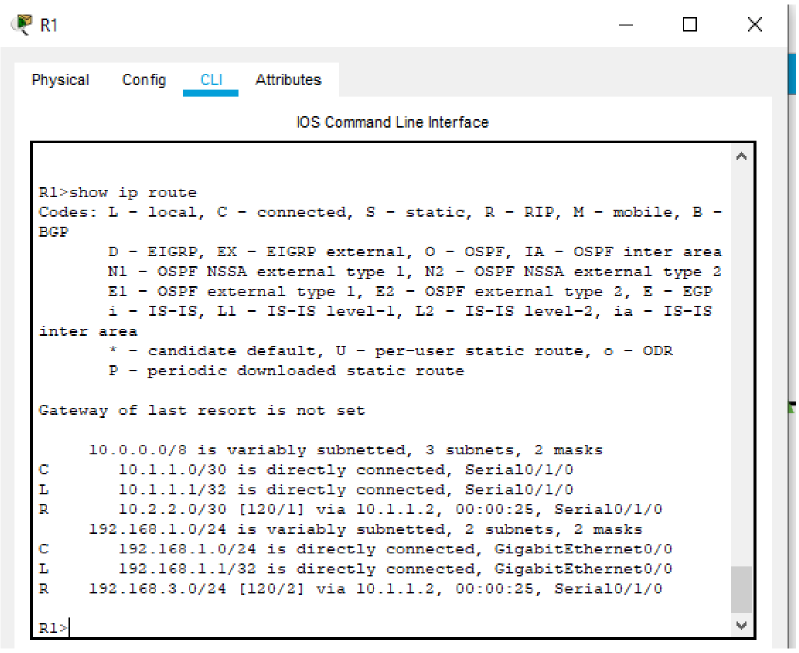
```
down down
R1>en
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#
R1(config)#router rip
R1(config-router)#network 192.168.1.0
R1(config-router)#network 10.1.1.0
R1(config-router)#exit
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console
exit
```



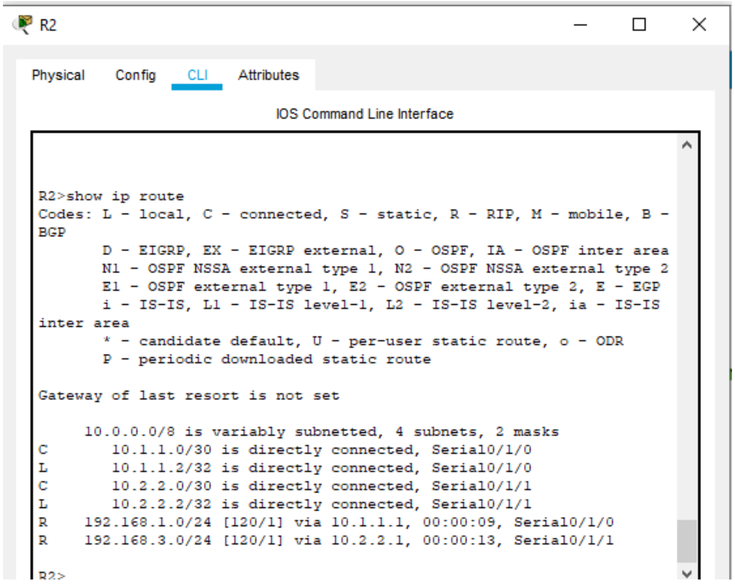
```
R2>en
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#router rip
R2(config-router)#network 10.1.1.0
R2(config-router)#network 10.2.2.0
R2(config-router)#exit
R2(config)#exit
R2#
%SYS-5-CONFIG_I: Configured from console by console
exit
```



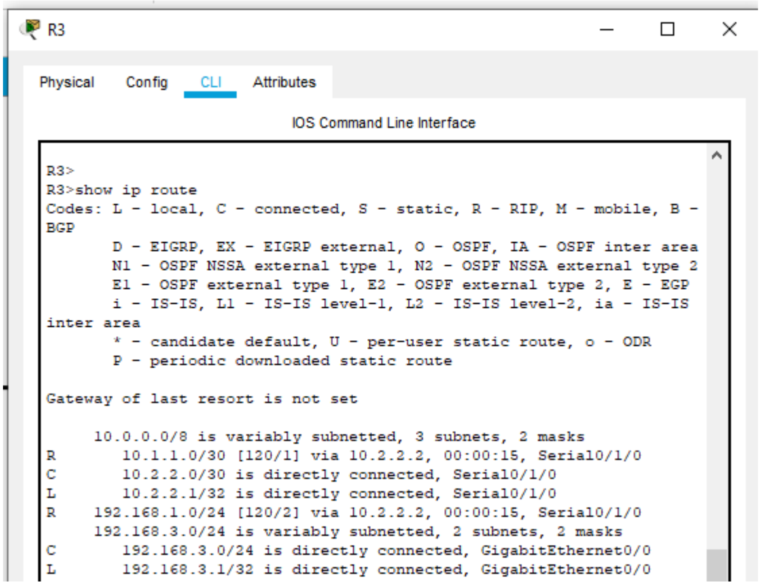
```
R3>en
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#router rip
R3(config-router)#network 10.2.2.0
R3(config-router)#network 192.168.3.0
R3(config-router)#exit
R3(config)#exit
R3#
%SYS-5-CONFIG_I: Configured from console by console
exit
```



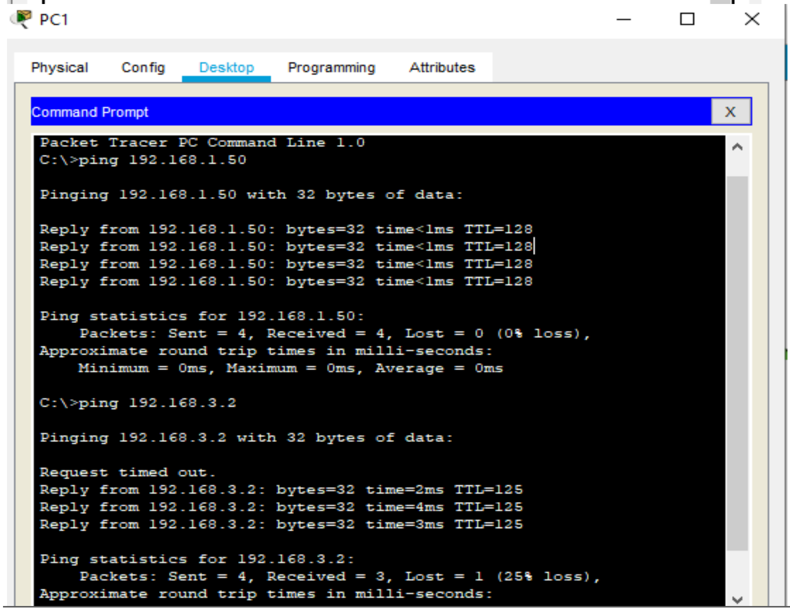
```
R1>show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B -
BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C       10.1.1.0/30 is directly connected, Serial0/1/0
L       10.1.1.1/32 is directly connected, Serial0/1/0
R       10.2.2.0/30 [120/1] via 10.1.1.2, 00:00:25, Serial0/1/0
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/0
L       192.168.1.1/32 is directly connected, GigabitEthernet0/0
R    192.168.3.0/24 [120/2] via 10.1.1.2, 00:00:25, Serial0/1/0

R1>
```



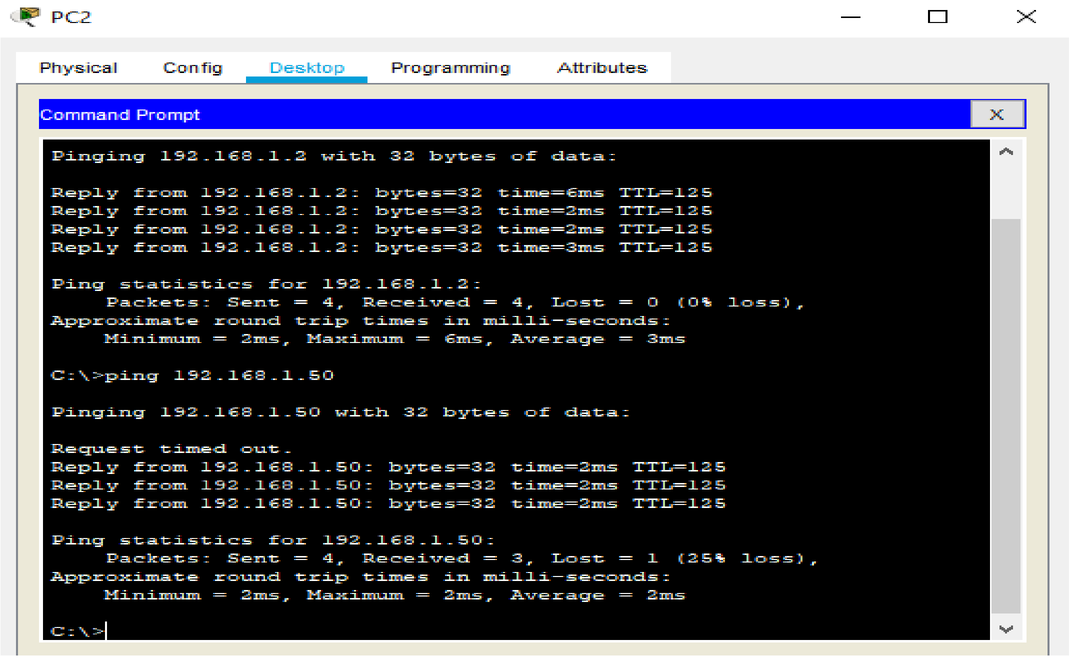
```
R2>show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B -
BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C       10.1.1.0/30 is directly connected, Serial0/1/0
L       10.1.1.2/32 is directly connected, Serial0/1/0
C       10.2.2.0/30 is directly connected, Serial0/1/1
L       10.2.2.2/32 is directly connected, Serial0/1/1
R    192.168.1.0/24 [120/1] via 10.1.1.1, 00:00:09, Serial0/1/0
R    192.168.3.0/24 [120/1] via 10.2.2.1, 00:00:13, Serial0/1/1

R2>
```



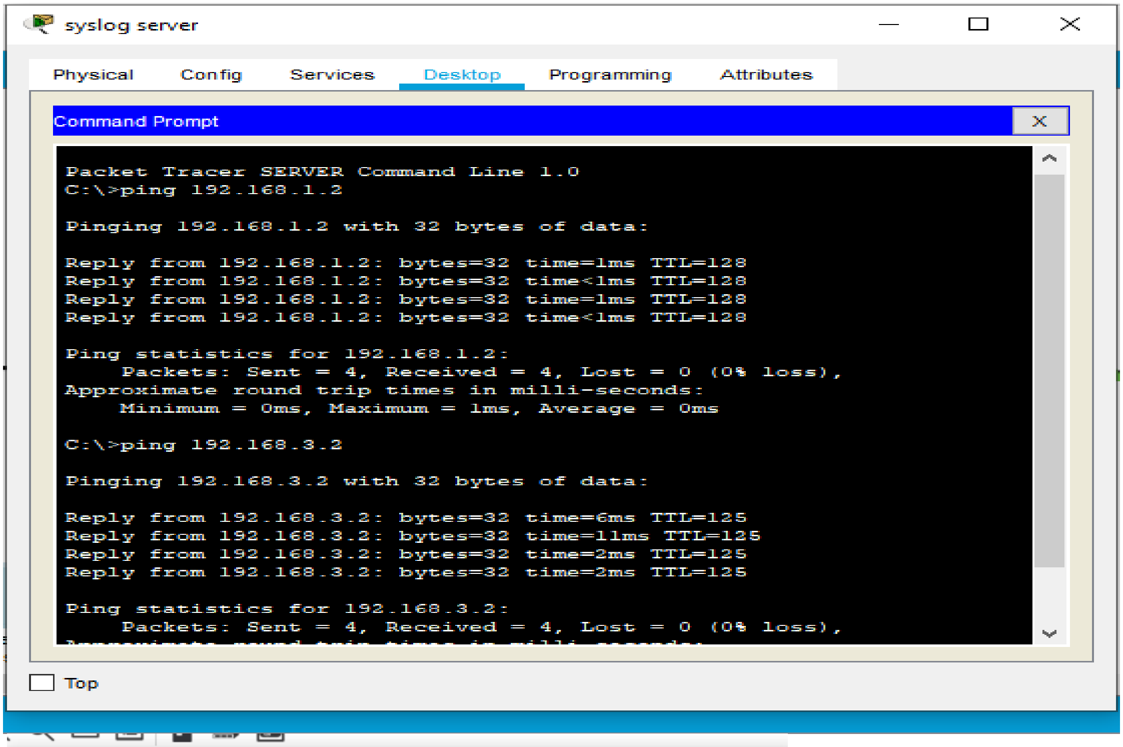
```
R3>
R3>show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B -
BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
R       10.1.1.0/30 [120/1] via 10.2.2.2, 00:00:15, Serial0/1/0
C       10.2.2.0/30 is directly connected, Serial0/1/0
L       10.2.2.1/32 is directly connected, Serial0/1/0
R    192.168.1.0/24 [120/2] via 10.2.2.2, 00:00:15, Serial0/1/0
     192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.3.0/24 is directly connected, GigabitEthernet0/0
L       192.168.3.1/32 is directly connected, GigabitEthernet0/0
```



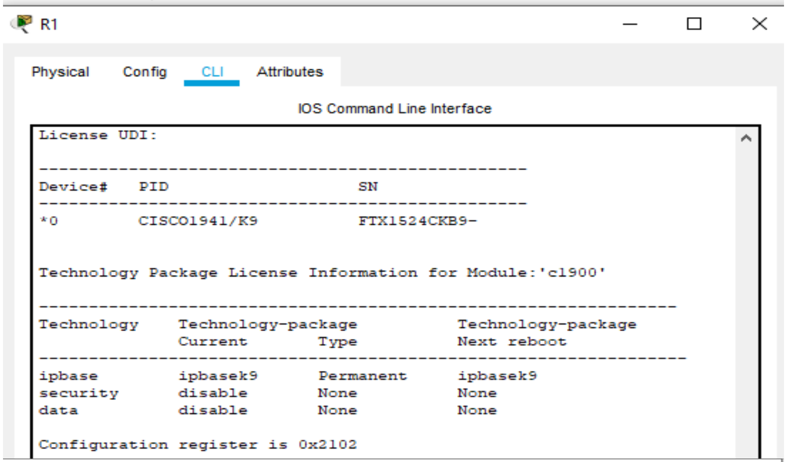
```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.50

Pinging 192.168.1.50 with 32 bytes of data:

Reply from 192.168.1.50: bytes=32 time<1ms TTL=128
Reply from 192.168.1.50: bytes=32 time<1ms TTL=128
Reply from 192.168.1.50: bytes=32 time<1ms TTL=128
Reply from 192.168.1.50: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.50:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.3.2

Pinging 192.168.3.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.3.2: bytes=32 time=2ms TTL=125
Reply from 192.168.3.2: bytes=32 time=4ms TTL=125
Reply from 192.168.3.2: bytes=32 time=3ms TTL=125

Ping statistics for 192.168.3.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
```



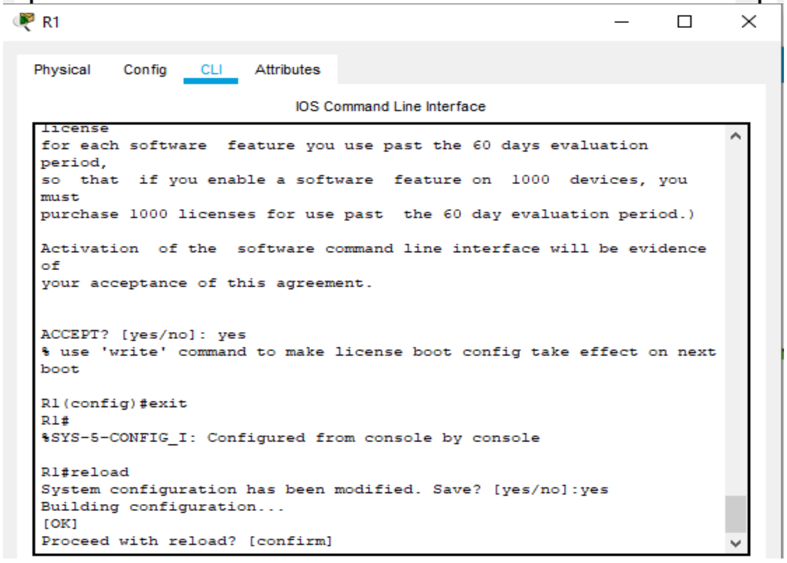
```
Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=6ms 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=3ms 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 = 6ms, Average = 3ms

C:\>ping 192.168.1.50

Pinging 192.168.1.50 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.50: bytes=32 time=2ms TTL=125
Reply from 192.168.1.50: bytes=32 time=2ms TTL=125
Reply from 192.168.1.50: bytes=32 time=2ms TTL=125

Ping statistics for 192.168.1.50:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 2ms, Average = 2ms

C:\>
```



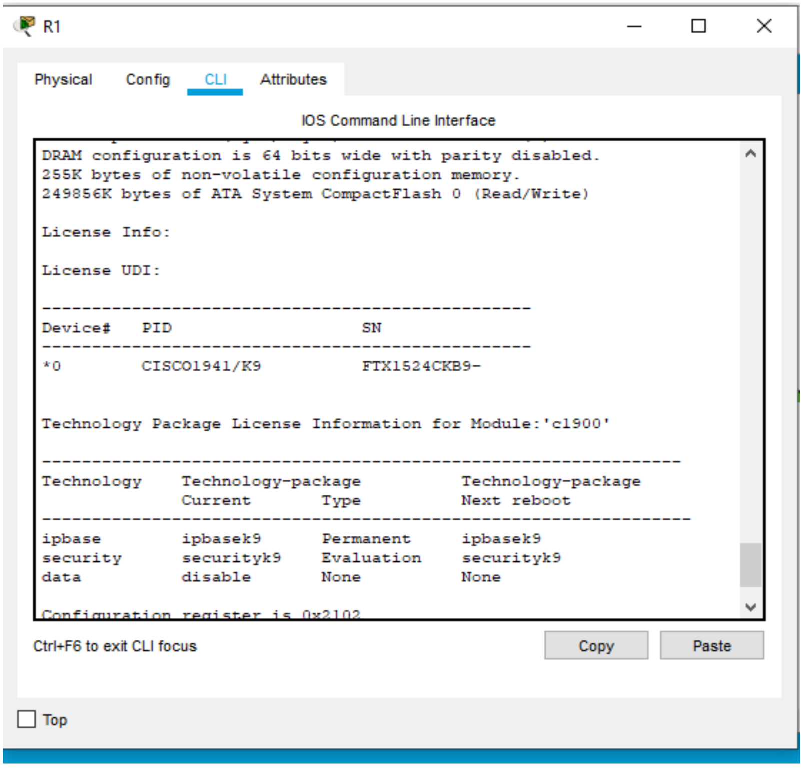
```
Packet Tracer SERVER Command Line 1.0
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time=1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128

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

C:\>ping 192.168.3.2

Pinging 192.168.3.2 with 32 bytes of data:

Reply from 192.168.3.2: bytes=32 time=6ms TTL=125
Reply from 192.168.3.2: bytes=32 time=11ms TTL=125
Reply from 192.168.3.2: bytes=32 time=2ms TTL=125
Reply from 192.168.3.2: bytes=32 time=2ms TTL=125

Ping statistics for 192.168.3.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
```



```
License UDI:

-------------------------------------------------
Device#   PID                   SN
-------------------------------------------------
*0        CISCO1941/K9          FTX1524CKB9-


Technology Package License Information for Module:'c1900'

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

Configuration register is 0x2102
```

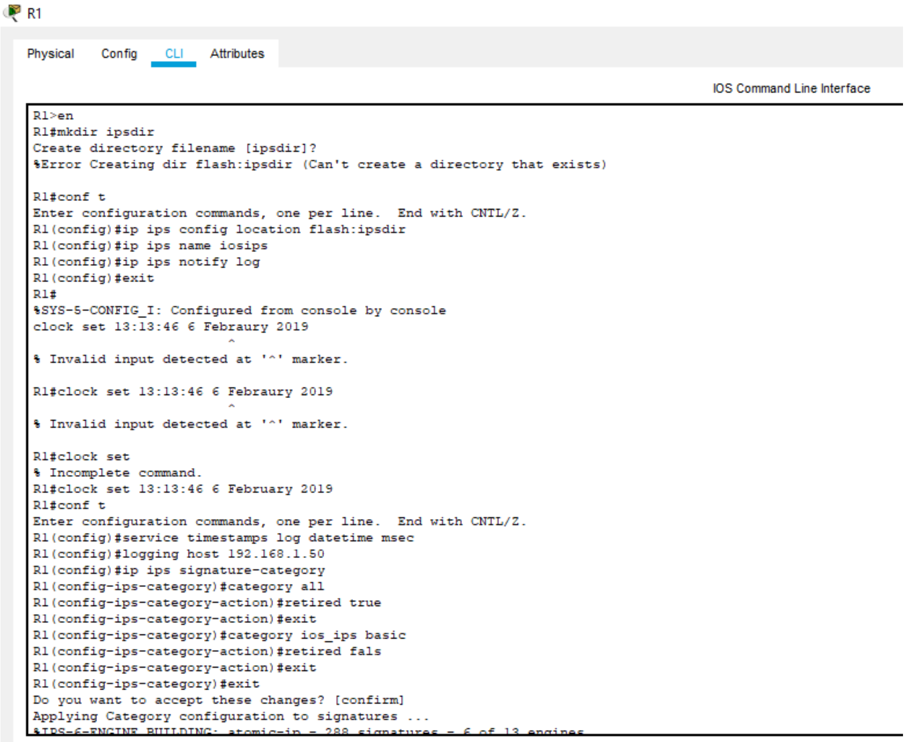


```
license
for each software  feature you use past the 60 days evaluation
period,
so  that  if you enable a software  feature on  1000  devices, you
must
purchase 1000 licenses for use past  the 60 day evaluation period.)

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

R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#reload
System configuration has been modified. Save? [yes/no]:yes
Building configuration...
[OK]
Proceed with reload? [confirm]
```

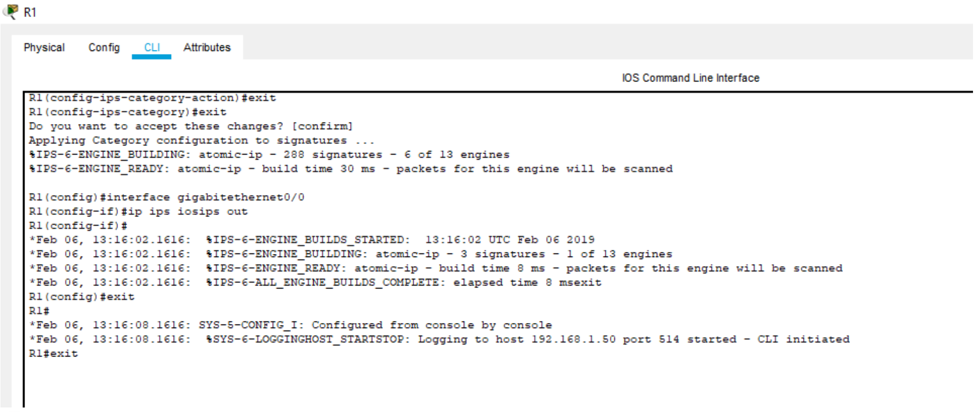


```
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)

License Info:

License UDI:

-------------------------------------------------
Device#   PID                   SN
-------------------------------------------------
*0        CISCO1941/K9          FTX1524CKB9-


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
```

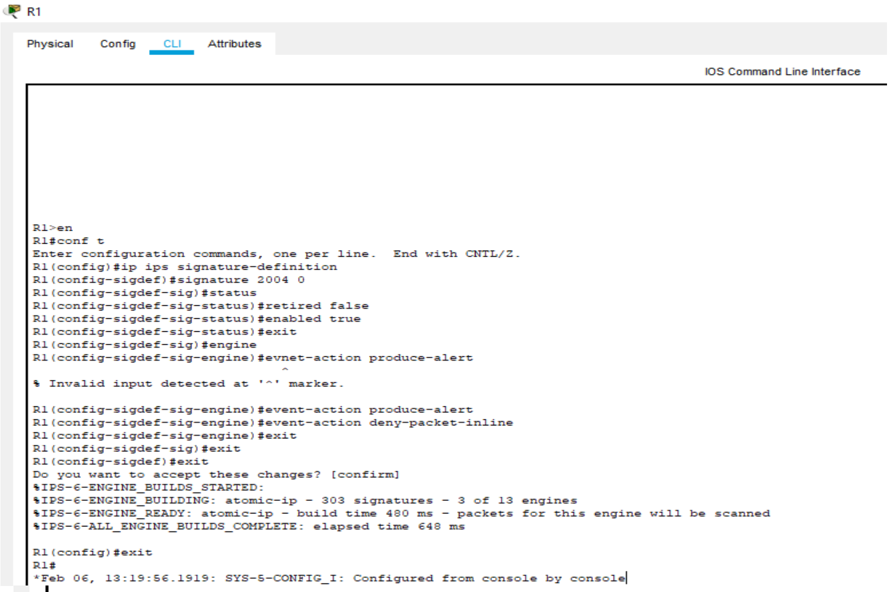
Enable IPS on R1



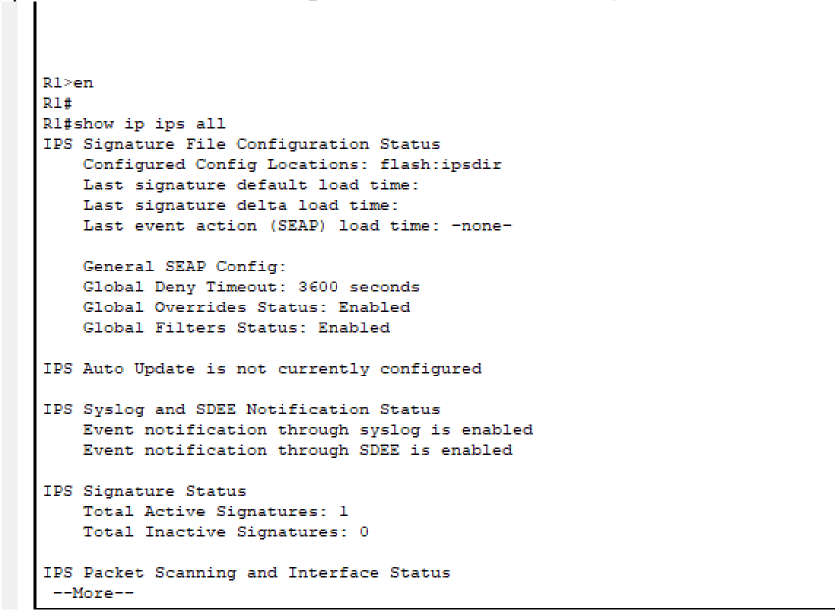
```
R1>en
R1#mkdir ipsdir
Create directory filename [ipsdir]?
%Error Creating dir flash:ipsdir (Can't create a directory that exists)

R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip ips config location flash:ipsdir
R1(config)#ip ips name iosips
R1(config)#ip ips notify log
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console
clock set 13:13:46 6 Febraury 2019
                         ^
% Invalid input detected at '^' marker.

R1#clock set 13:13:46 6 Febraury 2019
                         ^
% Invalid input detected at '^' marker.

R1#clock set
% Incomplete command.
R1#clock set 13:13:46 6 February 2019
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#service timestamps log datetime msec
R1(config)#logging host 192.168.1.50
R1(config)#ip ips signature-category
R1(config-ips-category)#category all
R1(config-ips-category-action)#retired true
R1(config-ips-category-action)#exit
R1(config-ips-category)#category ios_ips basic
R1(config-ips-category-action)#retired fals
R1(config-ips-category-action)#exit
R1(config-ips-category)#exit
Do you want to accept these changes? [confirm]
Applying Category configuration to signatures ...
%IPS-6-ENGINE_BUILDING: atomic-ip - 288 signatures - 6 of 13 engines
```



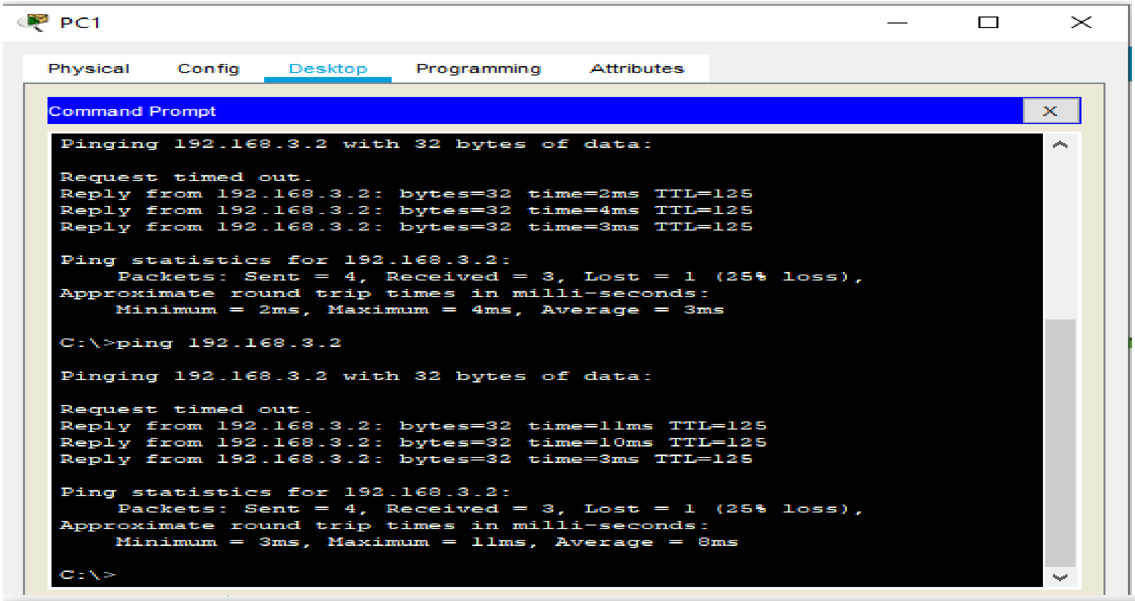
```
R1(config-ips-category-action)#exit
R1(config-ips-category)#exit
Do you want to accept these changes? [confirm]
Applying Category configuration to signatures ...
%IPS-6-ENGINE_BUILDING: atomic-ip - 288 signatures - 6 of 13 engines
%IPS-6-ENGINE_READY: atomic-ip - build time 30 ms - packets for this engine will be scanned

R1(config)#interface gigabitethernet0/0
R1(config-if)#ip ips iosips out
R1(config-if)#
*Feb 06, 13:16:02.1616:  %IPS-6-ENGINE_BUILDS_STARTED:  13:16:02 UTC Feb 06 2019
*Feb 06, 13:16:02.1616:  %IPS-6-ENGINE_BUILDING: atomic-ip - 3 signatures - 1 of 13 engines
*Feb 06, 13:16:02.1616:  %IPS-6-ENGINE_READY: atomic-ip - build time 8 ms - packets for this engine will be scanned
*Feb 06, 13:16:02.1616:  %IPS-6-ALL_ENGINE_BUILDS_COMPLETE: elapsed time 8 msexit
R1(config)#exit
R1#
*Feb 06, 13:16:08.1616: SYS-5-CONFIG_I: Configured from console by console
*Feb 06, 13:16:08.1616:  %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 192.168.1.50 port 514 started - CLI initiated
R1#exit
```



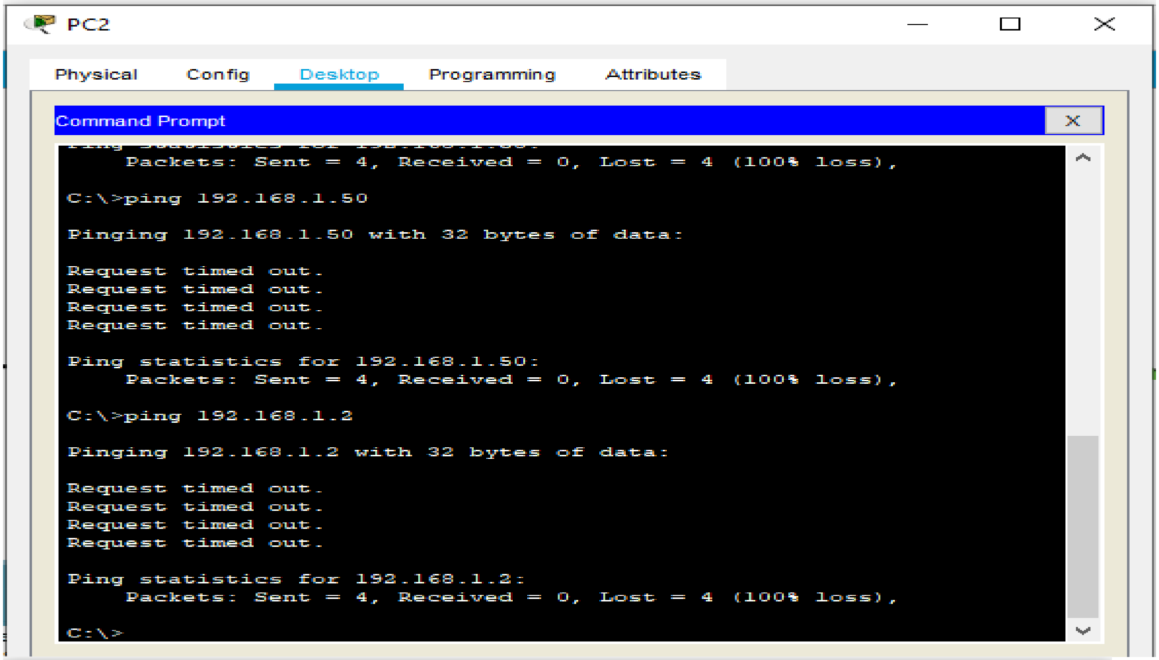
```
R1>en
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip ips signature-definition
R1(config-sigdef)#signature 2004 0
R1(config-sigdef-sig)#status
R1(config-sigdef-sig-status)#retired false
R1(config-sigdef-sig-status)#enabled true
R1(config-sigdef-sig-status)#exit
R1(config-sigdef-sig)#engine
R1(config-sigdef-sig-engine)#evnet-action produce-alert
                                ^
% Invalid input detected at '^' marker.

R1(config-sigdef-sig-engine)#event-action produce-alert
R1(config-sigdef-sig-engine)#event-action deny-packet-inline
R1(config-sigdef-sig-engine)#exit
R1(config-sigdef-sig)#exit
R1(config-sigdef)#exit
Do you want to accept these changes? [confirm]
%IPS-6-ENGINE_BUILDS_STARTED:
%IPS-6-ENGINE_BUILDING: atomic-ip - 303 signatures - 3 of 13 engines
%IPS-6-ENGINE_READY: atomic-ip - build time 480 ms - packets for this engine will be scanned
%IPS-6-ALL_ENGINE_BUILDS_COMPLETE: elapsed time 648 ms

R1(config)#exit
R1#
*Feb 06, 13:19:56.1919: SYS-5-CONFIG_I: Configured from console by console
```



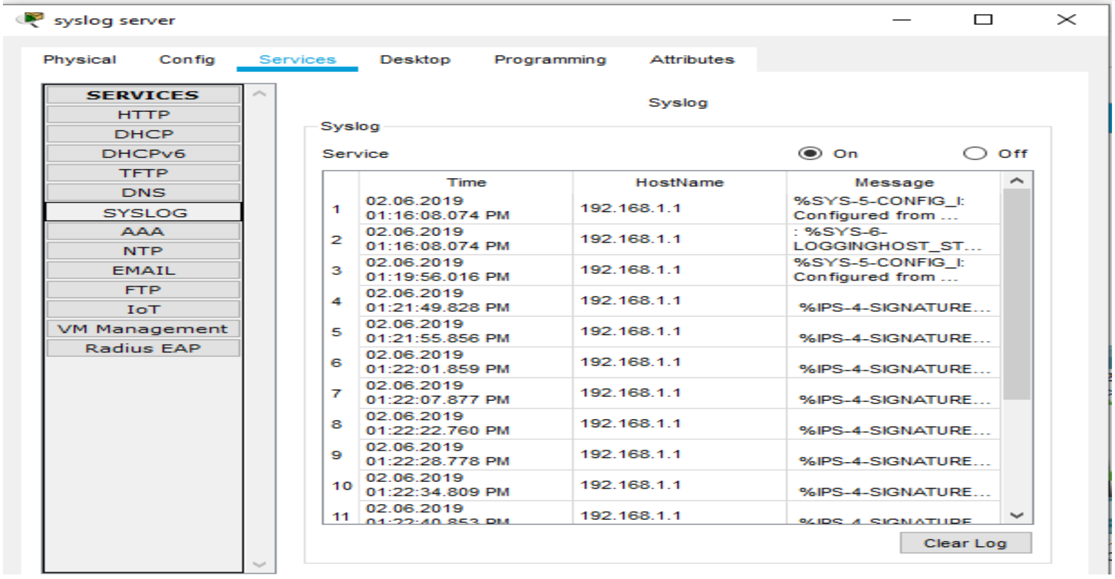
```
R1>en
R1#
R1#show ip ips all
IPS Signature File Configuration Status
    Configured Config Locations: flash:ipsdir
    Last signature default load time:
    Last signature delta load time:
    Last event action (SEAP) load time: -none-

    General SEAP Config:
    Global Deny Timeout: 3600 seconds
    Global Overrides Status: Enabled
    Global Filters Status: Enabled

IPS Auto Update is not currently configured

IPS Syslog and SDEE Notification Status
    Event notification through syslog is enabled
    Event notification through SDEE is enabled

IPS Signature Status
    Total Active Signatures: 1
    Total Inactive Signatures: 0

IPS Packet Scanning and Interface Status
 --More--
```



```
Pinging 192.168.3.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.3.2: bytes=32 time=2ms TTL=125
Reply from 192.168.3.2: bytes=32 time=4ms TTL=125
Reply from 192.168.3.2: bytes=32 time=3ms TTL=125

Ping statistics for 192.168.3.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 4ms, Average = 3ms

C:\>ping 192.168.3.2

Pinging 192.168.3.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.3.2: bytes=32 time=11ms TTL=125
Reply from 192.168.3.2: bytes=32 time=10ms TTL=125
Reply from 192.168.3.2: bytes=32 time=3ms TTL=125

Ping statistics for 192.168.3.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 11ms, Average = 8ms

C:\>
```



```
Ping statistics for 192.168.1.50:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.1.50

Pinging 192.168.1.50 with 32 bytes of data:

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

Ping statistics for 192.168.1.50:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

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

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```



Syslog

Service ● On ○ Off

	Time	HostName	Message
1	02.06.2019 01:16:08.074 PM	192.168.1.1	%SYS-5-CONFIG_I: Configured from ...
2	02.06.2019 01:16:08.074 PM	192.168.1.1	: %SYS-6-LOGGINGHOST_ST...
3	02.06.2019 01:19:56.016 PM	192.168.1.1	%SYS-5-CONFIG_I: Configured from ...
4	02.06.2019 01:21:49.828 PM	192.168.1.1	%IPS-4-SIGNATURE...
5	02.06.2019 01:21:55.856 PM	192.168.1.1	%IPS-4-SIGNATURE...
6	02.06.2019 01:22:01.859 PM	192.168.1.1	%IPS-4-SIGNATURE...
7	02.06.2019 01:22:07.877 PM	192.168.1.1	%IPS-4-SIGNATURE...
8	02.06.2019 01:22:22.760 PM	192.168.1.1	%IPS-4-SIGNATURE...
9	02.06.2019 01:22:28.778 PM	192.168.1.1	%IPS-4-SIGNATURE...
10	02.06.2019 01:22:34.809 PM	192.168.1.1	%IPS-4-SIGNATURE...
11	02.06.2019 01:22:40.853 PM	192.168.1.1	%IPS-4-SIGNATURE