CS581 (Computer & Network Security)

Lab-04

Group No.: 05
Group Members:
01. Rajnish Kumar (CIN: 304470392)
02. Jay Purohit (CIN: 304455065)
03. Rupal Jaiswal (CIN: 304442169)
04. Gaurav Prajapati (CIN: 304470132)

IPSec VPN

Setup a site-to-site IPSec VPN tunnel between your Cisco router and your Cisco ASA firewall. Submit (i) the configuration files used on the two Cisco devices and (ii) evidence that the IPSec tunnel works via output of debug ipsec, show crypto isakmp sa, and show crypto ipsec on both Cisco ASA firewall and on Cisco router.

We, Group No. 5, performed this lab on GNS3 in below steps:

Step 1: Draw a Network Topology Diagram

Step 2: Configuring PC & Router Configuration

Step 3: Checking Network Connectivity

Step 4: Configuring IKE & IPSec

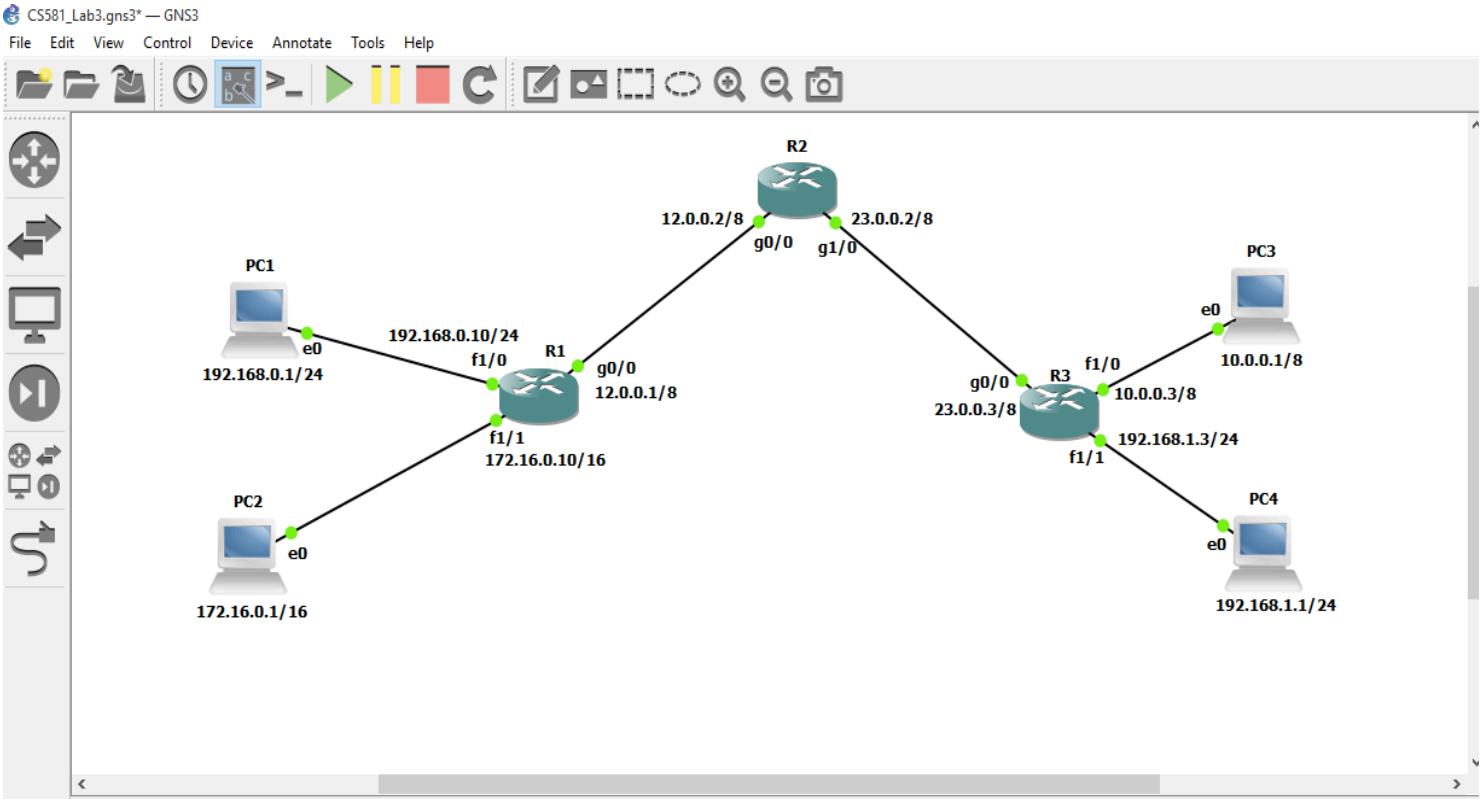
Step 5: Screenshots

Step 1: Draw a Network Topology Diagram

So, we kept 3 routers: R1, R2 and R3 and 4 PCs: PC1, PC2, PC3 and PC4

- R2 will simulate like as public network / cloud
- R1 and R3 will be connected to a public network i.e. R2
- R1 has two PCs i.e. PC1 and PC2
- R3 has also two PCs i.e. PC3 and PC4
- PC1 has an IP a/c to diagram is 192.168.0.1 and PC4 has an IP a/c to diagram is 192.168.1.1
- PC1 and PC4 has been connected to two different network i.e. one is in 192.168.0.0 network and another is in 192.168.1.0
- So, our aim is nothing but traffic going from PC1 (192.168.0.1) to PC4 (192.168.1.1) only should use VPN. In other words, no VPN should be available for PC1 – PC3.
- Only PC1 to PC4 should be a secured communication.
- The tunneling point is R1 and R3.
- We have formed a VPN tunnel between R1 to R3.

This is the below network diagram:



PC1 (e0): 192.168.0.1/24

PC2 (e0): 172.16.0.1/16

R1 (f1/0): 192.168.0.10/24

R1 (f1/1): 172.16.0.10/16

R1 (g0/0): 12.0.0.1/8

R2 (g0/0): 12.0.0.2/8

R2 (g1/0): 23.0.0.2/8

R3 (g0/0): 23.0.0.3/8

R3 (f1/0): 10.0.0.3/8

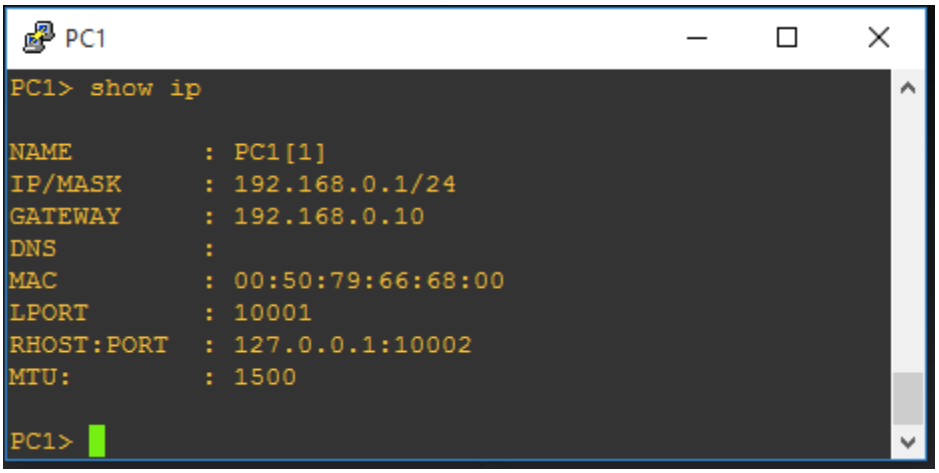
R3 (f1/1): 192.168.1.3/24

PC3 (e0): 10.0.0.1/8

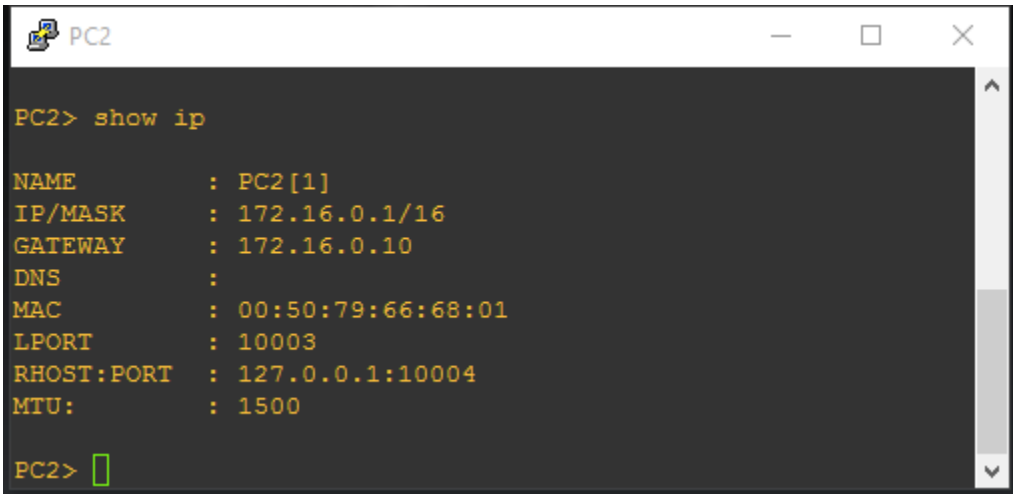
PC4 (e0): 192.168.1.1/24

Step 2: Configuring PC & Router Configuration

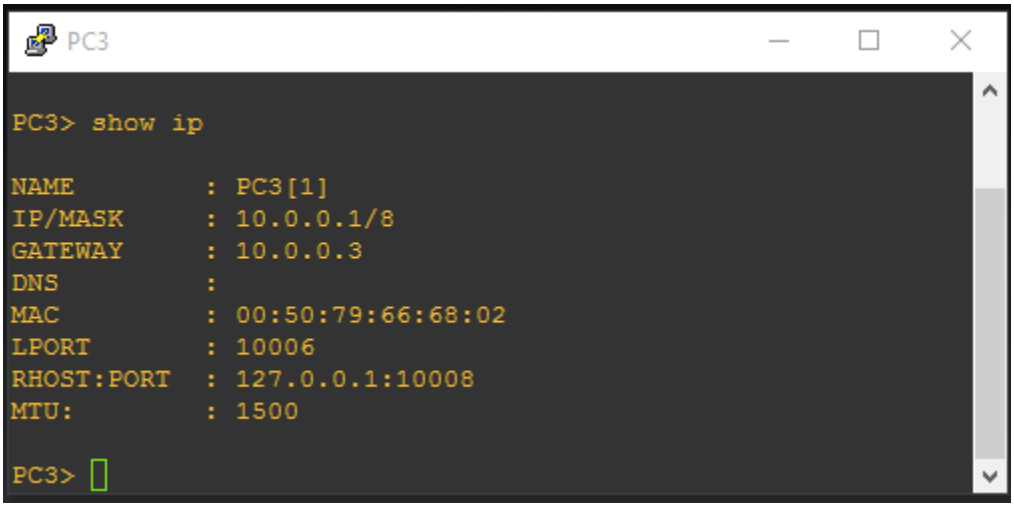
PC1 Configuration:



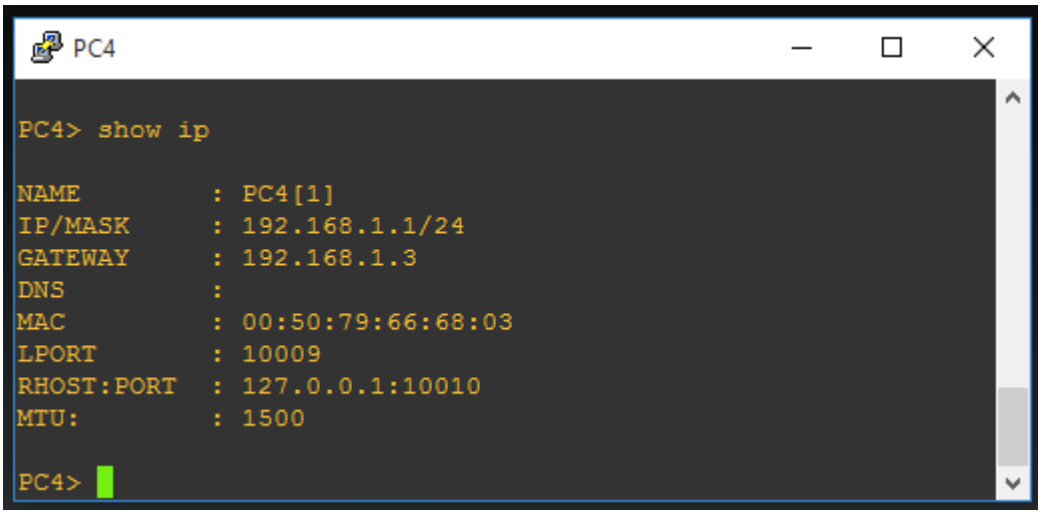
PC2 Configuration:



PC3 Configuration:

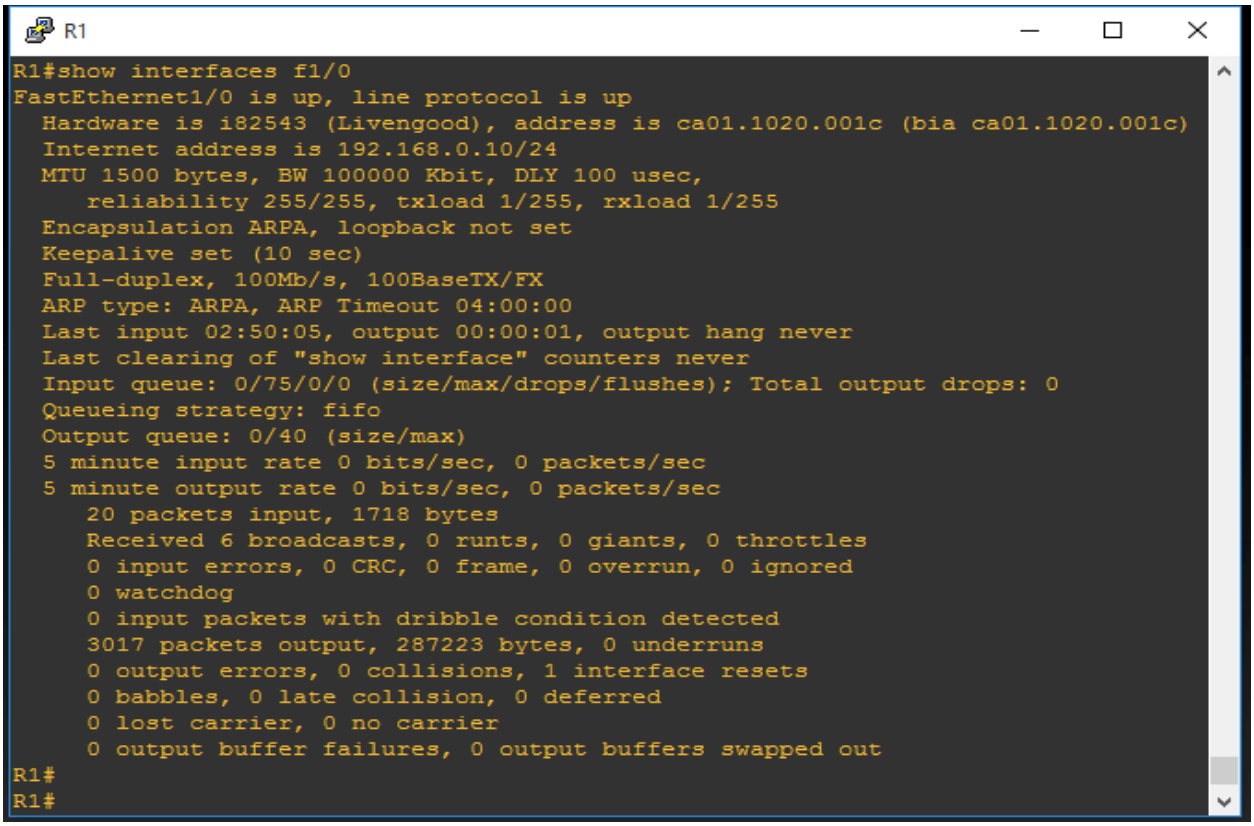


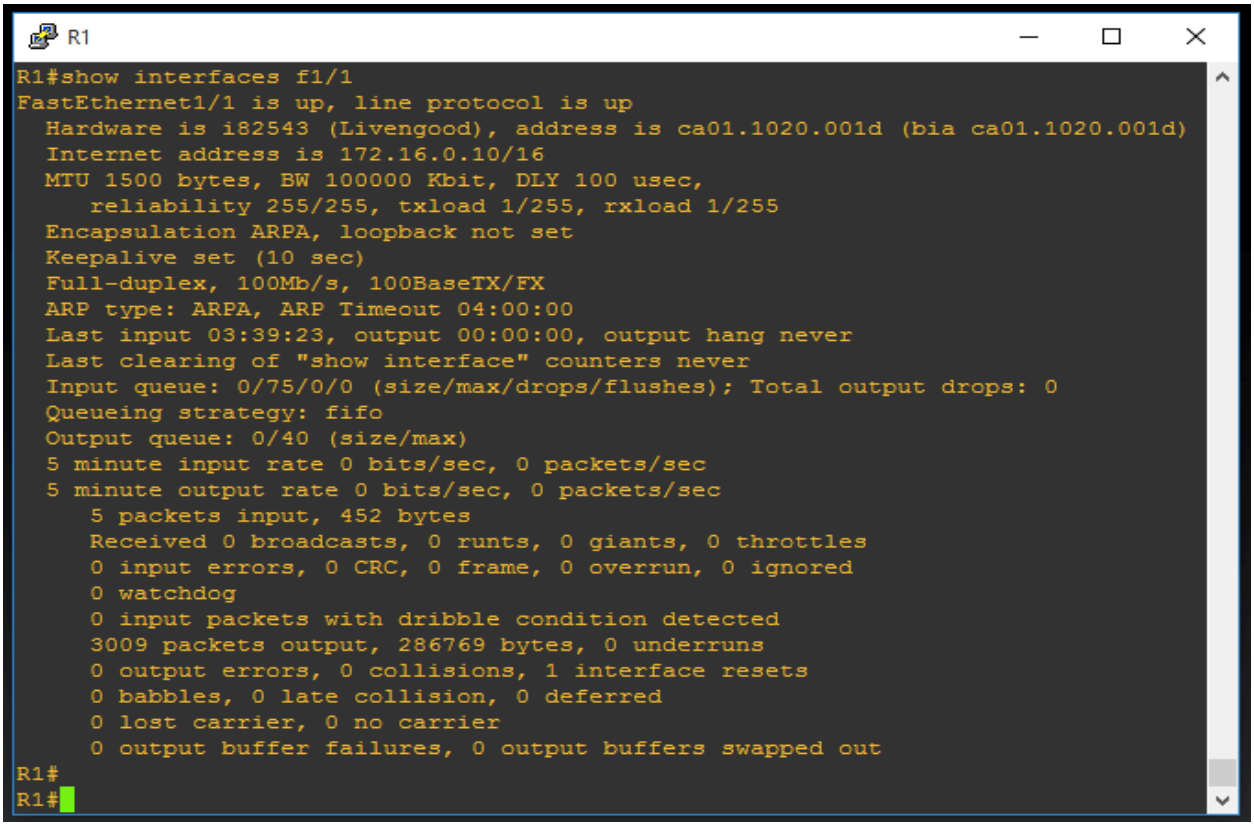
PC4 Configuration:

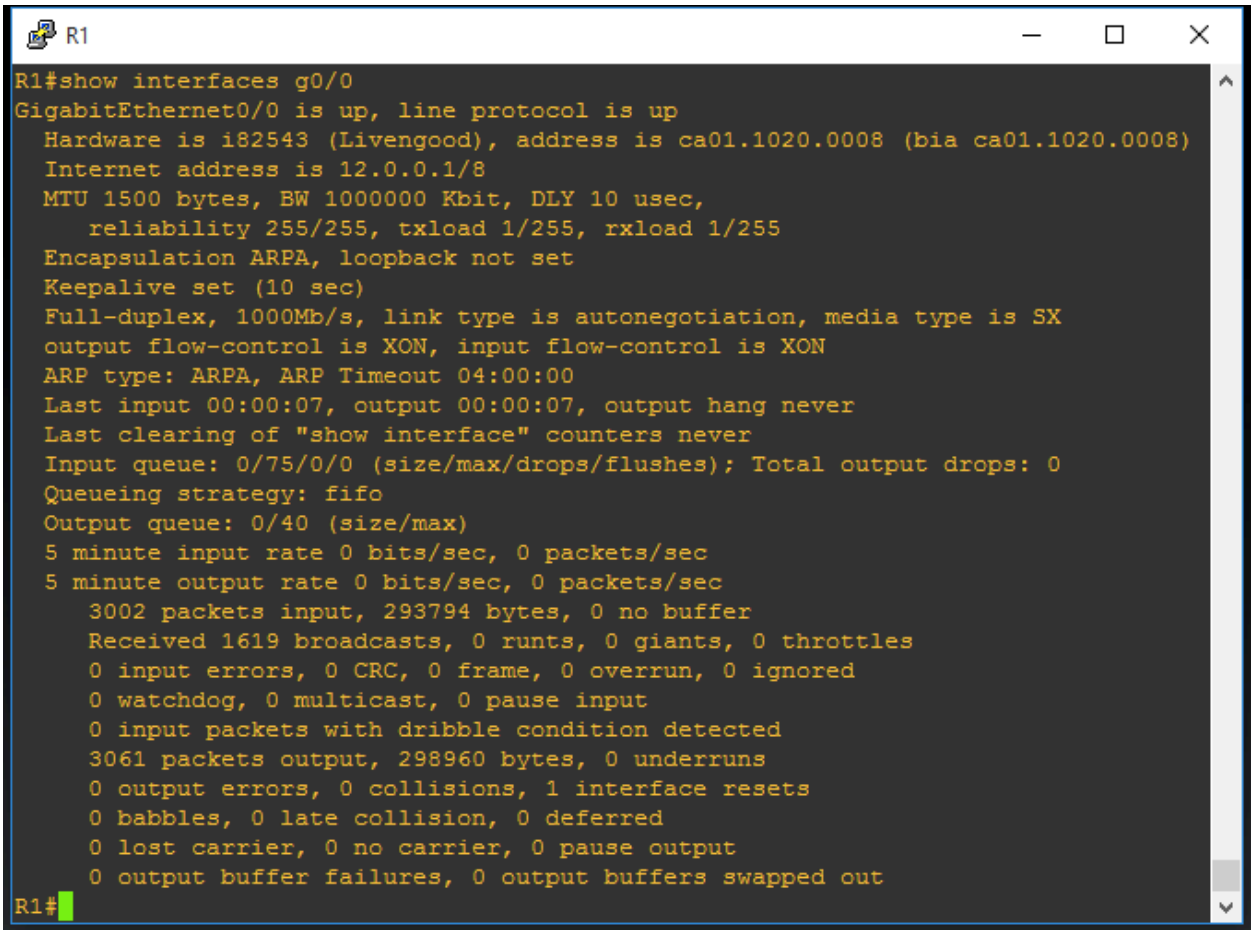


R1 (Interface Configuration):

```
R1# conf t
R1(config)# int f1/0
R1(config-if)# ip add 192.168.0.10 255.255.255.0
R1(config-if)# no sh
R1(config-if)# ip ospf 1 area 0
R1(config-if)# exit
R1(config)# int f1/1
R1(config-if)# ip add 172.16.0.10 255.255.0.0
R1(config-if)# no sh
R1(config-if)# ip ospf 1 area 0
R1(config-if)# exit
R1(config)# int g0/0
R1(config-if)# ip add 12.0.0.1 255.0.0.0
R1(config-if)# no sh
R1(config-if)# ip ospf 1 area 0
R1(config-if)# exit
R1(config)# exit
R1# wr me
```

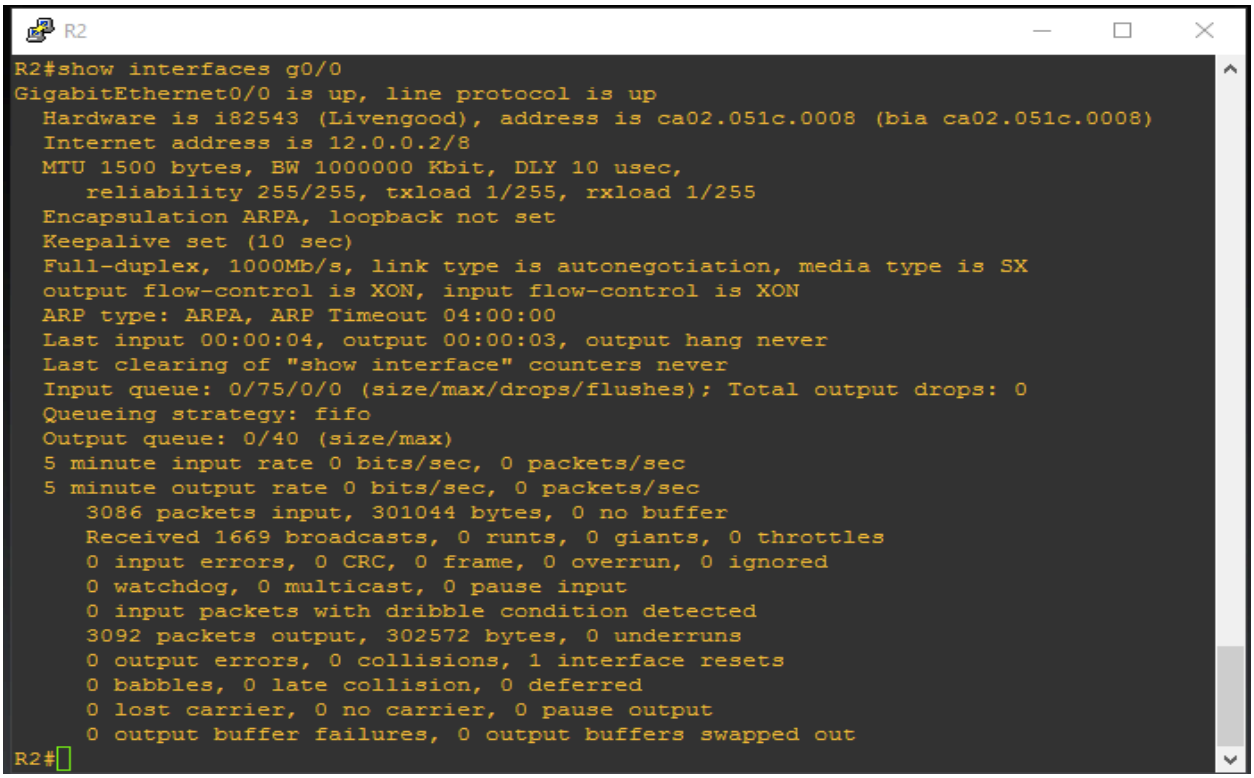

R1
R1#show interfaces f1/0
FastEthernet1/0 is up, line protocol is up
Hardware is i82543 (Livengood), address is ca01.1020.001c (bia ca01.1020.001c)
Internet address is 192.168.0.10/24
MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Full-duplex, 100Mb/s, 100BaseTX/FX
ARP type: ARPA, ARP Timeout 04:00:00
Last input 02:50:05, output 00:00:01, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
20 packets input, 1718 bytes
Received 6 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 watchdog
0 input packets with dribble condition detected
3017 packets output, 287223 bytes, 0 underruns
0 output errors, 0 collisions, 1 interface resets
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out
R1#
R1#

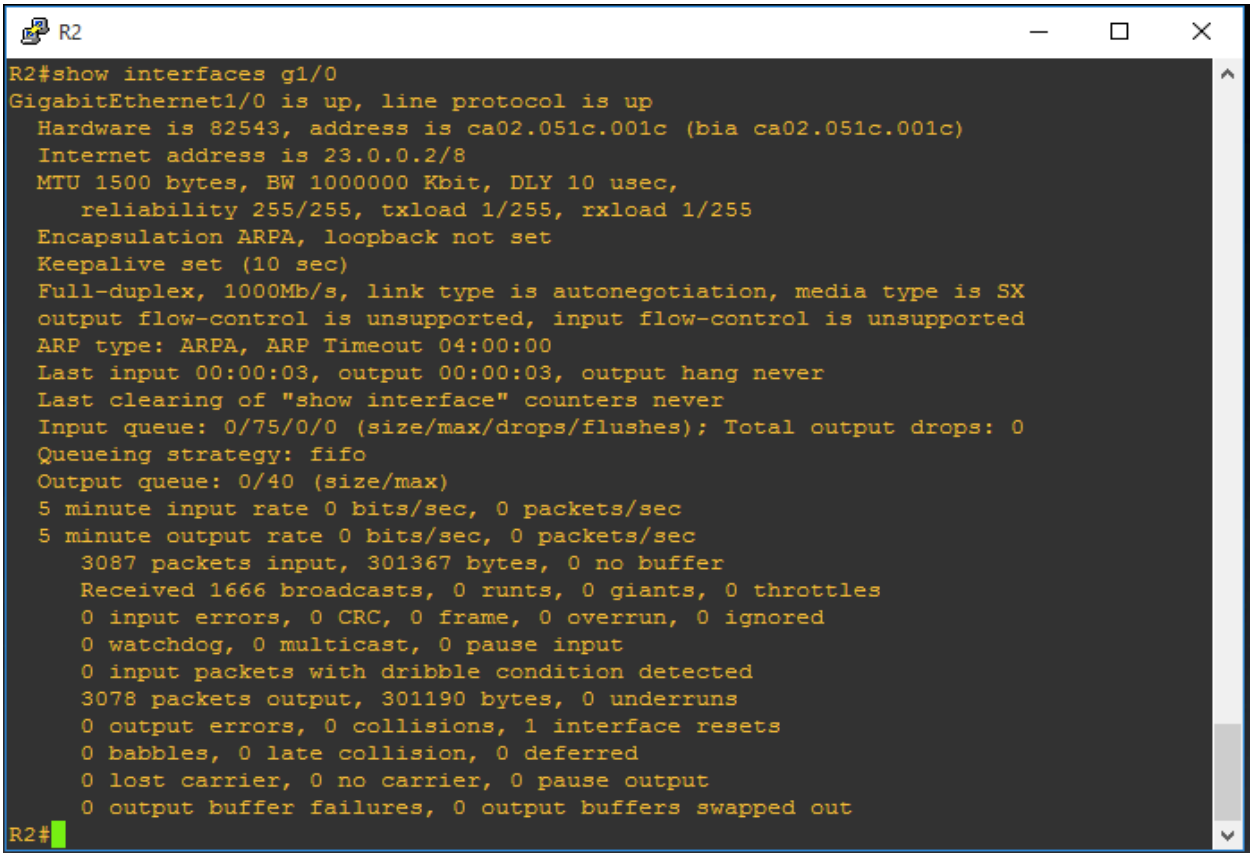

R1
R1#show interfaces f1/1
FastEthernet1/1 is up, line protocol is up
Hardware is i82543 (Livengood), address is ca01.1020.001d (bia ca01.1020.001d)
Internet address is 172.16.0.10/16
MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Full-duplex, 100Mb/s, 100BaseTX/FX
ARP type: ARPA, ARP Timeout 04:00:00
Last input 03:39:23, output 00:00:00, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
5 packets input, 452 bytes
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 watchdog
0 input packets with dribble condition detected
3009 packets output, 286769 bytes, 0 underruns
0 output errors, 0 collisions, 1 interface resets
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out
R1#
R1#


R1
R1#show interfaces g0/0
GigabitEthernet0/0 is up, line protocol is up
Hardware is i82543 (Livengood), address is ca01.1020.0008 (bia ca01.1020.0008)
Internet address is 12.0.0.1/8
MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Full-duplex, 1000Mb/s, link type is autonegotiation, media type is SX
output flow-control is XON, input flow-control is XON
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:07, output 00:00:07, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
3002 packets input, 293794 bytes, 0 no buffer
Received 1619 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 watchdog, 0 multicast, 0 pause input
0 input packets with dribble condition detected
3061 packets output, 298960 bytes, 0 underruns
0 output errors, 0 collisions, 1 interface resets
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier, 0 pause output
0 output buffer failures, 0 output buffers swapped out
R1#

R2 (Interface Configuration):

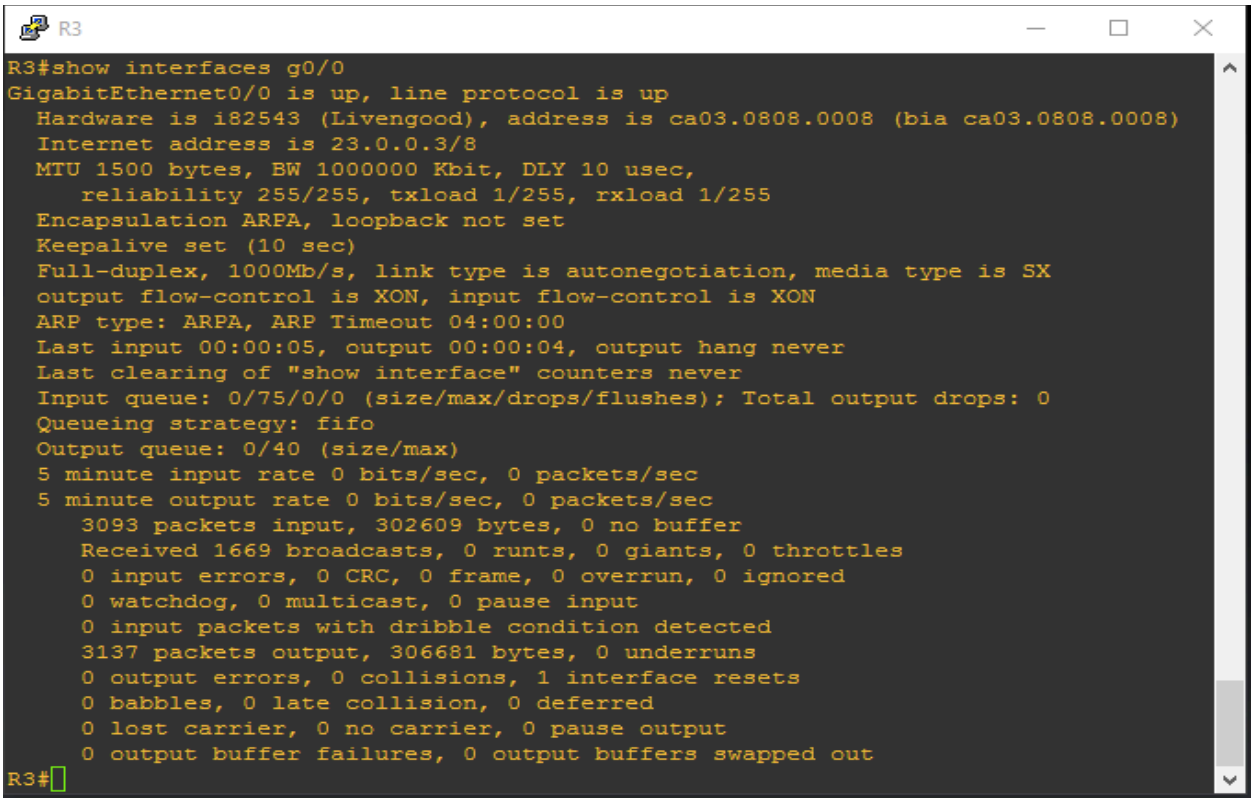
```
R2# conf t
R2(config)# int g0/0
R2(config-if)# ip add 12.0.0.2 255.0.0.0
R2(config-if)# no sh
R2(config-if)# ip ospf 1 area 0
R2(config-if)# exit
R2(config)# int g1/0
R2(config-if)# ip add 23.0.0.2 255.0.0.0
R2(config-if)# no sh
R2(config-if)# ip ospf 1 area 0
R2(config-if)# exit
R2(config)# exit
R2# wr me
```

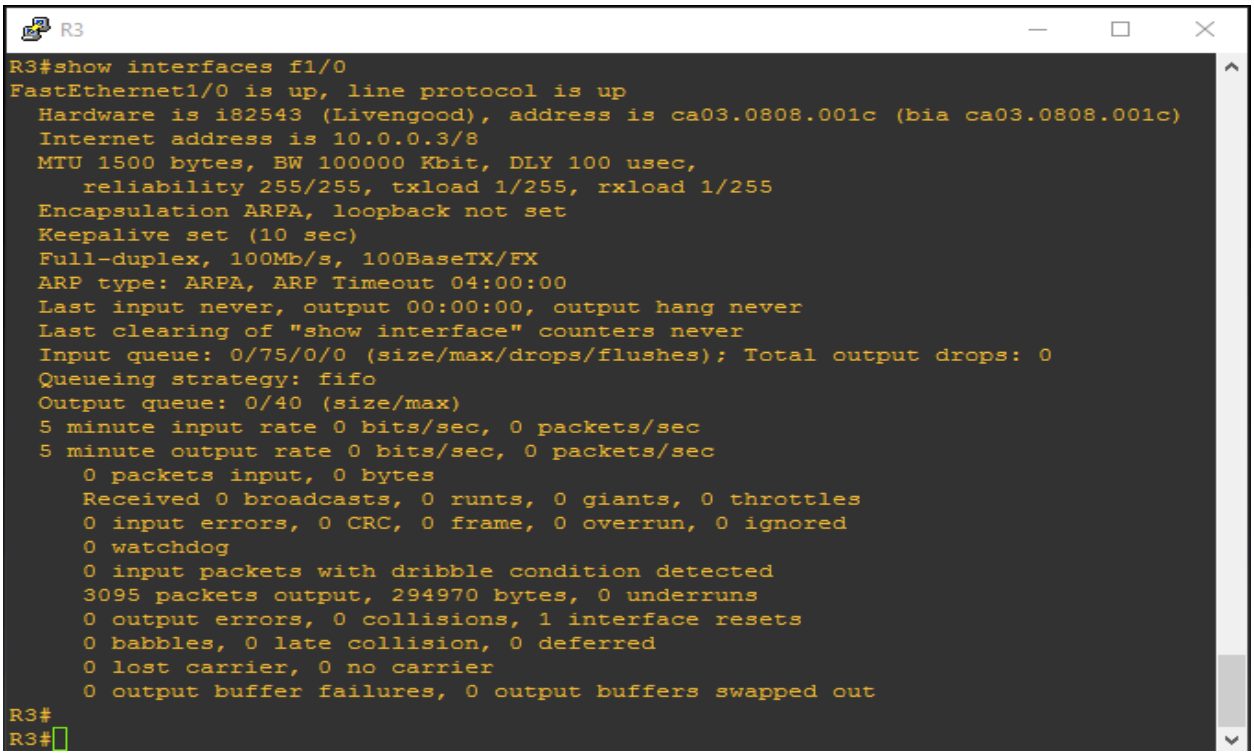

R2
R2#show interfaces g0/0
GigabitEthernet0/0 is up, line protocol is up
Hardware is i82543 (Livengood), address is ca02.051c.0008 (bia ca02.051c.0008)
Internet address is 12.0.0.2/8
MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Full-duplex, 1000Mb/s, link type is autonegotiation, media type is SX
output flow-control is XON, input flow-control is XON
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:04, output 00:00:03, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
3086 packets input, 301044 bytes, 0 no buffer
Received 1669 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 watchdog, 0 multicast, 0 pause input
0 input packets with dribble condition detected
3092 packets output, 302572 bytes, 0 underruns
0 output errors, 0 collisions, 1 interface resets
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier, 0 pause output
0 output buffer failures, 0 output buffers swapped out
R2#

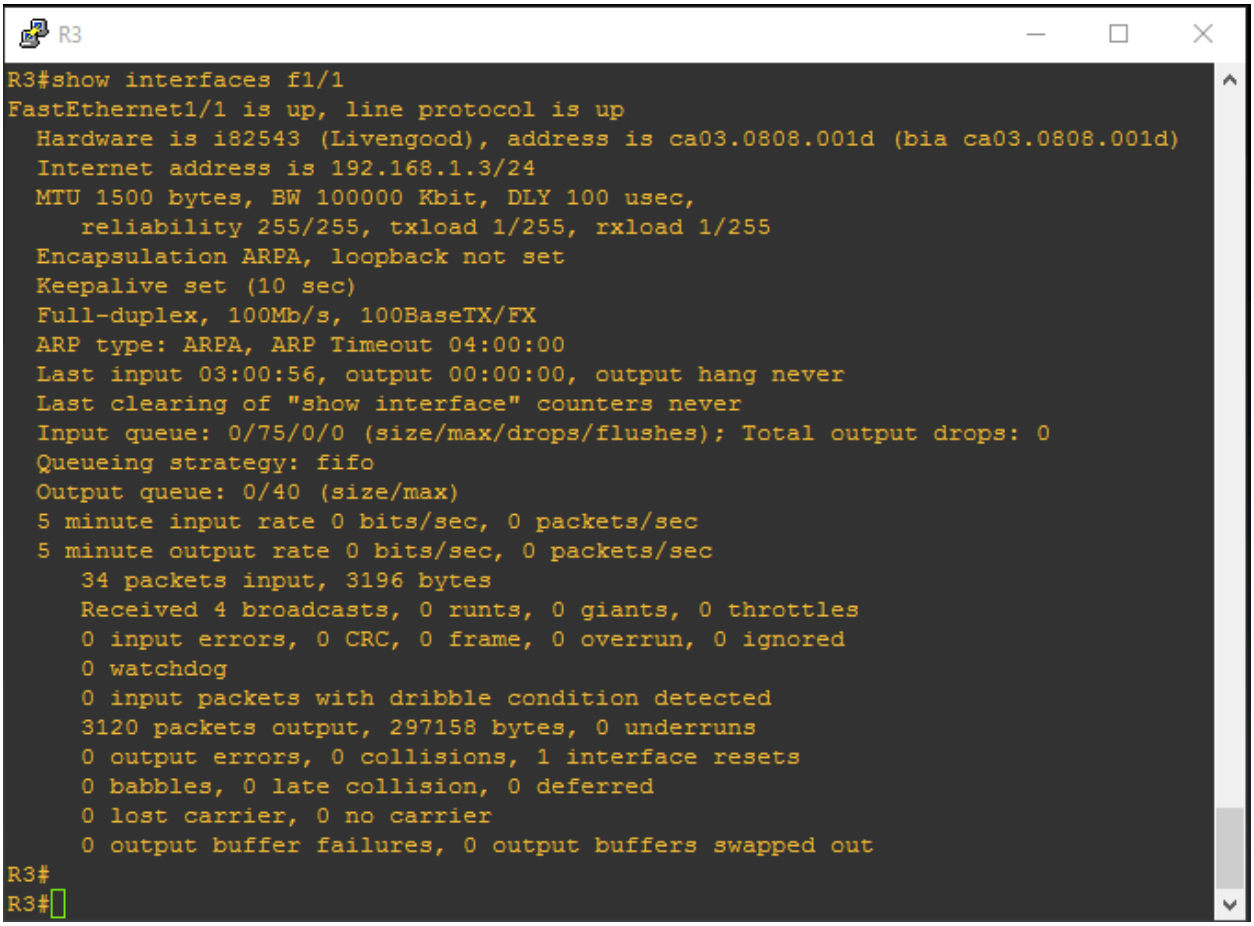

R2
R2#show interfaces g1/0
GigabitEthernet1/0 is up, line protocol is up
Hardware is 82543, address is ca02.051c.001c (bia ca02.051c.001c)
Internet address is 23.0.0.2/8
MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Full-duplex, 1000Mb/s, link type is autonegotiation, media type is SX
output flow-control is unsupported, input flow-control is unsupported
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:03, output 00:00:03, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
3087 packets input, 301367 bytes, 0 no buffer
Received 1666 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 watchdog, 0 multicast, 0 pause input
0 input packets with dribble condition detected
3078 packets output, 301190 bytes, 0 underruns
0 output errors, 0 collisions, 1 interface resets
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier, 0 pause output
0 output buffer failures, 0 output buffers swapped out
R2#

R3 (Interface Configuration):

```
R3# conf t
R3(config)# int f1/0
R3(config-if)# ip add 10.0.0.3 255.0.0.0
R3(config-if)# no sh
R3(config-if)# ip ospf 1 area 0
R3(config-if)# exit
R3(config)# int f1/1
R3(config-if)# ip add 192.168.1.3 255.255.255.0
R3(config-if)# no sh
R3(config-if)# ip ospf 1 area 0
R3(config-if)# exit
R3(config)# int g0/0
R3(config-if)# ip add 12.0.0.1 255.0.0.0
R3(config-if)# no sh
R3(config-if)# ip ospf 1 area 0
R3(config-if)# exit
R3(config)# exit
R3# wr me
```


R3
R3#show interfaces g0/0
GigabitEthernet0/0 is up, line protocol is up
Hardware is i82543 (Livengood), address is ca03.0808.0008 (bia ca03.0808.0008)
Internet address is 23.0.0.3/8
MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Full-duplex, 1000Mb/s, link type is autonegotiation, media type is SX
output flow-control is XON, input flow-control is XON
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:05, output 00:00:04, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
3093 packets input, 302609 bytes, 0 no buffer
Received 1669 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 watchdog, 0 multicast, 0 pause input
0 input packets with dribble condition detected
3137 packets output, 306681 bytes, 0 underruns
0 output errors, 0 collisions, 1 interface resets
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier, 0 pause output
0 output buffer failures, 0 output buffers swapped out
R3#

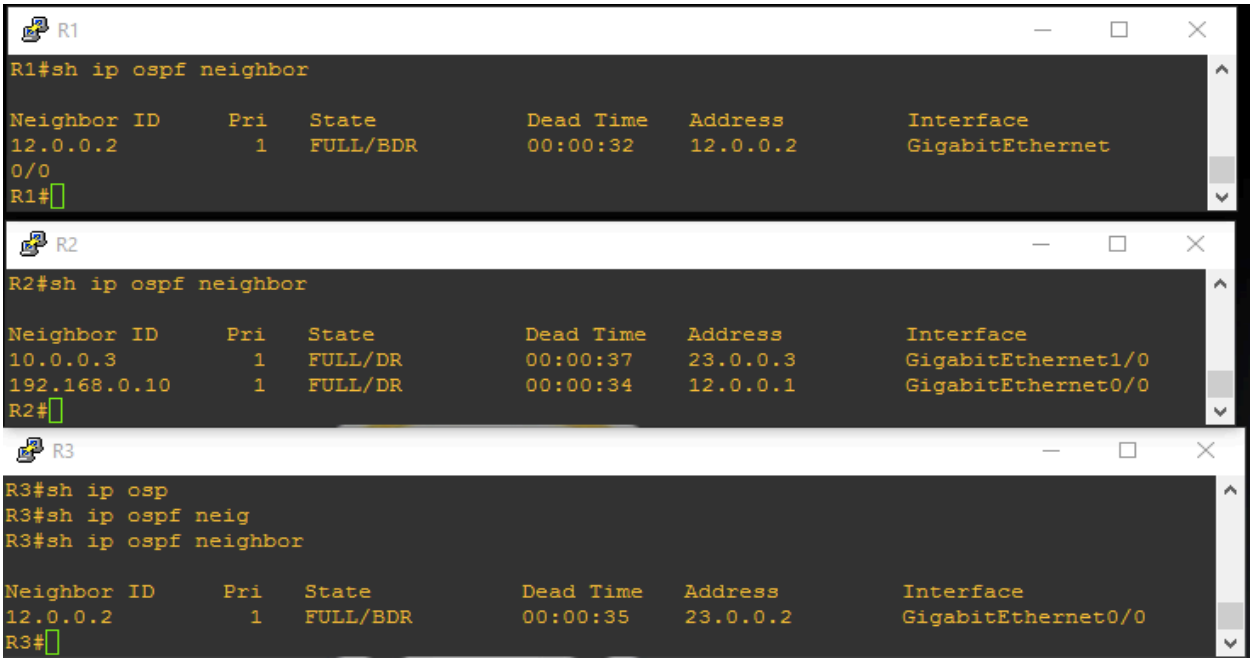

R3
R3#show interfaces f1/0
FastEthernet1/0 is up, line protocol is up
Hardware is i82543 (Livengood), address is ca03.0808.001c (bia ca03.0808.001c)
Internet address is 10.0.0.3/8
MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Full-duplex, 100Mb/s, 100BaseTX/FX
ARP type: ARPA, ARP Timeout 04:00:00
Last input never, output 00:00:00, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
0 packets input, 0 bytes
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 watchdog
0 input packets with dribble condition detected
3095 packets output, 294970 bytes, 0 underruns
0 output errors, 0 collisions, 1 interface resets
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out
R3#
R3#


R3
R3#show interfaces f1/1
FastEthernet1/1 is up, line protocol is up
Hardware is i82543 (Livengood), address is ca03.0808.001d (bia ca03.0808.001d)
Internet address is 192.168.1.3/24
MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Full-duplex, 100Mb/s, 100BaseTX/FX
ARP type: ARPA, ARP Timeout 04:00:00
Last input 03:00:56, output 00:00:00, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
34 packets input, 3196 bytes
Received 4 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 watchdog
0 input packets with dribble condition detected
3120 packets output, 297158 bytes, 0 underruns
0 output errors, 0 collisions, 1 interface resets
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out
R3#
R3#

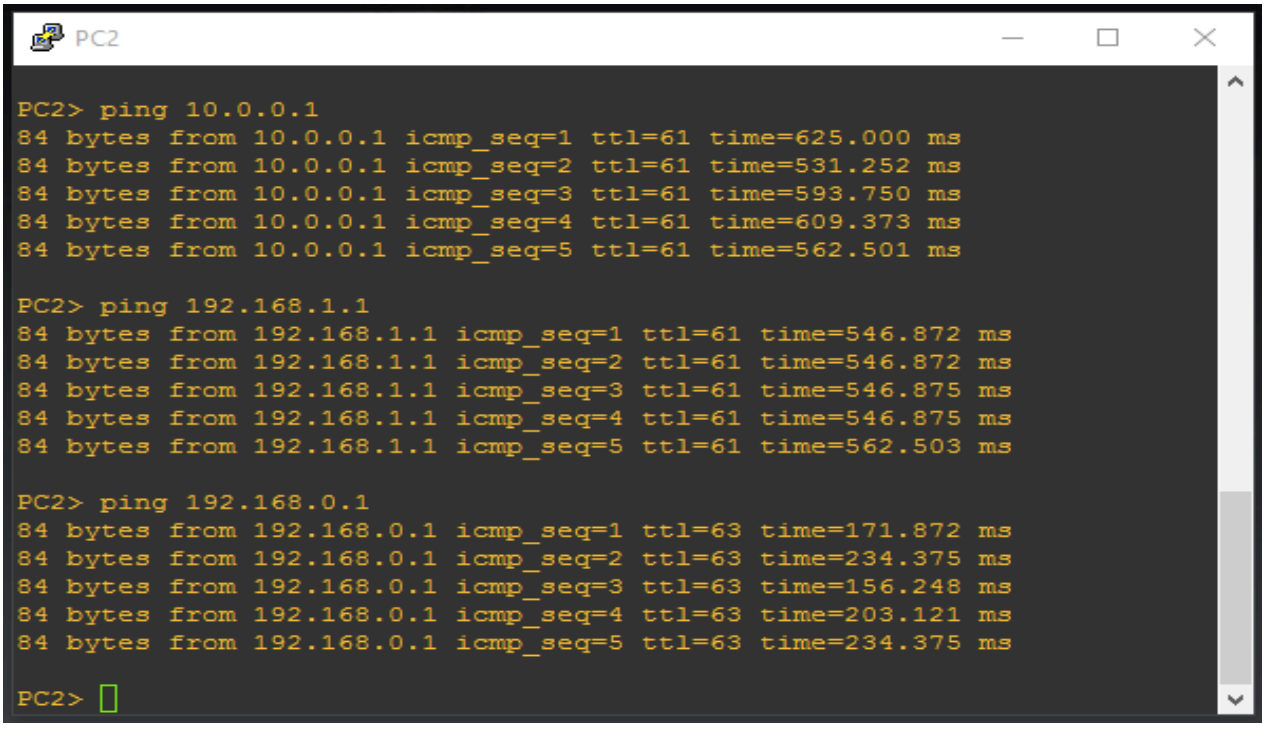
Step 3: Checking Network Connectivity

We configured ospf for network connectivity.

Following screenshot shows the ospf neighbor of each router:



Network Connectivity:



Step 4: Configuring IKE & IPSec

- Configure ISAKMP
- Create Crypto ACL
- Define Transform Sets
- Create Crypto map entries
- Set global lifetime for IPSec Sa
- Apply crypto map to the interfaces

Step 1:

R1 Configuration:

R1# conf t

R1(config)# crypto isakmp policy 1

R1(config-isakmp)# authentication pre-share

R1(config-isakmp)# encryption des

R1(config-isakmp)# group 2

R1(config-isakmp)# hash md5

R1(config-isakmp)# exit

R1(config)# crypto isakmp key cisco123 address 23.0.0.3

R3 Configuration:

R3# conf t

R3(config)# crypto isakmp policy 1

R3(config-isakmp)# authentication pre-share

R3(config-isakmp)# encryption des

R3(config-isakmp)# group 2

R3(config-isakmp)# hash md5

R3(config-isakmp)# exit

R3(config)# crypto isakmp key cisco123 address 12.0.0.1

Step 2:

R1 Configuration:

```
R1(config)# crypto ipsec transform-set TR_SET esp-3des esp-md5-hmac
R1(cfg-crypto-trans)# exit
R1(config)#
```

R3 Configuration:

```
R3(config)# crypto ipsec transform-set TR_SET esp-3des esp-md5-hmac
R3(cfg-crypto-trans)# exit
R3(config)#
```

Step 3:

R1 Configuration:

```
R1(config)# access-list 101 permit ip host 192.168.0.1 host 192.168.1.1
R1(config)# crypto map cmap 1 ipsec-isakmp
R1(config-crypto-map)# set peer 23.0.0.3
R1(config-crypto-map)# set transform-set TR_SET
R1(config-crypto-map)# match address 101
R1(config-crypto-map)# exit
R1(config)# interface g0/0
R1(config-if)# crypto map cmap
R1(config-if)# exit
R1(config)#
```

R3 Configuration:

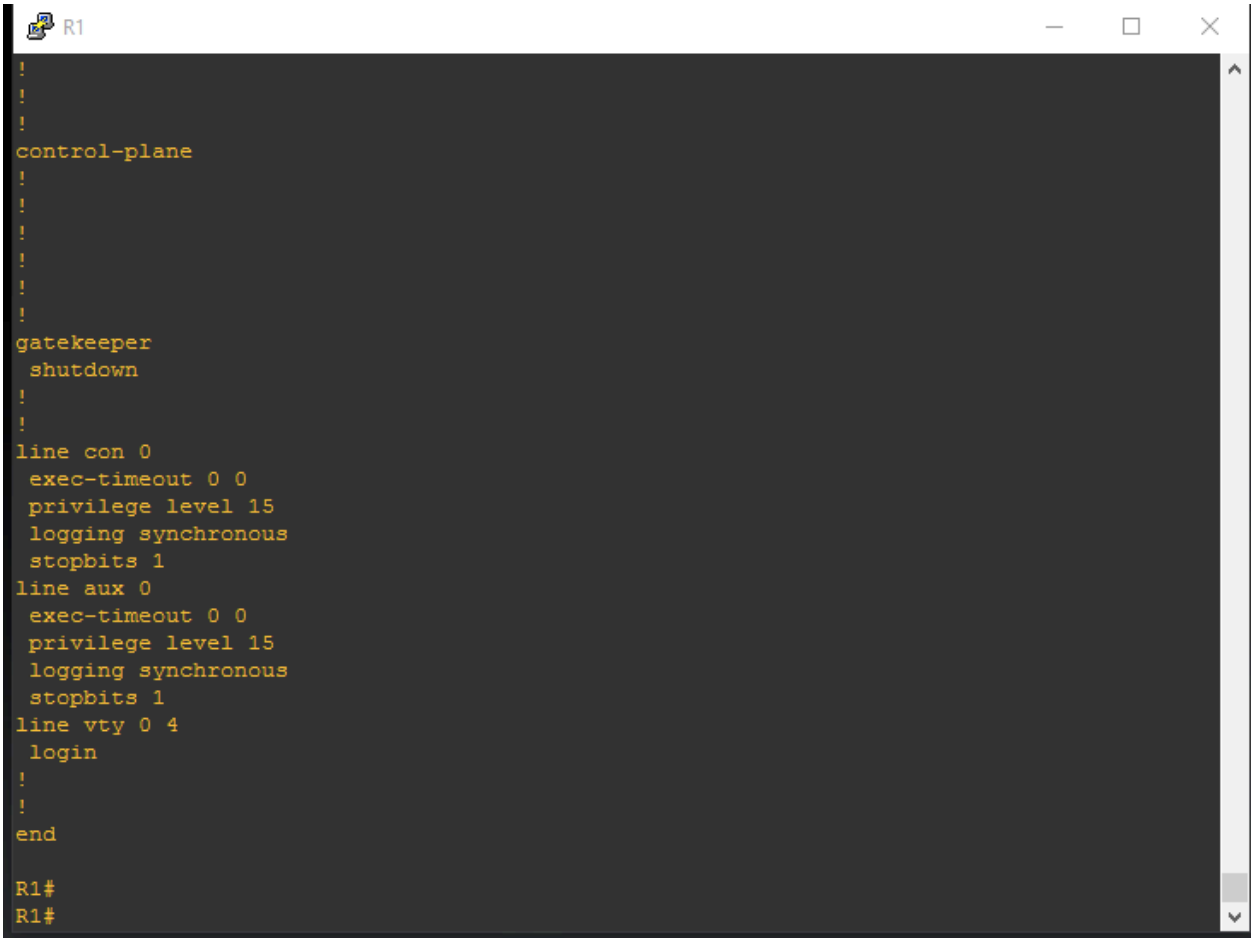
```
R3(config)# access-list 101 permit ip host 192.168.1.1 host 192.168.0.1
R3(config)# crypto map cmap 1 ipsec-isakmp
R3(config-crypto-map)# set peer 12.0.0.1
R3(config-crypto-map)# set transform-set TR_SET
R3(config-crypto-map)# match address 101
R3(config-crypto-map)# exit
R3(config)# interface g0/0
R3(config-if)# crypto map cmap
R3(config-if)# exit
R3(config)#
```

Step 5: Screenshots

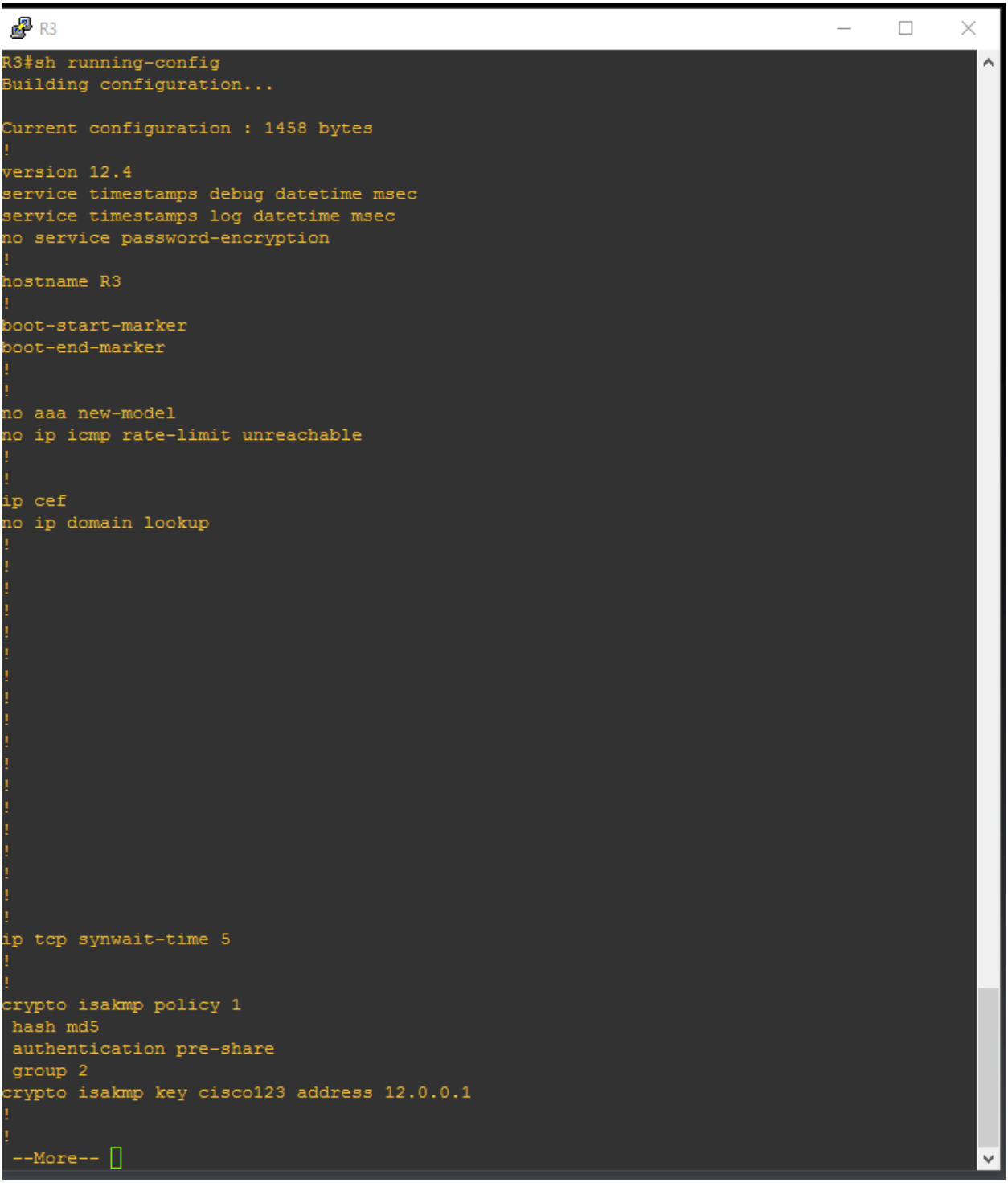
1. Output of Configuration File on both cisco devices i.e. for R1 and R3:

- Router 1 [R1]:

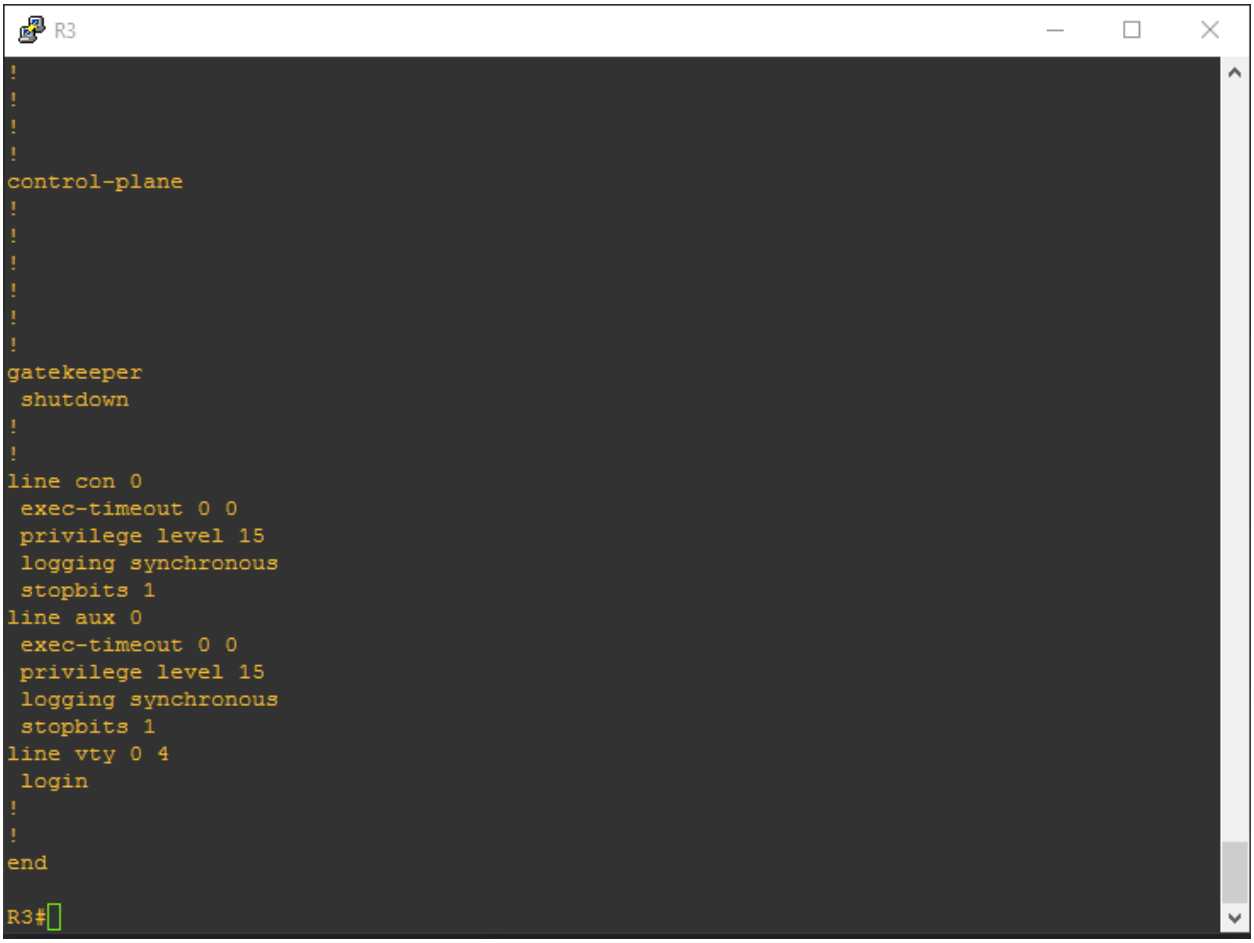

R1
!
!
crypto ipsec transform-set TR_SET esp-3des esp-md5-hmac
!
crypto map cmap 1 ipsec-isakmp
 set peer 23.0.0.3
 set transform-set TR_SET
 match address 101
!
!
!
!
interface Ethernet0/0
 no ip address
 shutdown
 duplex auto
!
interface GigabitEthernet0/0
 ip address 12.0.0.1 255.0.0.0
 ip ospf 1 area 0
 duplex full
 speed 1000
 media-type gbic
 negotiation auto
 crypto map cmap
!
interface FastEthernet1/0
 ip address 192.168.0.10 255.255.255.0
 ip ospf 1 area 0
 duplex auto
 speed auto
!
interface FastEthernet1/1
 ip address 172.16.0.10 255.255.0.0
 ip ospf 1 area 0
 duplex auto
 speed auto
!
router ospf 1
 log-adjacency-changes
!
!
no ip http server
no ip http secure-server
!
!
access-list 101 permit ip host 192.168.0.1 host 192.168.1.1
no cdp log mismatch duplex
!
 --More--


R1
!
!
!
control-plane
!
!
!
!
!
!
gatekeeper
 shutdown
!
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 login
!
!
end
R1#
R1#

- Router 3 [R3]:


R3
R3#sh running-config
Building configuration...
Current configuration : 1458 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R3
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
no ip icmp rate-limit unreachable
!
!
ip cef
no ip domain lookup
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
ip tcp synwait-time 5
!
!
crypto isakmp policy 1
 hash md5
 authentication pre-share
 group 2
crypto isakmp key cisco123 address 12.0.0.1
!
!
 --More--


R3
!
!
crypto ipsec transform-set TR_SET esp-3des esp-md5-hmac
!
crypto map cmap 1 ipsec-isakmp
 set peer 12.0.0.1
 set transform-set TR_SET
 match address 101
!
!
!
!
interface Ethernet0/0
 no ip address
 shutdown
 duplex auto
!
interface GigabitEthernet0/0
 ip address 23.0.0.3 255.0.0.0
 ip ospf 1 area 0
 duplex full
 speed 1000
 media-type gbic
 negotiation auto
 crypto map cmap
!
interface FastEthernet1/0
 ip address 10.0.0.3 255.0.0.0
 ip ospf 1 area 0
 duplex auto
 speed auto
!
interface FastEthernet1/1
 ip address 192.168.1.3 255.255.255.0
 ip ospf 1 area 0
 duplex auto
 speed auto
!
router ospf 1
 log-adjacency-changes
!
!
no ip http server
no ip http secure-server
!
!
access-list 101 permit ip host 192.168.1.1 host 192.168.0.1
no cdp log mismatch duplex
!
!
 --More--


R3
!
!
!
!
control-plane
!
!
!
!
!
!
gatekeeper
 shutdown
!
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 login
!
!
end
R3#

2. Output of **debug crypto isakmp** and **debug crypto ipsec** on both cisco devices i.e. for R1 and R3

R1: <**debug crypto isakmp**>

R1: <**debug crypto ipsec**>

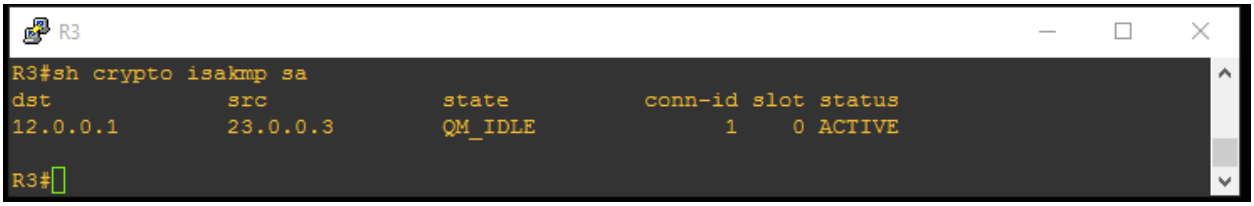
R3: <**debug crypto isakmp**>

R3: <**debug crypto ipsec**>

3. Output of **show crypto isakmp sa** for both cisco devices

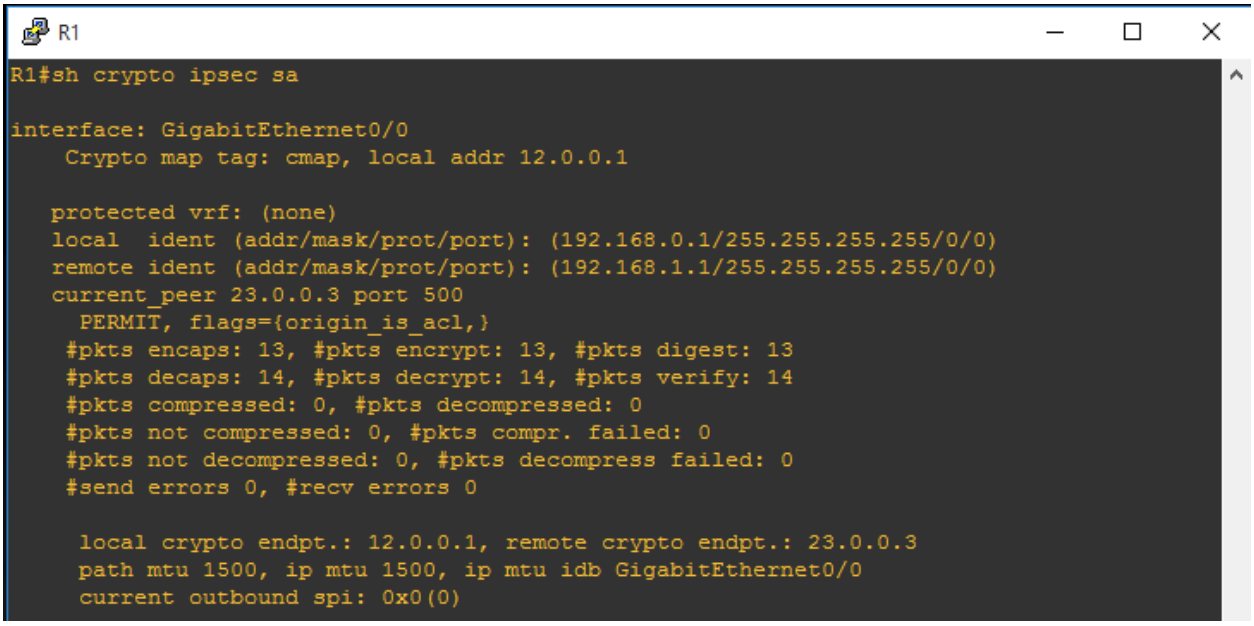
R1:

R3:



4. Output of **show crypto ipsec sa** for both cisco devices i.e. for R1 and R3

R1:



R3: