Today's Task

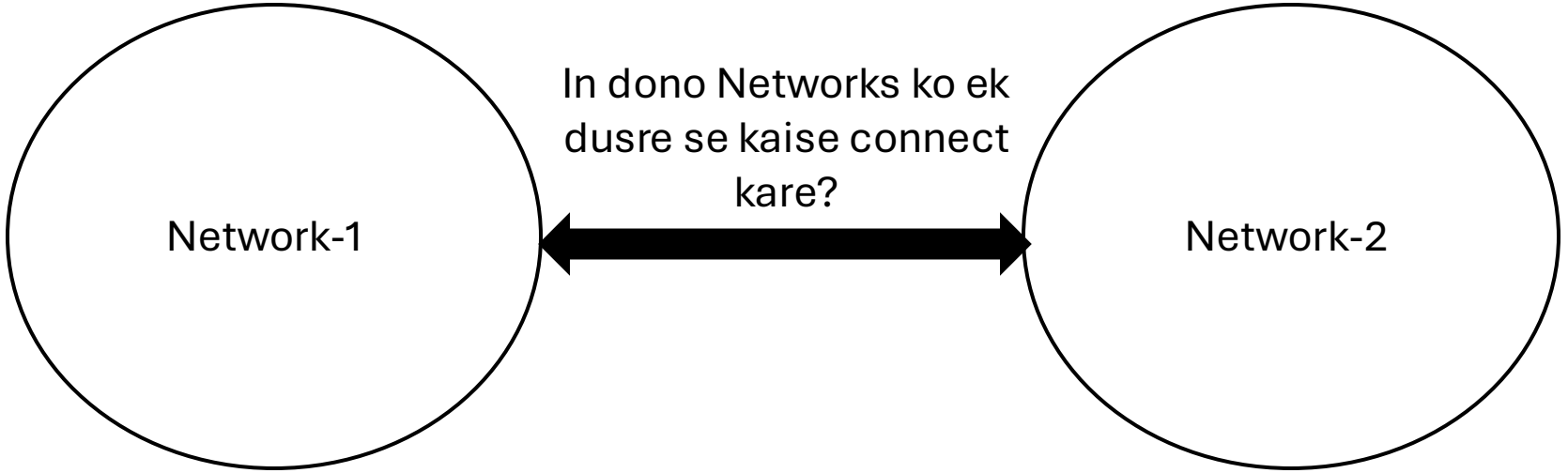
Task 1: Subnetting on GNS 3

Task 2: IPsec site to site VPN

Task 1: Subnetting on GNS 3

- **Subnetting in computer** networks is the **process of dividing a large network** (such as a class A, B, or C network) **into smaller**, more manageable **sub-networks**, called **subnets.**

Problem Statement:



What we need?

4x 

VPCS

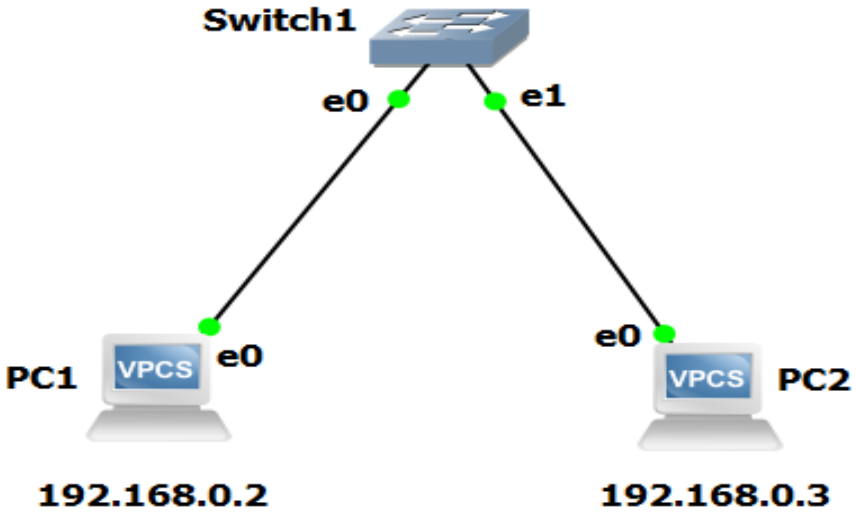
2x 

Electronic Switch

1x 

C3725

Step-1: e0= Ethernet 0
e1= Ethernet 1



Network 1
(Students)

Step-2: Assigning the given IP to PC1 and PC2.

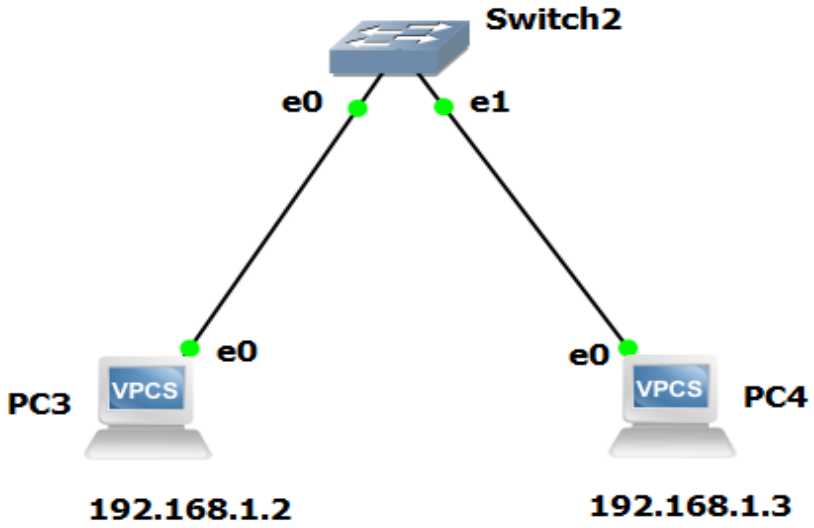
PC1 Console

```
PC1> sh ip

NAME        : PC1[1]
IP/MASK     : 0.0.0.0/0
GATEWAY     : 0.0.0.0
DNS         :
MAC         : 00:50:79:66:68:00
LPORT       : 10020
RHOST:PORT  : 127.0.0.1:10021
MTU:        : 1500

PC1> ip 192.168.0.2
Checking for duplicate address...
PC1 : 192.168.0.2 255.255.255.0
```

PC2 Console

```
PC2> sh ip

NAME        : PC2[1]
IP/MASK     : 0.0.0.0/0
GATEWAY     : 0.0.0.0
DNS         :
MAC         : 00:50:79:66:68:01
LPORT       : 10006
RHOST:PORT  : 127.0.0.1:10007
MTU:        : 1500

PC2> ip 192.168.0.3
Checking for duplicate address...
PC1 : 192.168.0.3 255.255.255.0
```

Step-3: e0= Ethernet 0
e1= Ethernet 1



Network 2
(Staffs)

Step-4: Assigning the given IP to PC3 and PC4.

PC3 Console

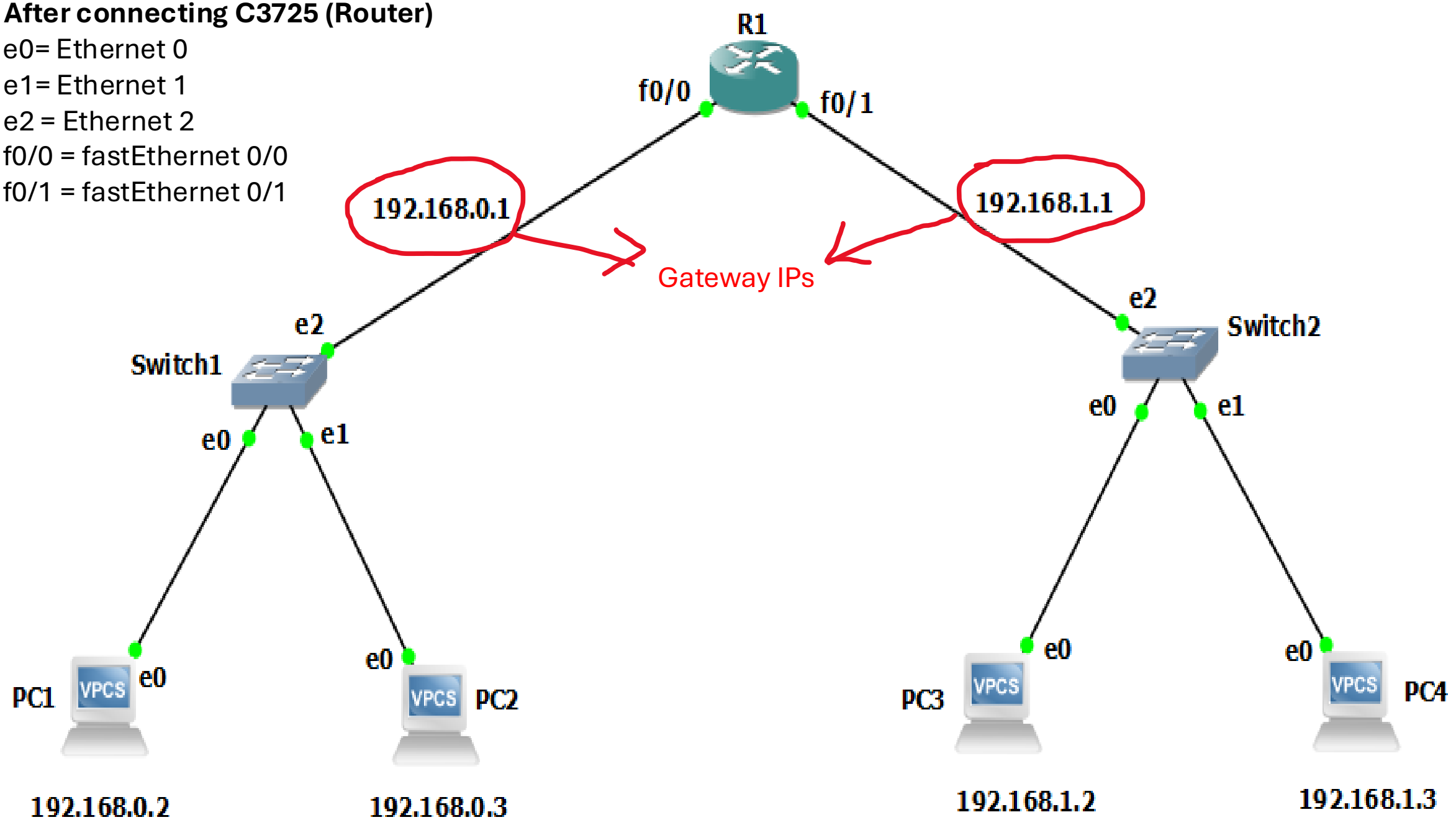
```
PC3> sh ip

NAME        : PC3[1]
IP/MASK     : 0.0.0.0/0
GATEWAY     : 0.0.0.0
DNS         :
MAC         : 00:50:79:66:68:02
LPORT       : 10012
RHOST:PORT  : 127.0.0.1:10013
MTU:        : 1500

PC3> ip 192.168.1.2
Checking for duplicate address...
PC1 : 192.168.1.2 255.255.255.0
```

PC4 Console

```
PC4> sh ip

NAME        : PC4[1]
IP/MASK     : 0.0.0.0/0
GATEWAY     : 0.0.0.0
DNS         :
MAC         : 00:50:79:66:68:03
LPORT       : 10014
RHOST:PORT  : 127.0.0.1:10015
MTU:        : 1500

PC4> ip 192.168.1.3
Checking for duplicate address...
PC1 : 192.168.1.3 255.255.255.0
```

Step-5: After connecting C3725 (Router)

e0= Ethernet 0
e1= Ethernet 1
e2 = Ethernet 2
f0/0 = fastEthernet 0/0
f0/1 = fastEthernet 0/1



Step-6: *R1 Console*

```
enable
sh run
q
conf t
int f0/0
ip address 192.168.0.1 255.255.255.0
no sh
exit
int f0/1
ip address 192.168.1.1 255.255.255.0
no sh
exit
do wr
exit
exit
write mem
```

```
R1#enable
R1#sh run
Building configuration...

Current configuration : 1465 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
!
!
!
!
no ip domain lookup

R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#int f0/0
R1(config-if)#ip address 192.168.0.1 255.255.255.0
R1(config-if)#no sh
R1(config-if)#exit
*Mar  1 00:03:54.747: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar  1 00:03:55.747: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to
 up
R1(config-if)#exit
R1(config)#do wr
Building configuration...
[OK]
R1(config)#exit
R1#
*Mar  1 00:04:30.863: %SYS-5-CONFIG_I: Configured from console by console
R1#write mem
Building configuration...
[OK]
```

Step-7:

PC1 Console

```
ip 192.168.0.2 255.255.255.0 192.168.0.1
```

```
PC1> ip 192.168.0.2 /24 192.168.0.1
Checking for duplicate address...
PC1 : 192.168.0.2 255.255.255.0 gateway 192.168.0.1
```

PC2 Console

```
ip 192.168.0.3 255.255.255.0 192.168.0.1
```

```
PC2> ip 192.168.0.3 /24 192.168.0.1
Checking for duplicate address...
PC1 : 192.168.0.3 255.255.255.0 gateway 192.168.0.1
```

PC3 Console

```
ip 192.168.1.2 255.255.255.0 192.168.1.1
```

```
PC3> ip 192.168.1.2 /24 192.168.1.1
Checking for duplicate address...
PC1 : 192.168.1.2 255.255.255.0 gateway 192.168.1.1
```

PC4 Console

```
ip 192.168.1.3 255.255.255.0 192.168.1.1
```

```
PC4> ip 192.168.1.3 /24 192.168.1.1
Checking for duplicate address...
PC1 : 192.168.1.3 255.255.255.0 gateway 192.168.1.1
```

ALL SET

Additional

Dynamic Host Configuration Protocol (DHCP):

It provides an Internet Protocol (IP) host with its IP address.

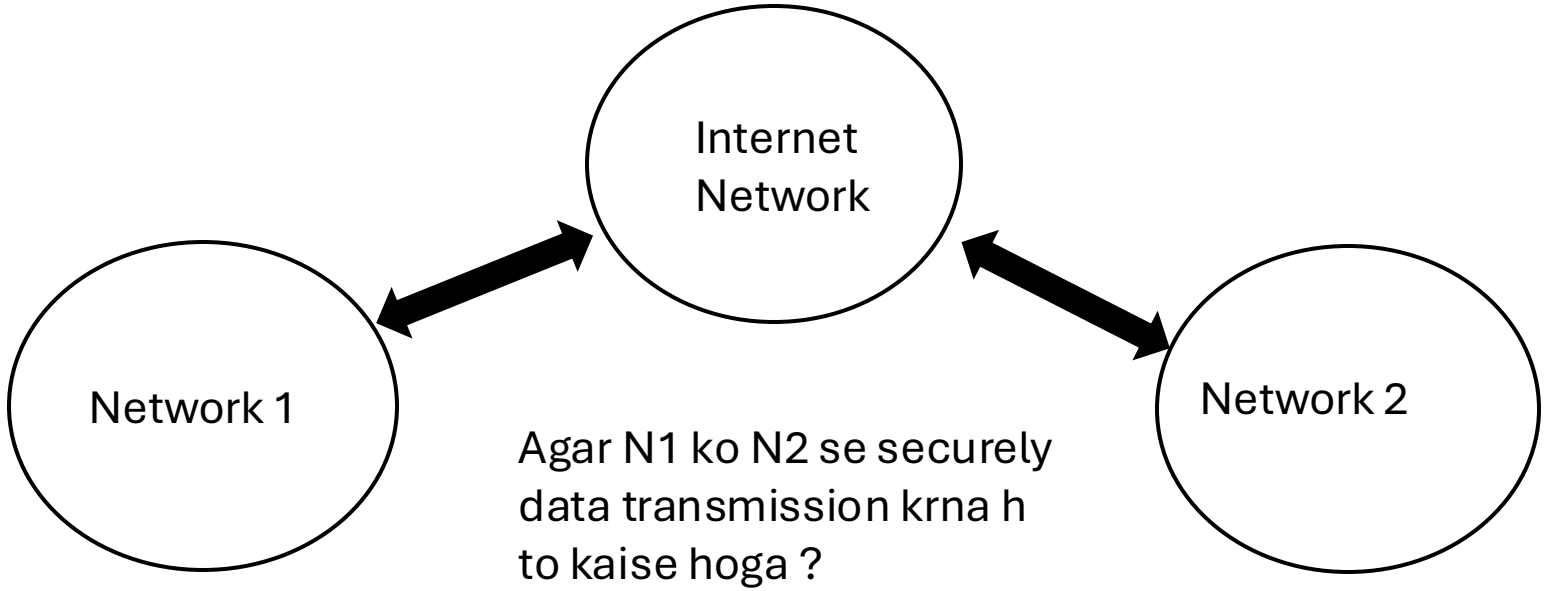
```
*R1 Console*
enable
sh run
q
conf t
ip dhcp pool students
network 192.168.0.0 255.255.255.0
default-router 192.168.0.1
dns-server 8.8.8.8
exit
ip dhcp pool staff
network 192.168.1.0 255.255.255.0
default-router 192.168.1.1
dns-server 8.8.8.8
exit
do wr
exit
write mem
```

```
R1#enable
R1#sh run
Building configuration...

Current configuration : 1478 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
!
!
!
!
no ip domain lookup

R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip dhcp pool students
R1(dhcp-config)#network 192.168.0.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.0.1
R1(dhcp-config)#dns-server 8.8.8.8
R1(dhcp-config)#exit
R1(config)#ip dhcp pool staff
R1(dhcp-config)#network 192.168.1.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.1.1
R1(dhcp-config)#dns-server 8.8.8.8
R1(dhcp-config)#exit
R1(config)#do wr
Building configuration...
[OK]
R1(config)#exit
R1#
*Mar  1 00:36:57.475: %SYS-5-CONFIG_I: Configured from console by console
R1#write mem
Building configuration...
[OK]
```

Task 2: IPSec Site to Site VPN

- **Site to Site IPSec VPN Tunnels** are used to allow the **secure transmission** of data, voice and video between two sites(e.g. offices or branches). The VPN tunnel is created over the Internet public network and **encrypted using a number of advanced encryption algorithms** to provide confidentiality of the data transmitted between the two sites.

Problem Statement:



What we need?

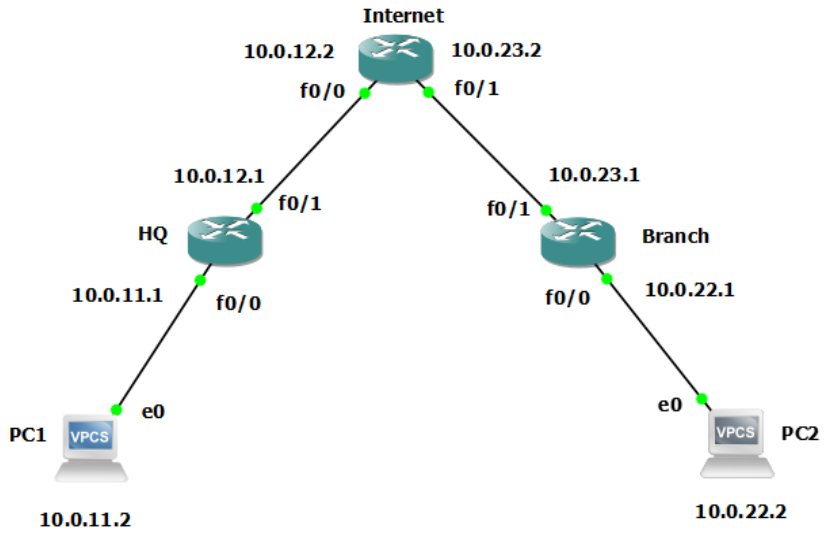
2x 

VPCS

3x 

C3725

Step-1: Configuration of PCs – PC1 and PC2




```
PC1> ip 10.0.11.2 255.255.255.0 10.0.11.1
Checking for duplicate address...
PC1 : 10.0.11.2 255.255.255.0 gateway 10.0.11.1
```

```
PC2> ip 10.0.22.2 255.255.255.0 10.0.22.1
Checking for duplicate address...
PC1 : 10.0.22.2 255.255.255.0 gateway 10.0.22.1
```

Step-2: Configuration of Router HQ

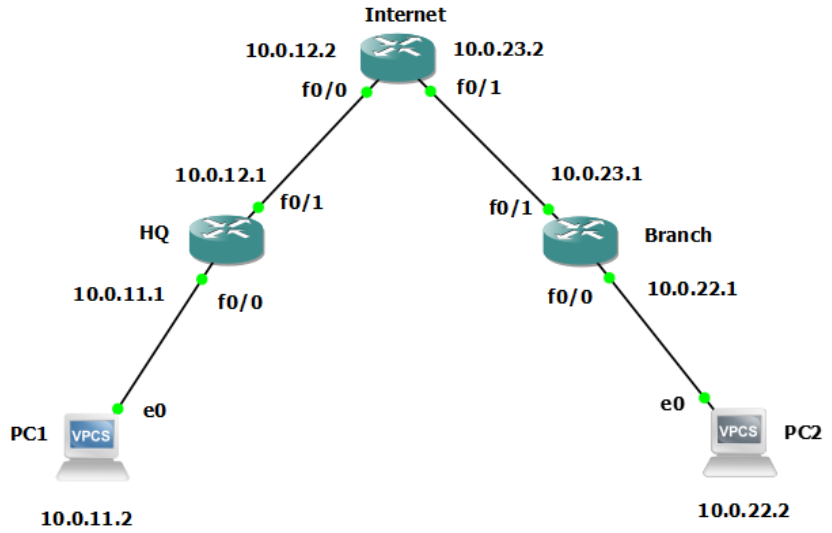
Configuring EIGRP (Enhanced Interior Gateway Routing Protocol) :

- The command router eigrp 1 starts the EIGRP process with the Autonomous System (AS) number 1.
- The command network 0.0.0.0 is used to include all directly connected networks in the EIGRP process.

```
HQ#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
HQ(config)#int f0/0
HQ(config-if)#ip address 10.0.11.1 255.255.255.0
HQ(config-if)#no shut
HQ(config-if)#e
*Mar  1 00:07:55.079: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar  1 00:07:56.079: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state
 to up
HQ(config-if)#exit
HQ(config)#int f0/1
HQ(config-if)#ip address 10.0.12.1 255.255.255.0
HQ(config-if)#no shut
HQ(config-if)#
*Mar  1 00:08:56.835: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
*Mar  1 00:08:57.835: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state
 to up
HQ(config-if)#exit
HQ(config)#router eigrp 1
HQ(config-router)#network 0.0.0.0
HQ(config-router)#exit
HQ(config)#exit
HQ#wr
*Mar  1 00:09:50.495: %SYS-5-CONFIG_I: Configured from console by console
HQ#wr
Building configuration...
[OK]
HQ#wr
Building configuration...
[OK]
HQ#
```

Step-3: Configuration of Router Internet.

```
et1/0, changed state to down
Internet#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Internet(config)#int f0/0
Internet(config-if)#ip address 10.0.12.2 255.255.255.0
Internet(config-if)#no shut
Internet(config-if)#
*Mar  1 00:11:32.899: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar  1 00:11:33.899: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state
 to up
Internet(config-if)#exit
Internet(config)#int f0/1
Internet(config-if)#ip address 10.0.23.2 255.255.255.0
Internet(config-if)#no shut
Internet(config-if)#exi
*Mar  1 00:12:06.867: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
*Mar  1 00:12:07.867: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state
 to up
Internet(config-if)#exit
Internet(config)#router eigrp 1
Internet(config-router)#network 0.0.0.0
Internet(config-router)#
*Mar  1 00:12:31.847: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 10.0.12.1 (FastEthernet0/0) is up:
new adjacency
Internet(config-router)#exit
Internet(config)#exit
Internet#
*Mar  1 00:12:37.843: %SYS-5-CONFIG_I: Configured from console by console
Internet#wr
Building configuration...
[OK]
Internet#
```



Step-4: Configuration of Router Branch

```
et0/0, changed state to down
Branch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Branch(config)#int f0/1
Branch(config-if)#ip address 10.0.23.1 255.255.255.0
Branch(config-if)#no shut
Branch(config-if)#
*Mar  1 00:12:55.099: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
*Mar  1 00:12:56.099: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state
 to up
Branch(config-if)#exit
Branch(config)#int f0/0
Branch(config-if)#ip address 10.0.22.1 255.255.255.0
Branch(config-if)#no shut
Branch(config-if)#
*Mar  1 00:13:25.455: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar  1 00:13:26.455: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state
 to up
Branch(config-if)#exit
Branch(config)#router eigrp 1
Branch(config-router)#network 0.0.0.0
Branch(config-router)#
*Mar  1 00:13:48.495: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 10.0.23.2 (FastEthernet0/1) is up:
new adjacency
Branch(config-router)#exit
Branch(config)#exit
Branch#wr
Building configuration...

*Mar  1 00:13:58.915: %SYS-5-CONFIG_I: Configured from console by console[OK]
Branch#
```

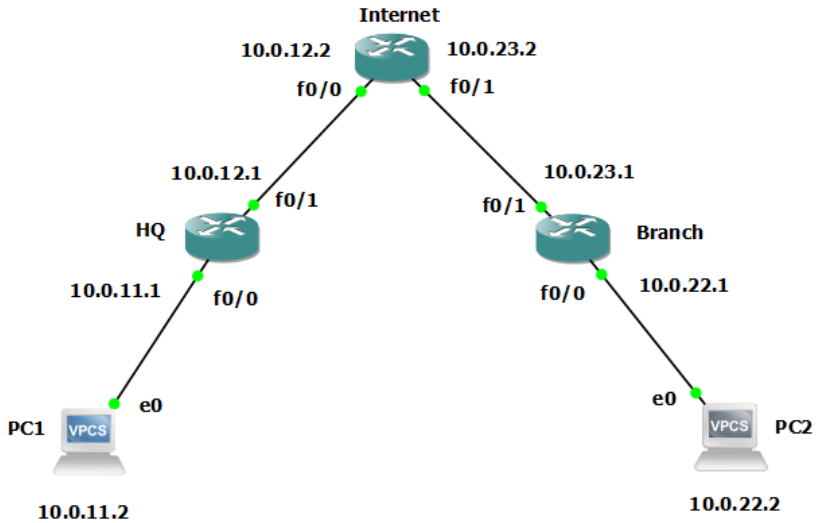
Configuring EIGRP (Enhanced Interior Gateway Routing Protocol) :

- The command router eigrp 1 starts the EIGRP process with the Autonomous System (AS) number 1.
- The command network 0.0.0.0 is used to include all directly connected networks in the EIGRP process.

Step-5: Check configuration working or not.

So we will try to ping PC1 with PC2

```
PC1> ping 10.0.22.2
10.0.22.2 icmp_seq=1 timeout
84 bytes from 10.0.22.2 icmp_seq=2 ttl=61 time=91.869 ms
84 bytes from 10.0.22.2 icmp_seq=3 ttl=61 time=94.326 ms
84 bytes from 10.0.22.2 icmp_seq=4 ttl=61 time=96.520 ms
84 bytes from 10.0.22.2 icmp_seq=5 ttl=61 time=78.437 ms
```



Step-6: Configuration of IPSec VPN Tunnel

- **HQ Router**

```
HQ#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
HQ(config)#crypto isakmp policy 1
HQ(config-isakmp)#encryption aes 128
HQ(config-isakmp)#authentication pre-share
HQ(config-isakmp)#group 2
HQ(config-isakmp)#hash sha
HQ(config-isakmp)#crypto isakmp key 6 referux123 address 0.0.0.0
HQ(config)#crypto ipsec transform-set OUR-SET esp-aes 128 esp-sha-hmac
HQ(cfg-crypto-trans)#exit
HQ(config)#ip access-list extended 100
HQ(config-ext-nacl)#permit ip 10.0.11.0 0.0.0.255 10.0.22.0 0.0.0.255
HQ(config-ext-nacl)#exit
HQ(config)#crypto map OUR-MAP 1 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
HQ(config-crypto-map)#match address 100
HQ(config-crypto-map)#set peer 10.0.23.1
HQ(config-crypto-map)#set transform-set OUR-SET
HQ(config-crypto-map)#exit
HQ(config)#int f0/1
HQ(config-if)#crypto map OUR-MAP
HQ(config-if)#
*Mar  1 00:28:04.023: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
HQ(config-if)#end
HQ#
*Mar  1 00:28:12.007: %SYS-5-CONFIG_I: Configured from console by console
HQ#wr
Building configuration...
[OK]
```

If you want to understand each of the command, then go to next page where we explained with the analogy of "Setting up a secure gate system."

Consider setting up a Secure Gate System

conf t (Enter Configuration Mode)
Analogy: You are entering the control room to configure the security system.

crypto isakmp policy 1 (Create ISAKMP Policy)
Analogy: You are setting up a rule for the way people will enter the building, like deciding that people can only use an ID card to enter.

encryption aes 128 (Set Encryption)
Analogy: You install a lock on the gate that uses a complex, 128-bit combination.

authentication pre-share (Use Pre-Shared Key for Authentication)
Analogy: The gate will require people to know a shared password to enter.

group 2 (Use Diffie-Hellman Group 2)
Analogy: This defines the complexity of the key exchange mechanism, like deciding how strong and long the key for the gate's lock will be.

hash sha (Use SHA for Integrity)
Analogy: When someone uses the gate, they must leave a fingerprint to verify that nothing has been tampered with.

crypto isakmp key 6 referux123 address 0.0.0.0 (Set Pre-shared Key for ISAKMP)
Analogy: You create a master key (referux123) that anyone trying to enter must know, and it will work for everyone (since 0.0.0.0 represents all possible users).

crypto ipsec transform-set OUR-SET esp-aes 128 esp-sha-hmac (Create IPSec Transform Set)
Analogy: You are configuring how people must communicate through the gate – they must speak a secret code (AES encryption) and use a special handshake (SHA HMAC).

ip access-list extended 100 (Create Access Control List)
Analogy: You are creating a list of approved people (addresses) who can pass through the gate.

permit ip 10.0.11.0 0.0.0.255 10.0.22.0 0.0.0.255 (Permit Traffic Between Networks)
Analogy: You allow people from the 10.0.11.x group to enter and communicate with the 10.0.22.x group.

crypto map OUR-MAP 1 ipsec-isakmp (Create Crypto Map)
Analogy: You are setting up a special path (crypto map) that uses the secure gate (IPSec) to allow people to pass through.

match address 100 (Match ACL 100 to Crypto Map)
Analogy: You tell the system to only let people on the approved guest list (Access Control List 100) use the secure path.

set peer 10.0.23.1 (Set Peer Address for VPN)
Analogy: You tell the security system who to expect as the guest at the gate (peer 10.0.23.1).

set transform-set OUR-SET (Set Transform Set for Crypto Map)
Analogy: You specify the secret code (OUR-SET) that must be used to communicate through the gate.

int f0/1 (Enter Interface FastEthernet 0/1 Configuration Mode)
Analogy: You choose which gate (interface) will be used for the secure communication.

crypto map OUR-MAP (Apply Crypto Map to Interface)
Analogy: You attach the security rules (OUR-MAP) to this specific gate, so anyone passing through must follow those rules.

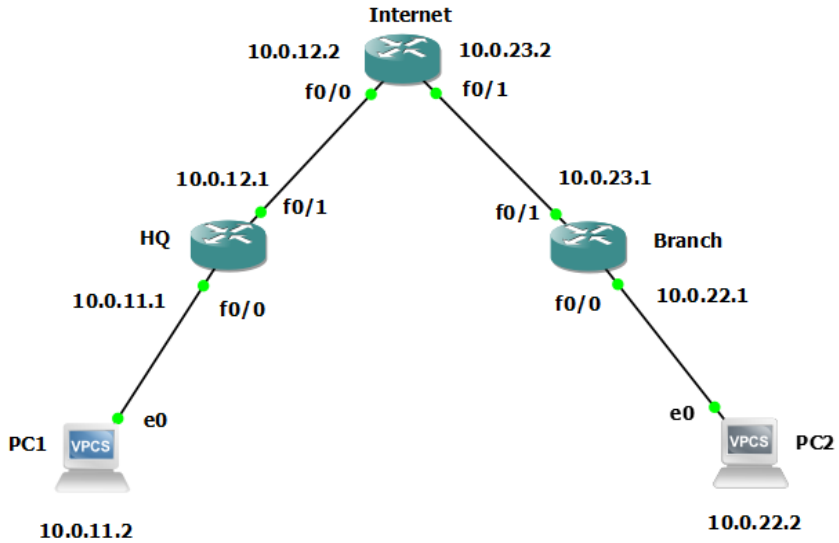
end (Exit Configuration Mode)
Analogy: You leave the control room after setting up the entire security system.

wr (Save the Configuration)
Analogy: You press "Save" to ensure all your gate settings are permanent and won’t be lost.

Step-7: Configuration of IPSec VPN Tunnel

- **Branch Router**

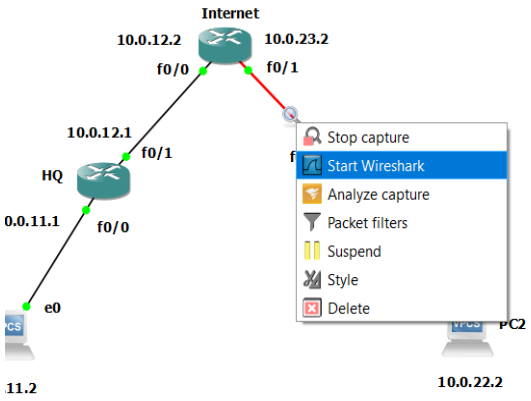
```
Branch#conf t
Branch(config)#
*Mar  1 00:57:52.287: %CRYPTO-6-IKMP_MODE_FAILURE: Processing of Quick mode fail
ed with peer at 10.0.12.1
Branch(config)#crypto isakmp enable
Branch(config)#crypto isakmp policy 1
Branch(config-isakmp)#encryption aes 128
Branch(config-isakmp)#authentication pre-share
Branch(config-isakmp)#group 2
Branch(config-isakmp)#hash sha
Branch(config-isakmp)#exit
Branch(config)#ip access-list extended 100
Branch(config-ext-nacl)#permit ip 10.0.22.0 0.0.0.255 10.0.11.0 0.0.0.255
Branch(config-ext-nacl)#exit
Branch(config)#crypto map OUR-MAP 1 ipsec-isakmp
Branch(config-crypto-map)#match address 100
Branch(config-crypto-map)#set peer 10.0.12.1
Branch(config-crypto-map)#set transform-set OUR-SET
Branch(config-crypto-map)#exit
Branch(config)#int f0/1
Branch(config-if)#crypto map OUR-MAP
Branch(config-if)#end
Branch#
*Mar  1 01:01:00.299: %SYS-5-CONFIG_I: Configured from console by console
Branch#wr
Building configuration...
[OK]
Branch#
```

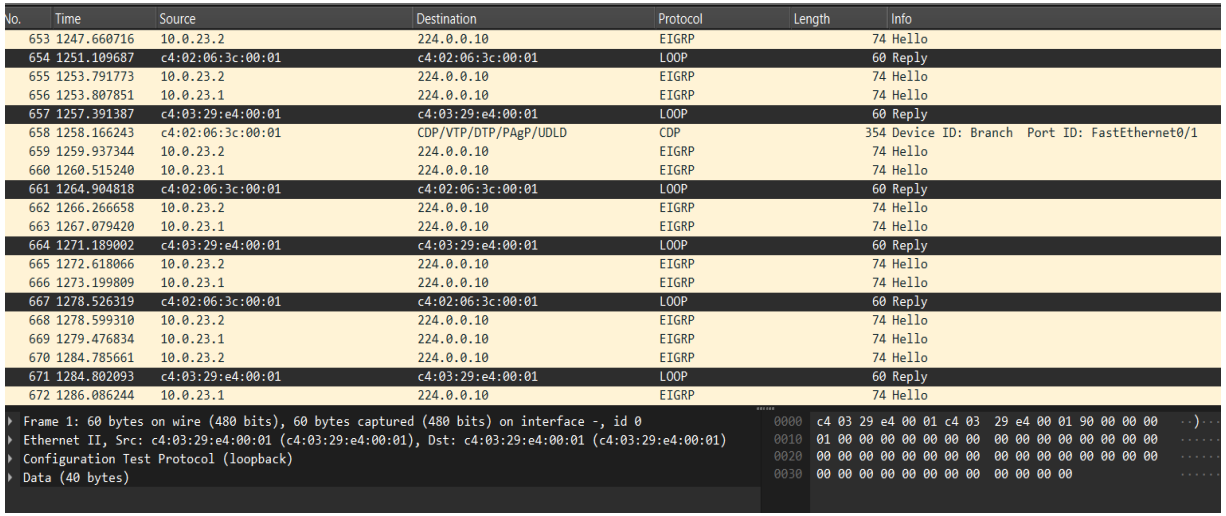


OUTPUT

Last Step: Traffic Analysis from Internet to Branch Routers

- Right click on wire(from Intenet to Branch) and start wireshark.





No.	Time	Source	Destination	Protocol	Length	Info
653	1247.660716	10.0.23.2	224.0.0.10	EIGRP	74	Hello
654	1251.109687	c4:02:06:3c:00:01	c4:02:06:3c:00:01	LOOP	60	Reply
655	1253.791773	10.0.23.2	224.0.0.10	EIGRP	74	Hello
656	1253.807851	10.0.23.1	224.0.0.10	EIGRP	74	Hello
657	1257.391387	c4:03:29:e4:00:01	c4:03:29:e4:00:01	LOOP	60	Reply
658	1258.166243	c4:02:06:3c:00:01	CDP/VTP/DTP/PAgP/UDLD	CDP	354	Device ID: Branch Port ID: FastEthernet0/1
659	1259.937344	10.0.23.2	224.0.0.10	EIGRP	74	Hello
660	1260.515240	10.0.23.1	224.0.0.10	EIGRP	74	Hello
661	1264.904818	c4:02:06:3c:00:01	c4:02:06:3c:00:01	LOOP	60	Reply
662	1266.266658	10.0.23.2	224.0.0.10	EIGRP	74	Hello
663	1267.079420	10.0.23.1	224.0.0.10	EIGRP	74	Hello
664	1271.189002	c4:03:29:e4:00:01	c4:03:29:e4:00:01	LOOP	60	Reply
665	1272.618066	10.0.23.2	224.0.0.10	EIGRP	74	Hello
666	1273.199809	10.0.23.1	224.0.0.10	EIGRP	74	Hello
667	1278.526319	c4:02:06:3c:00:01	c4:02:06:3c:00:01	LOOP	60	Reply
668	1278.599310	10.0.23.2	224.0.0.10	EIGRP	74	Hello
669	1279.476834	10.0.23.1	224.0.0.10	EIGRP	74	Hello
670	1284.785661	10.0.23.2	224.0.0.10	EIGRP	74	Hello
671	1284.802093	c4:03:29:e4:00:01	c4:03:29:e4:00:01	LOOP	60	Reply
672	1286.086244	10.0.23.1	224.0.0.10	EIGRP	74	Hello

```
Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface -, id 0
Ethernet II, Src: c4:03:29:e4:00:01 (c4:03:29:e4:00:01), Dst: c4:03:29:e4:00:01 (c4:03:29:e4:00:01)
Configuration Test Protocol (loopback)
Data (40 bytes)
```

```
0000  c4 03 29 e4 00 01 c4 03  29 e4 00 01 90 00 00 00   ··)·····  ·)·····
0010  01 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········  ········
0020  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········  ········
0030  00 00 00 00 00 00 00 00  00 00 00 00               ········  ····
```

If you understood it and It's working
Clap your