NETWORK SECURITY
PROJECT ROUTING / IPSEC

We used our 2 different .pkt to realize the screenshot, that's why sometimes the name of the device are not exactly the same.

1. Configure the VTP into switches (SWD is the server and the others in mode client)

- **Use version 2, domain name and password**
- **Make Show vtp status of each switch(copy screenshot hereafter)..**

SWD :

```
en
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vtp domain labIPSEC
Changing VTP domain name from lol to labIPSEC
Switch(config)#vtp vers 2
Switch(config)#vtp password marion
Setting device VLAN database password to marion
Switch(config)#vtp mode server
Device mode already VTP SERVER.


Switch#show vtp status
VTP Version                     : 2
Configuration Revision          : 1
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 5
VTP Operating Mode              : Server
VTP Domain Name                 : labIPSEC
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Enabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x29 0x8F 0x07 0x5B
0x18 0xF8 0x2C 0x0F
Configuration last modified by 0.0.0.0 at 3-1-93
00:21:10
Local updater ID is 0.0.0.0 (no valid interface found)
```

SWA1 :

```
Switch>
Switch>en
Switch#config t
Enter configuration commands, one per line.  End with
CNTL/Z.
Switch(config)#vtp domain labIPSEC
Changing VTP domain name from NULL to labIPSEC
Switch(config)#vtp vers 2
Switch(config)#vtp password marion
Setting device VLAN database password to marion
Switch(config)#vtp mode client
Setting device to VTP CLIENT mode.
```

```
Switch#show vtp status
VTP Version                     : 2
Configuration Revision          : 1
Maximum VLANs supported locally : 255
Number of existing VLANs        : 5
VTP Operating Mode              : Client
VTP Domain Name                 : labIPSEC
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Enabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x37 0xFD 0x8F 0x83
0xC6 0xEC 0xCC 0x79
Configuration last modified by 0.0.0.0 at 3-1-93
00:28:32
```

SWA2 :

```
SWA2>en
SWA2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
SWA2(config)#vtp domain labIPSEC
Changing VTP domain name from NULL to labIPSEC
SWA2(config)#vtp vers 2
SWA2(config)#vtp password marion
Setting device VLAN database password to marion
SWA2(config)#vtp mode client
Setting device to VTP CLIENT mode.
```

```
Switch#show vtp status
VTP Version                     : 2
Configuration Revision          : 1
Maximum VLANs supported locally : 255
Number of existing VLANs        : 5
VTP Operating Mode              : Client
VTP Domain Name                 : labIPSEC
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Enabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x74 0x5C 0xA6 0xAC
0xDB 0x94 0xDA 0xA9
Configuration last modified by 0.0.0.0 at 3-1-93
00:32:25
```

2. Vlans configuration :

Configure the following vlan :

- **Manage & Production (PCT and HTTP Server): ID VLAN = 3**
- **Users Site A (PCA and DHCP Server): ID VLAN = 2**
- **Interconnection with router RA: VLAN ID = 10**
- **Make show vlan brief on each switch (copy screenshot hereafter).**

On SWD :

- Create the vlan :

```
Switch>en
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 3
Switch(config-vlan)#exit
Switch(config)#vlan 2
Switch(config-vlan)#exit
Switch(config)#vlan 10
Switch(config-vlan)#exit
```

- Configure the interfaces of SWD in trunk mode :

```
Switch(config)#interface fa 0/1
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#switchport mode trunk

Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/1, changed state to up
Switch(config)#interface fa 0/2
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#switchport mode trunk

Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/2, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/2, changed state to up
Switch#show int trunk
Port        Mode         Encapsulation  Status
Native vlan
Fa0/1       on           802.1q         trunking      1
Fa0/2       on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/1       1-1005
Fa0/2       1-1005

Port        Vlans allowed and active in management
domain
Fa0/1       1,2,3,10
Fa0/2       1,2,3,10

Port        Vlans in spanning tree forwarding state and
not pruned
Fa0/1       1,2,3,10
Fa0/2       1,2,3,10
```

- Configure the interfaces of SWA1 :

We have 2 interfaces on trunk mode (between SWA1 and SWA2, and SWA1 and SWD) and 2 interfaces on access mode (between PCA and DHCP Server).
To see the status of all the interfaces we use the command : *show int switchport*

```
Name: Fa0/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 2 (VLAN0002)
Name: Fa0/2
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Name: Fa0/3
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 2 (VLAN0002)
Name: Fa0/4
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Switch#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- ---------
-------------------------------
1    default                          active    Fa0/5,
Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9,
Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13,
Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17,
Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21,
Fa0/22, Fa0/23, Fa0/24
                                                Gig0/1,
Gig0/2
2    VLAN0002                         active    Fa0/1,
Fa0/3
3    VLAN0003                         active
10   VLAN0010                         active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

- configure the interfaces of SWA2

Same as SWA1 : mode trunk between SWA2 and SWA1, and SWD and SWA2

```
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
```

```
Name: Fa0/2
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 3 (VLAN0003)
```

```
Name: Fa0/3
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 3 (VLAN0003)
```

```
Name: Fa0/4
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
```

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/5,
Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9,
Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13,
Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17,
Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21,
Fa0/22, Fa0/23, Fa0/24
                                                 Gig0/1,
Gig0/2
2    VLAN0002                          active
3    VLAN0003                          active    Fa0/2,
Fa0/3
10   VLAN0010                          active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

Make a show spanning-tree vlan VLAN_ID on each switch (copy screenshot hereafter).

On SWA2 : show spanning-tree

```
SWA2#show spanning-tree vlan 3
VLAN0003
  Spanning tree enabled protocol ieee
  Root ID     Priority    4099
              Address     000A.F396.8749
              Cost        19
              Port        4(FastEthernet0/4)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15
sec

  Bridge ID   Priority    32771  (priority 32768 sys-id-ext 3)
              Address     0060.47C1.7105
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15
sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- --------
--------------------------------
Fa0/4            Root FWD 19        128.4    P2p
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/3            Desg FWD 19        128.3    P2p
Fa0/1            Altn BLK 19        128.1    P2p
```

By doing *show spanning-tree vlan 3*, we can notice that only the interface Fa0/2 (connected to SWA2) and Fa0/4 (connected to SWD) appear. These two interface are on trunk mode so they will appear on every VLAN because the trunk mode lets all the vlan to flow.

When we do *show spanning-tree vlan 2*, only the interfaces on trunk mode appear :

```
SWA2#show spanning-tree vlan 2
VLAN0002
  Spanning tree enabled protocol ieee
  Root ID     Priority    4098
              Address     000A.F396.8749
              Cost        19
              Port        4(FastEthernet0/4)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15
sec

  Bridge ID   Priority    32770  (priority 32768 sys-id-ext 2)
              Address     0060.47C1.7105
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15
sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- --------
--------------------------------
Fa0/4            Root FWD 19        128.4    P2p
Fa0/1            Altn BLK 19        128.1    P2p
```

We have exactly the same by doing *show spanning-tree vlan 10* :

```
SWA2#show spanning-tree vlan 10
VLAN0010
  Spanning tree enabled protocol ieee
  Root ID     Priority    4106
              Address     000A.F396.8749
              Cost        19
              Port        4(FastEthernet0/4)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15
sec

  Bridge ID   Priority    32778  (priority 32768 sys-id-ext 10)
              Address     0060.47C1.7105
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15
sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- --------
--------------------------------
Fa0/4            Root FWD 19        128.4    P2p
Fa0/1            Altn BLK 19        128.1    P2p
```

On SWA1 : *show spanning-tree*

```
SWA1#show spanning-tree vlan 2
VLAN0002
  Spanning tree enabled protocol ieee
  Root ID     Priority    4098
              Address     000A.F396.8749
              Cost        19
              Port        4(FastEthernet0/4)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15
sec

  Bridge ID   Priority    32770  (priority 32768 sys-id-ext 2)
              Address     000A.41E7.98B6
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15
sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- --------
--------------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/3            Desg FWD 19        128.3    P2p
Fa0/4            Root FWD 19        128.4    P2p
```

We can see all the interfaces which are on the VLAN 2 and also the interfaces on trunk mode as we explained before.

On SWD : *show spanning-tree*

```
Switch#show spanning-tree vlan 10
VLAN0010
  Spanning tree enabled protocol ieee
  Root ID     Priority    4106
              Address     000A.F396.8749
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15
sec

  Bridge ID   Priority    4106  (priority 4096 sys-id-ext 10)
              Address     000A.F396.8749
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15
sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- --------
--------------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/2            Desg FWD 19        128.2    P2p
```

```
Switch#show spanning-tree vlan 2
VLAN0002
  Spanning tree enabled protocol ieee
  Root ID     Priority    4098
              Address     000A.F396.8749
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15
sec

  Bridge ID   Priority    4098  (priority 4096 sys-id-ext 2)
              Address     000A.F396.8749
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15
sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- --------
--------------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/2            Desg FWD 19        128.2    P2p

Switch#show spanning-tree vlan 3
VLAN0003
  Spanning tree enabled protocol ieee
  Root ID     Priority    4099
              Address     000A.F396.8749
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15
sec

  Bridge ID   Priority    4099  (priority 4096 sys-id-ext 3)
              Address     000A.F396.8749
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15
sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- --------
--------------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/2            Desg FWD 19        128.2    P2p
```

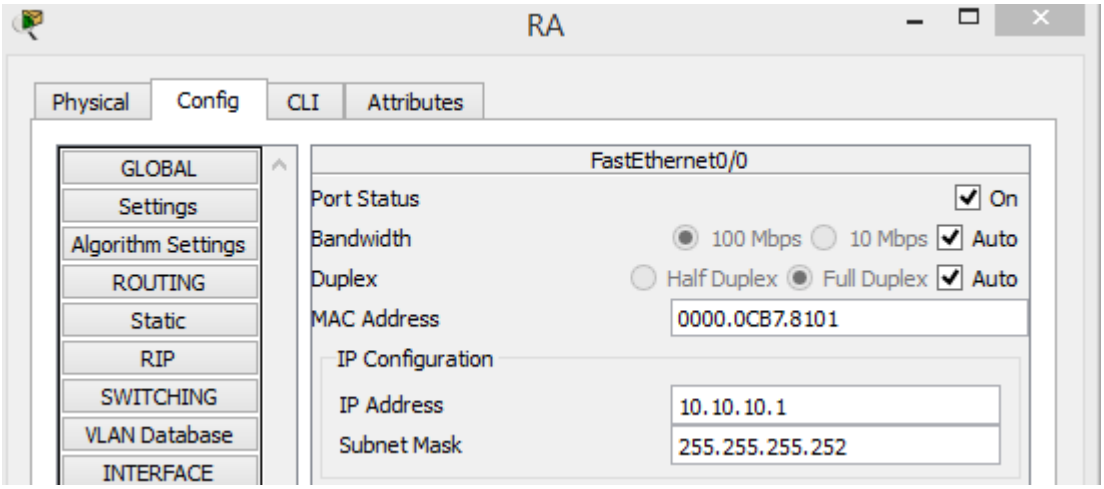
For every Vlan, we can see the interface Fa0/1 (connected to SWA2) and the interface Fa0/2 (connected to SWA1) which are on trunk mode.

What is the root bridge for each vlan and why?

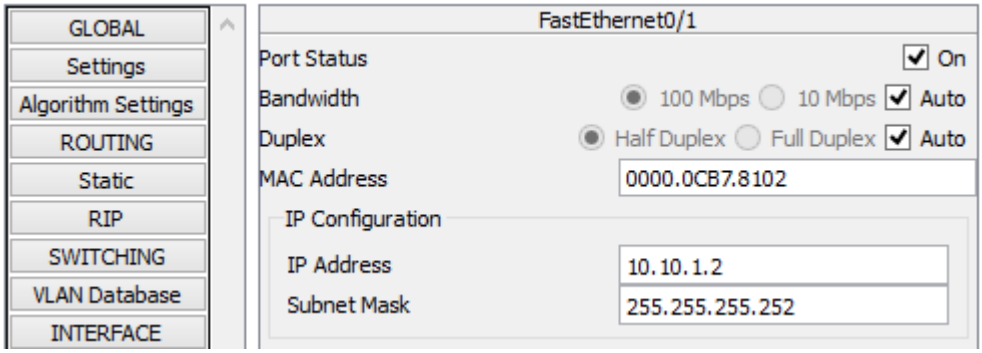
The root bridge for VLAN2, VLAN3 and VLAN10 is SWD because it allows the connexion to the site B and also internet for each vlan.

4. Configure IP for cisco devices

Connect RA to a DSL modem and use a phone link to connect the DSL modem to the cloud (modem 3): LAN (Fa0/0) : 10.10.10.1/30 , WAN (Fa0/0) use dhcp




```
RA#config t
Enter configuration commands, one per line.  End with CNTL/Z.
RA(config)#interface fa0/1
RA(config-if)#ip address dhcp
RA(config-if)#
%DHCP-6-ADDRESS_ASSIGN: Interface FastEthernet0/1 assigned DHCP
address 10.10.1.2, mask 255.255.255.252, hostname RA
```



Make show interfaces fastEthernet 0/1, (copy the result in text format and not a screenshot), what is the IP WAN of the router?

```
RA#show interfaces fastEthernet 0/1
FastEthernet0/1 is up, line protocol is up (connected)
Hardware is Lance, address is 0000.0cb7.8102 (bia 0000.0cb7.8102)
Internet address is 10.10.1.2/30
MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
ARP type: ARPA, ARP Timeout 04:00:00,
Last input 00:00:08, output 00:00:05, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0 (size/max/drops); 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
2 packets input, 186 bytes, 0 no buffer
Received 2 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 input packets with dribble condition detected
2 packets output, 178 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
```

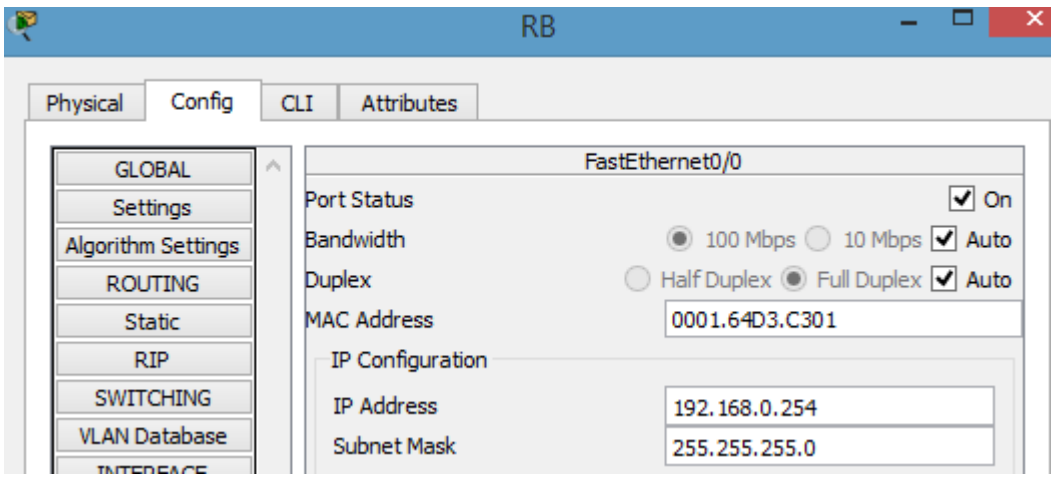
The IP WAN of the router is : 10.10.1.2/30

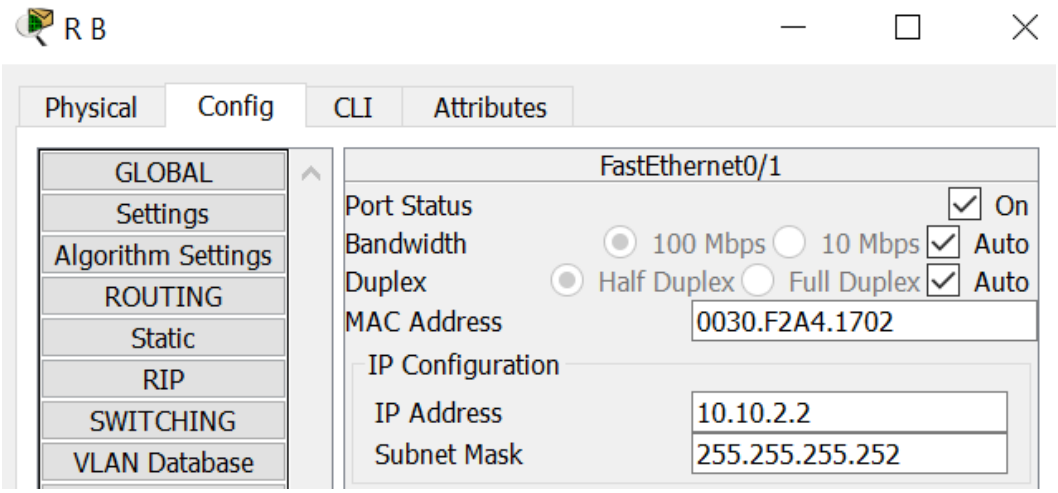
Make show ip route , what is the default gateway of the router ?

```
RA#show ip route
Codes: C - connected, S - static, I - IGRP, 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 10.10.1.1 to network 0.0.0.0

     10.0.0.0/30 is subnetted, 2 subnets
C       10.10.1.0 is directly connected, FastEthernet0/1
C       10.10.10.0 is directly connected, FastEthernet0/0
S*   0.0.0.0/0 [254/0] via 10.10.1.1
```

The default gateway of the router is 10.10.1.1

Connect RB to a DSL modem and use a phone link to connect the DSL modem to the cloud (modem 4): LAN (Fa0/0): 192.168.0.254/24, WAN (Fa0/1) use dhcp.





Make show interfaces fastEthernet 0/1, ((copy the result in text format and not a screenshot), what is the IP WAN of the router?

```
Router#show interface fa0/1
FastEthernet0/1 is up, line protocol is up (connected)
Hardware is Lance, address is 0030.f2a4.1702 (bia 0030.f2a4.1702)
Internet address is 10.10.2.2/30
MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
ARP type: ARPA, ARP Timeout 04:00:00,
Last input 00:00:08, output 00:00:05, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0 (size/max/drops); 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
4 packets input, 372 bytes, 0 no buffer
Received 4 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 input packets with dribble condition detected
5 packets output, 418 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
```

The IP WAN of the Router is 10.10.2.2/30

Make show ip route , what is the default gateway of the router ?

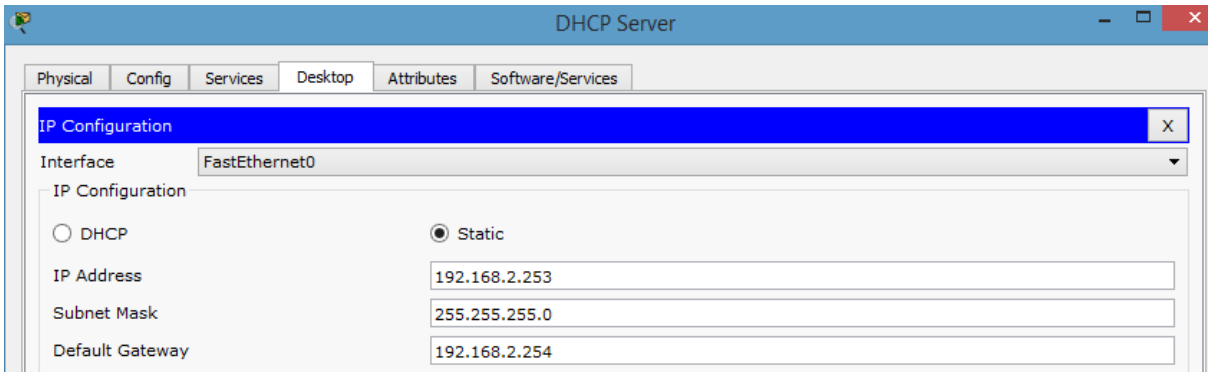
```
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile,
B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter
area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external
type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E -
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 10.10.2.1 to network 0.0.0.0

     10.0.0.0/30 is subnetted, 1 subnets
C       10.10.2.0 is directly connected, FastEthernet0/1
C    192.168.0.0/24 is directly connected, FastEthernet0/0
S*   0.0.0.0/0 [254/0] via 10.10.2.1
```

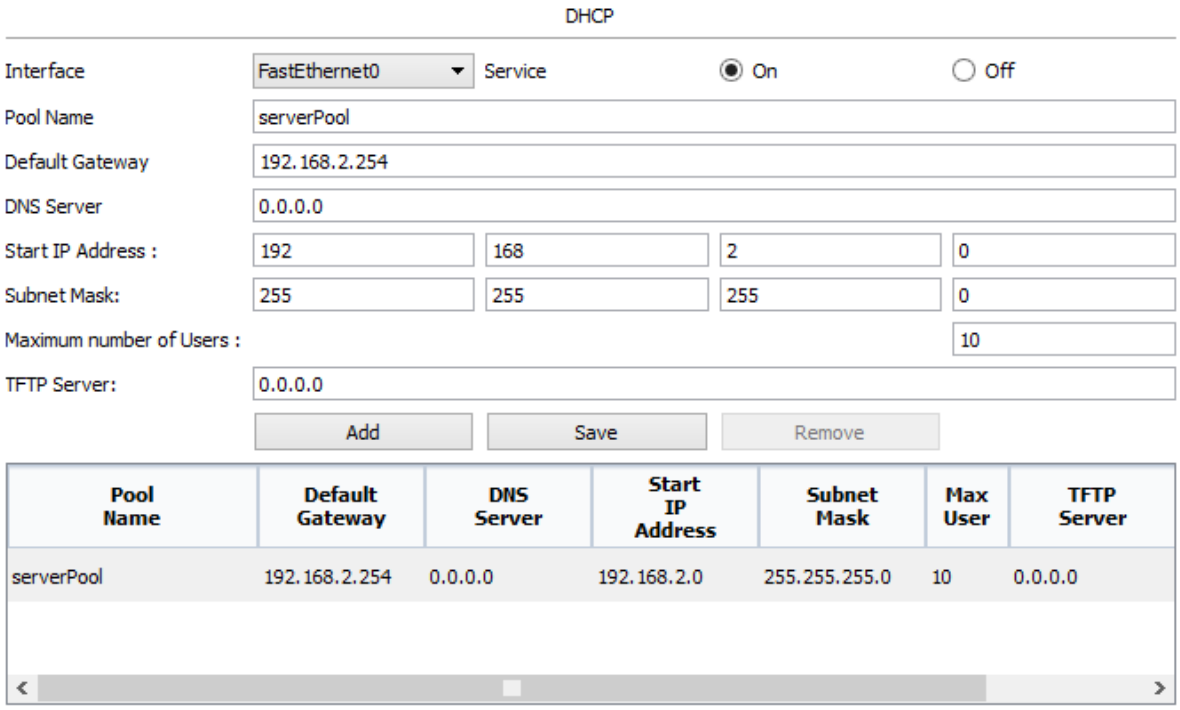
The default gateway of the router is 10.10.2.1

SWD : VLAN interfaces
VLAN 2 : 192.168.2.254/24
VLAN 3: 192.168.3.254/24
VLAN 10 : 10.10.10.2/30

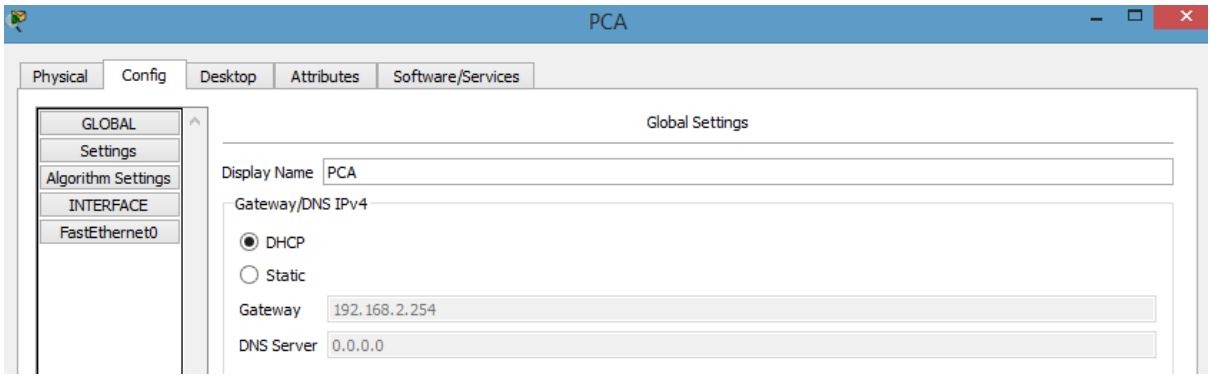
```
Switch(config)#int vlan 2
Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan2, changed
state to up

Switch(config-if)#ip address 192.168.2.254 255.255.255.0


Switch(config)#int vlan 3
Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan3, changed
state to up

Switch(config-if)#ip address 192.168.3.254 255.255.255.0


Switch(config)#int vlan 10
Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan10, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed
state to up

Switch(config-if)#ip address 10.10.10.2 255.255.255.252
```

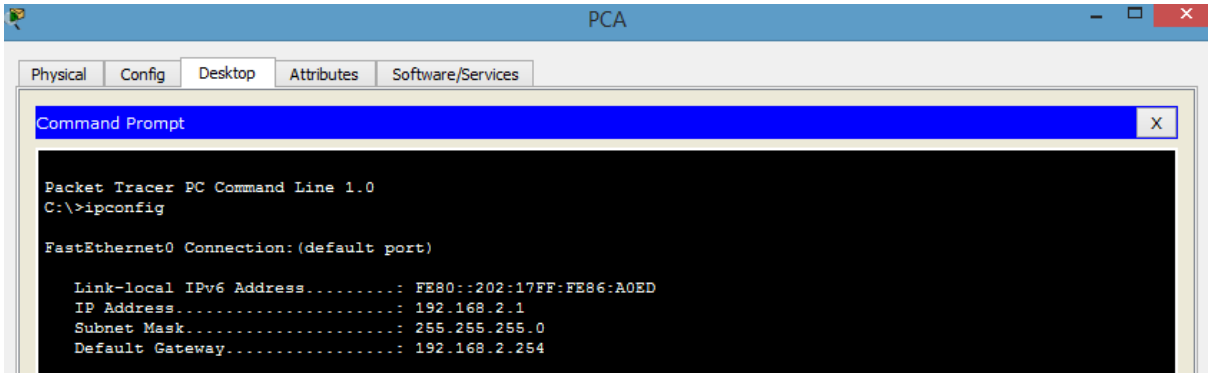
5. Configure the DHCP Server to attribute the IP configuration to PCA.



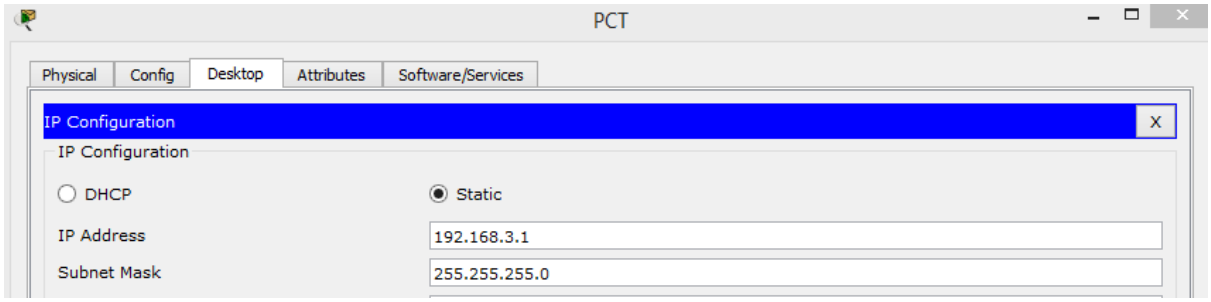


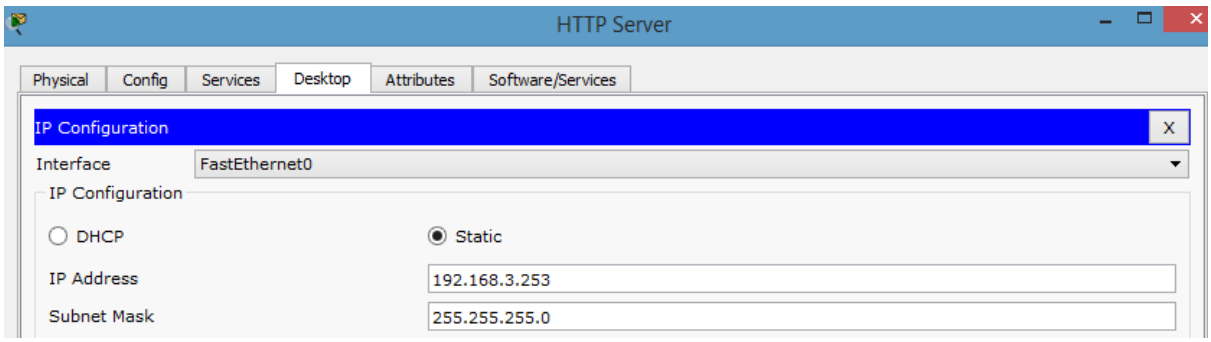
6. Configure the PCA on DHCP

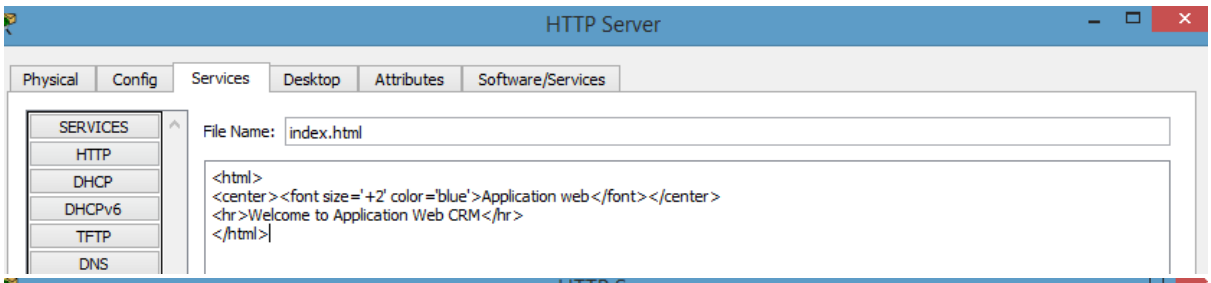


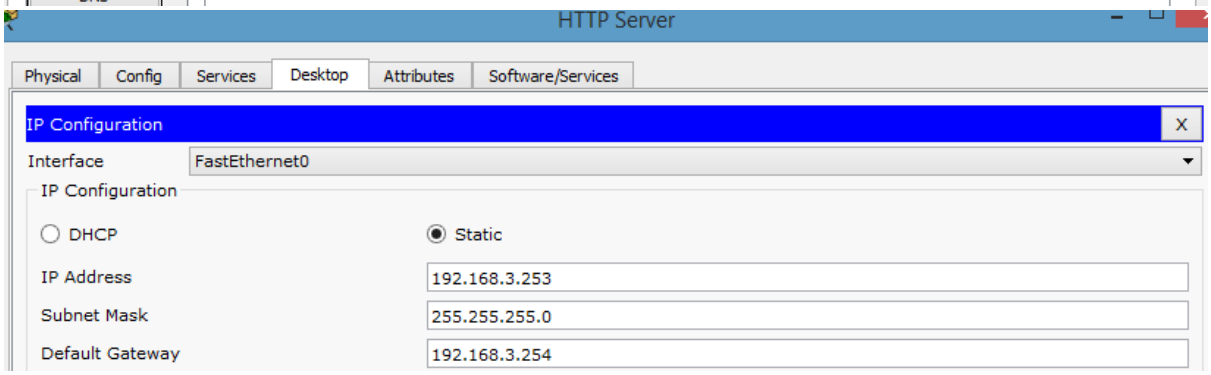


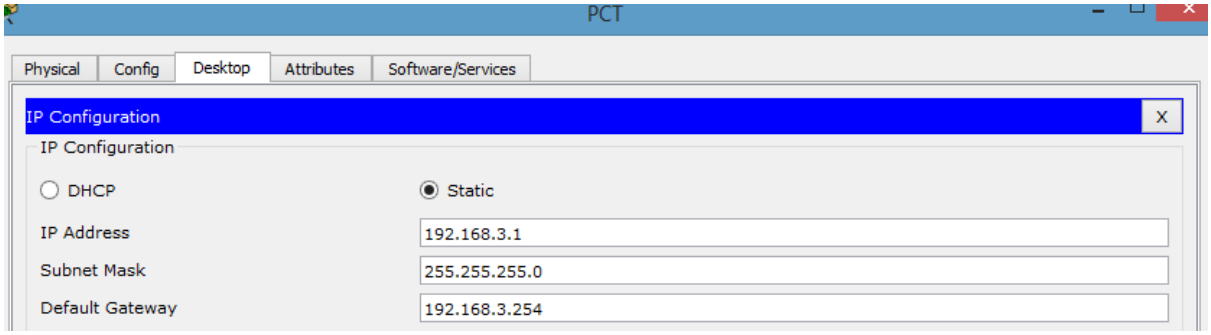
7. Configure PCT et HTTP server











8. Verification (copy screenshot hereafter).

- **Ping & tracert**

Before pinging we must right the command *ip routing* on the SWD

From PCT to PCA and DHCP Server

```
C:\>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

Reply from 192.168.2.1: bytes=32 time=1ms TTL=127
Reply from 192.168.2.1: bytes=32 time=1ms TTL=127
Reply from 192.168.2.1: bytes=32 time=1ms TTL=127
Reply from 192.168.2.1: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

```
C:\>ping 192.168.2.253

Pinging 192.168.2.253 with 32 bytes of data:

Reply from 192.168.2.253: bytes=32 time=1ms TTL=127
Reply from 192.168.2.253: bytes=32 time<1ms TTL=127
Reply from 192.168.2.253: bytes=32 time<1ms TTL=127
Reply from 192.168.2.253: bytes=32 time=1ms TTL=127

Ping statistics for 192.168.2.253:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

```
C:\>tracert 192.168.2.1

Tracing route to 192.168.2.1 over a maximum of 30 hops:

  1    0 ms      0 ms      0 ms      192.168.3.254
  2    1 ms      1 ms      0 ms      192.168.2.1

Trace complete.
```

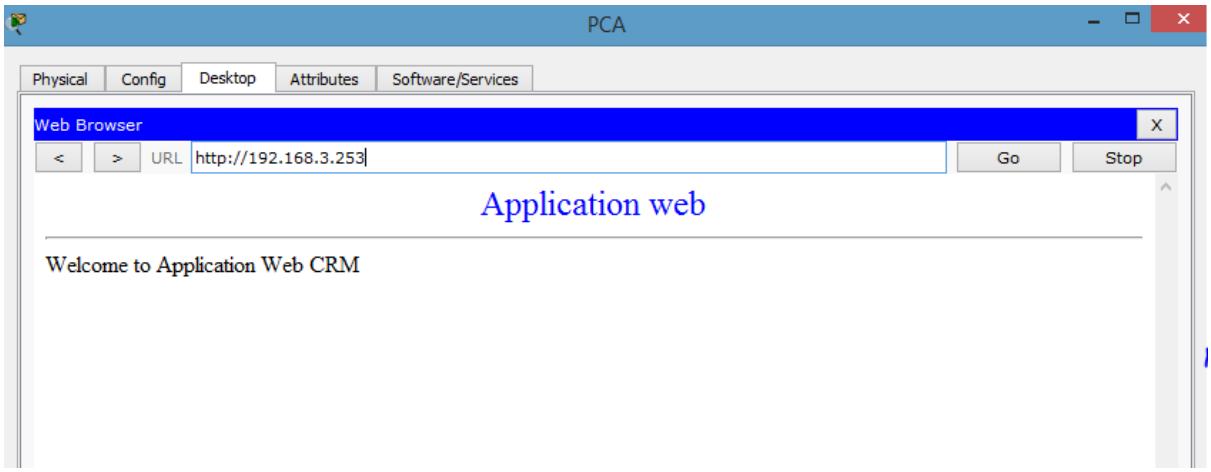
```
C:\>tracert 192.168.2.253

Tracing route to 192.168.2.253 over a maximum of 30 hops:

  1    1 ms      1 ms      14 ms     192.168.3.254
  2    0 ms      0 ms      0 ms      192.168.2.253

Trace complete.
```

From PCA to HTTP Server

```
C:\>ping 192.168.3.253

Pinging 192.168.3.253 with 32 bytes of data:

Reply from 192.168.3.253: bytes=32 time<1ms TTL=127
Reply from 192.168.3.253: bytes=32 time<1ms TTL=127
Reply from 192.168.3.253: bytes=32 time<1ms TTL=127
Reply from 192.168.3.253: bytes=32 time=1ms TTL=127

Ping statistics for 192.168.3.253:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

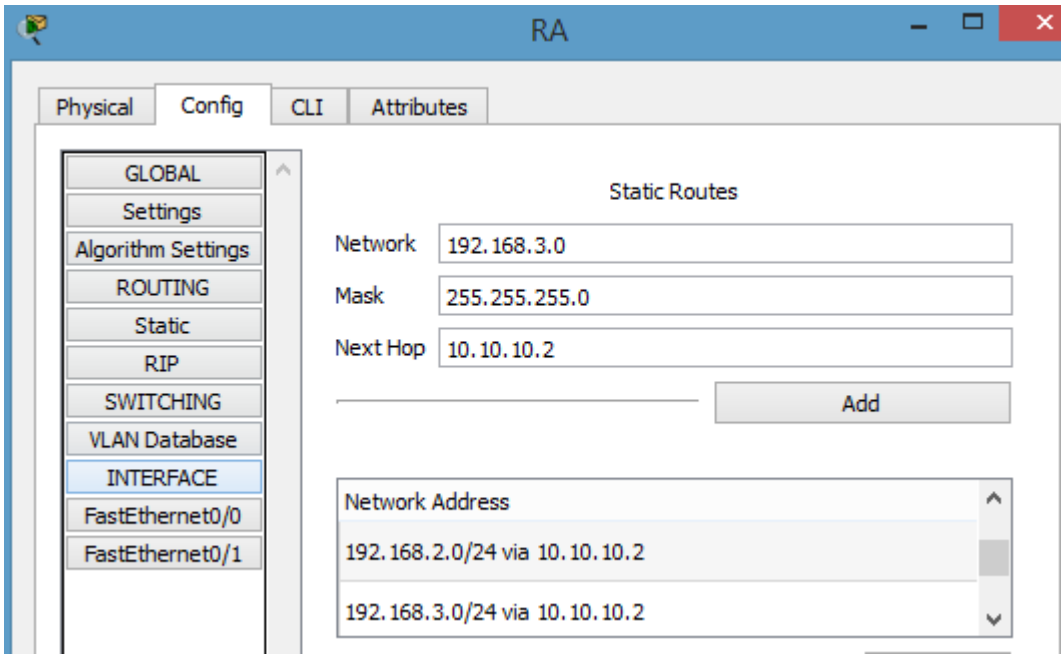
```
C:\>tracert 192.168.3.253

Tracing route to 192.168.3.253 over a maximum of 30 hops:

  1    0 ms      0 ms      0 ms      192.168.2.254
  2    0 ms      1 ms      1 ms      192.168.3.253

Trace complete.
```

Use the Web Browser of PCA to connect to the HTTP Server

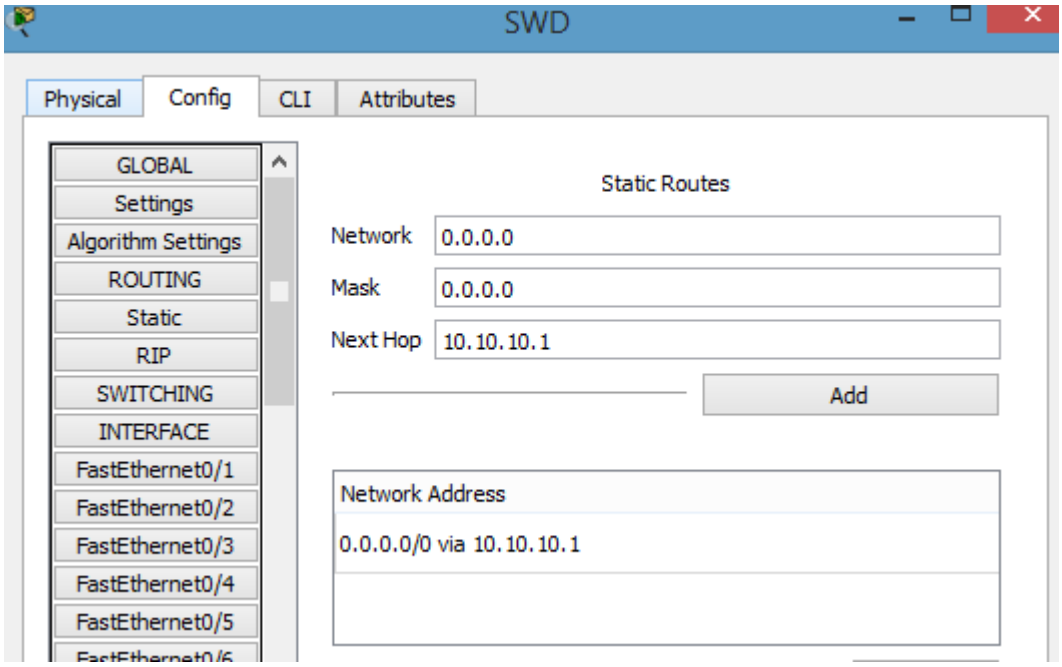


9. Configure the routing on SWD and RA :

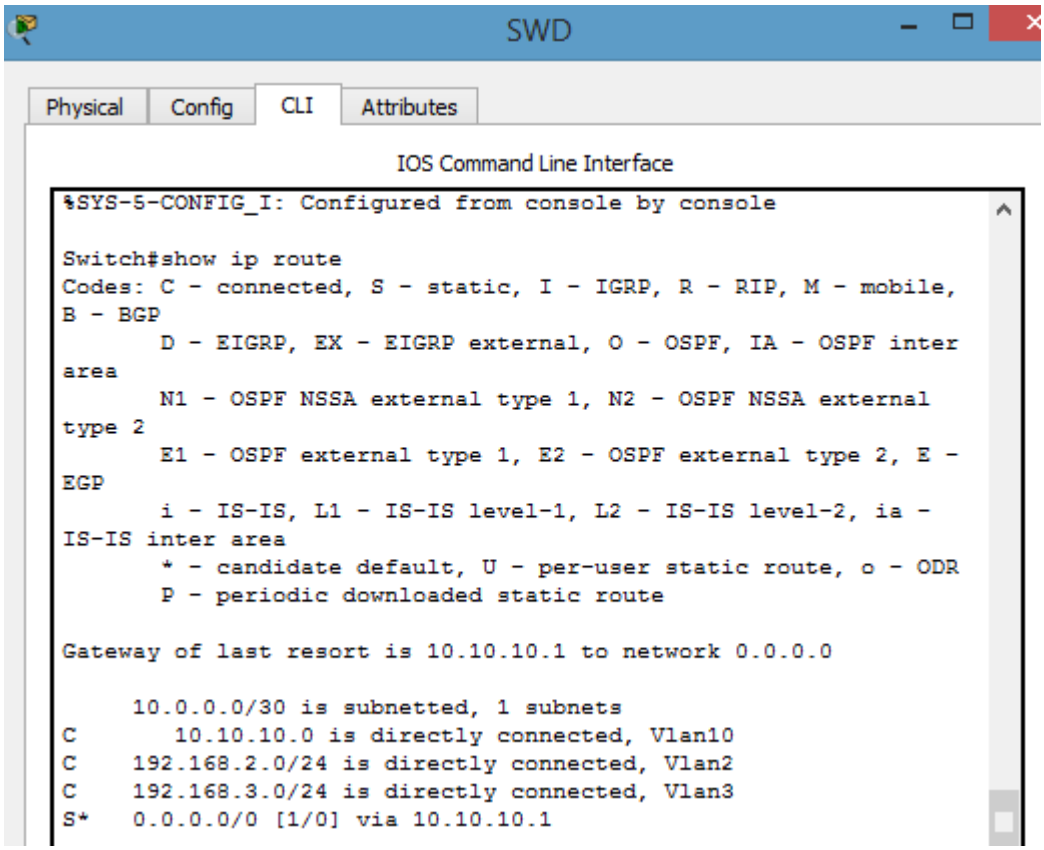
- **Add static routes 192.168.2.0/24 and 192.168.3.0/24 to SWD on RA.**

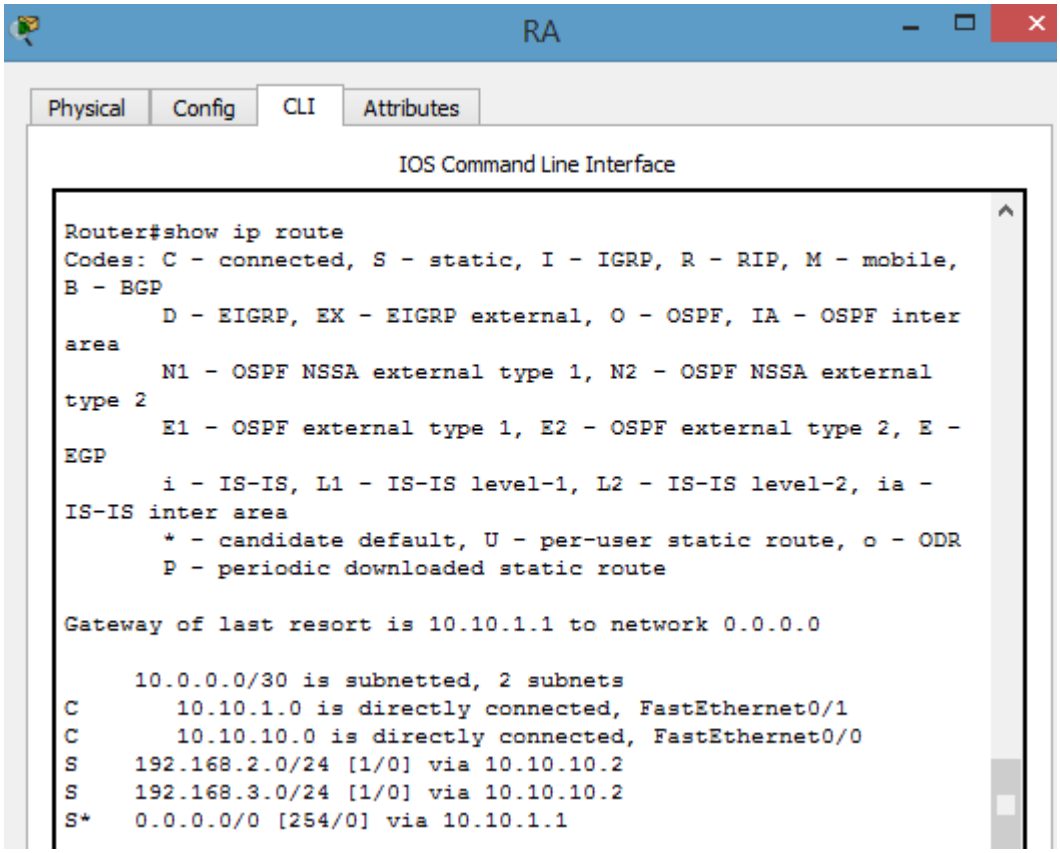


- **The default gateway of the SWD is RA.**



- **Make a show ip route on RA and SWD (copy screenshot hereafter)**





10. Configure dhcp server on the router RB

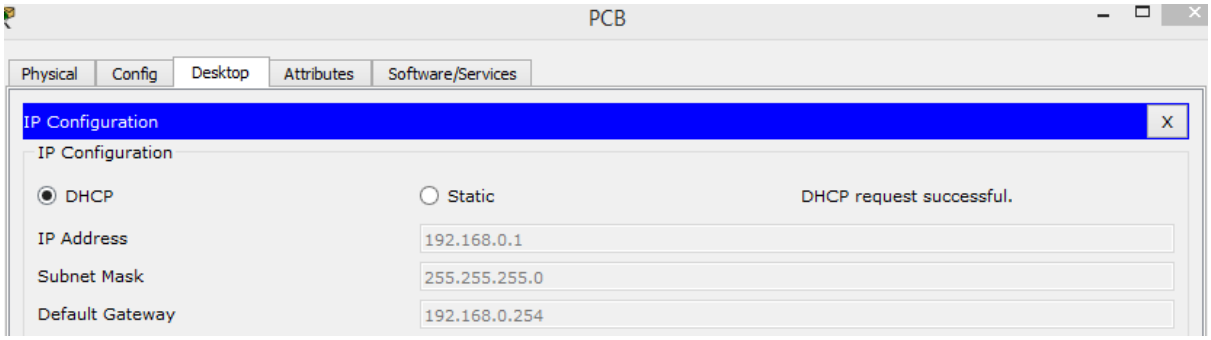
- The default gateway of the LAN Site B is RB

- Create a pool containing 10 IP addresses.

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
Router(config)#
Router(config)#ip dhcp pool dhcpsiteB
Router(dhcp-config)#network 192.168.0.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.0.254
Router(dhcp-config)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip dhcp excluded-address 192.168.0.11
192.168.0.253
```

11. Configure the PCB on DHCP

- **Copy a screenshot of the ipconfig**




```
Router#show ip dhcp binding
IP address       Client-ID/              Lease expiration
Type
                 Hardware address
192.168.0.1      0060.3E46.BA72           --
Automatic
```

By writting this command, we can see the pool we have created and the only address that has been given to PCB with dhcp.

```
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Link-local IPv6 Address.....: FE80::260:3EFF:FE46:BA72
   IP Address.....: 192.168.0.1
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: 192.168.0.254
```

12. Make show ip arp on : RA, RB, and SWD (copy screenshot hereafter).

On RA :

```
Router#show ip arp
Protocol  Address          Age (min)  Hardware Addr   Type
Interface
Internet  10.10.1.2              -   0002.1722.5902  ARPA
FastEthernet0/1
Internet  10.10.10.1             -   0002.1722.5901  ARPA
FastEthernet0/0
```

On RB :

```
Router#show ip arp
Protocol  Address          Age (min)  Hardware Addr   Type
Interface
Internet  10.10.2.2              -   0030.F2A4.1702  ARPA
FastEthernet0/1
Internet  192.168.0.254          -   0030.F2A4.1701  ARPA
FastEthernet0/0
```

On SWD :

```
SWD#show ip arp
Protocol  Address          Age (min)  Hardware Addr   Type
Interface
Internet  10.10.10.2             -   0006.2A3C.8303  ARPA
Vlan10
Internet  192.168.2.254          -   0006.2A3C.8301  ARPA
Vlan2
Internet  192.168.3.254          -   0006.2A3C.8302  ARPA
Vlan3
```

13. You will configure a tunnel IPSec between RA and RB to provide a secure communication between Site A and Site B.

- **Configure a ISAKMP policy**
  - **Use a shared key for authentication**
  - **Encryption algorithm DES**
  - **Hash algorithm md5**

```
RA#config t
Enter configuration commands, one per line.  End with CNTL/Z.
RA(config)#crypto isakmp enable
RA(config)#crypto isakmp policy 10
RA(config-isakmp)#authentication pre-share
RA(config-isakmp)#encryption des
RA(config-isakmp)#hash md5
RA(config-isakmp)#exit
```

```
RB(config)#crypto isakmp enable
RB(config)#crypto isakmp policy 10
RB(config-isakmp)#authentication pre-share
RB(config-isakmp)#encryption des
RB(config-isakmp)#hash md5
```

- **Configure a pre-shard key (the same key must be configured on the two routers) with the peer WAN IP address (RA is the peer of RB)**

```
RA(config)#crypto isakmp key marion address 10.10.2.2
RB(config)#crypto isakmp key marion address 10.10.1.2
```

- **Configure transform-set labset , you will use esp protocol**
  - **Encryption algorithm 3DES**
  - **Hash algorithm sha**

```
RA(config)#crypto ipsec transform-set labset esp-3des esp-sha-hmac
RB(config)#crypto ipsec transform-set labset esp-3des esp-sha-hmac
```

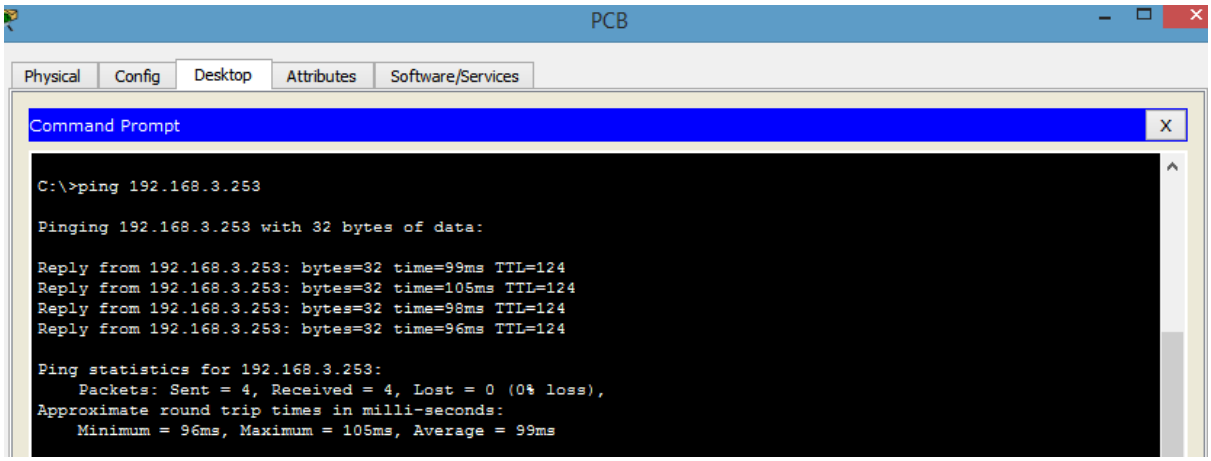
- **Configure an access-list 100 to define interesting VPN traffic (the LANs subnet => encryption domains).**

```
RA(config)#access-list 100 permit ip 10.10.10.1 0.0.0.3
192.168.0.254 0.0.0.255
RA(config)#access-list 100 permit ip 192.168.2.0 0.0.0.255
192.168.0.0 0.0.0.255
RA(config)#access-list 100 permit ip 192.168.3.0 0.0.0.255
192.168.0.0 0.0.0.255

RB(config)#access-list 100 permit ip 192.168.0.254 0.0.0.255 10.10.10.1 0.0.0.3
RB(config)#access-list 100 permit ip 192.168.0.0 0.0.0.255
192.168.2.0 0.0.0.255
RB(config)#access-list 100 permit ip 192.168.0.0 0.0.0.255
192.168.3.0 0.0.0.255
```

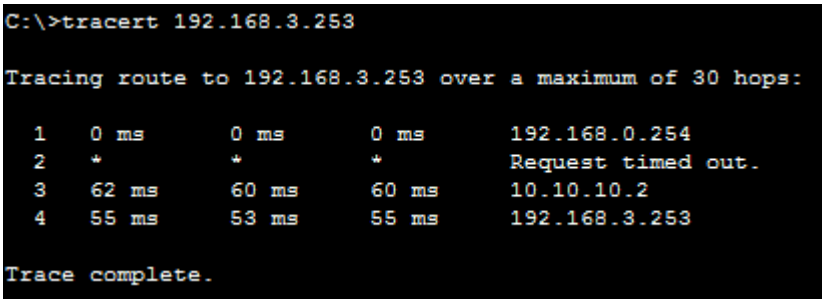
- **Configure the crypto map labmap**
  - **Set the peer address**
  - **Use the transform labset.**
  - **Match the access-list 100**

```
RA(config)#crypto map labmap 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
RA(config-crypto-map)#set peer 10.10.2.2
RA(config-crypto-map)#set transform-set labset
RA(config-crypto-map)#match address 100
RA(config-crypto-map)#exit
RA(config)#int fa 0/1
RA(config-if)#crypto map labmap
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON



RB(config)#crypto map labmap 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
RB(config-crypto-map)#set peer 10.10.1.2
RB(config-crypto-map)#set transform-set labset
RB(config-crypto-map)#match address 100
RB(config)#int fa 0/1
RB(config-if)#crypto map labmap
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

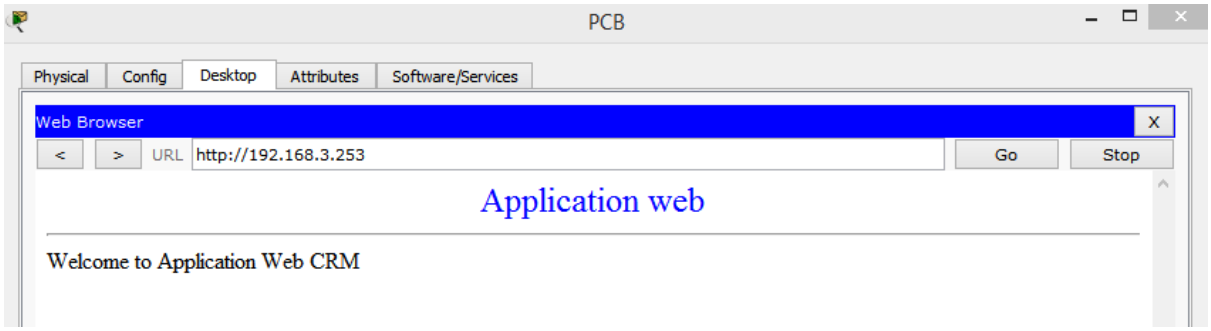
14. Ping Server HTTP from PCB (copy screenshot hereafter).



15. Make a traceroute to Server HTTP from PCB (copy screenshot hereafter).



16. Use the Web Browser of PCB to connect to the HTTP Server (copy screenshot hereafter).



17. Execute the commands on the RA and RB (copy screenshot hereafter).

- **show crypto map**

```
RA#show crypto map
Crypto Map labmap 10 ipsec-isakmp
        Peer = 10.10.2.2
        Extended IP access list 100
            access-list 100 permit ip 10.10.10.0 0.0.0.3
192.168.0.0 0.0.0.255
            access-list 100 permit ip 192.168.2.0 0.0.0.255
192.168.0.0 0.0.0.255
            access-list 100 permit ip 192.168.3.0 0.0.0.255
192.168.0.0 0.0.0.255
        Current peer: 10.10.2.2
        Security association lifetime: 4608000 kilobytes/3600
seconds
        PFS (Y/N): N
        Transform sets={
                labset,
        }
        Interfaces using crypto map labmap:
                FastEthernet0/1
```

```
RB#show crypto map
Crypto Map labmap 10 ipsec-isakmp
        Peer = 10.10.1.2
        Extended IP access list 100
            access-list 100 permit ip 192.168.0.0 0.0.0.255
10.10.10.0 0.0.0.3
            access-list 100 permit ip 192.168.0.0 0.0.0.255
192.168.2.0 0.0.0.255
            access-list 100 permit ip 192.168.0.0 0.0.0.255
192.168.3.0 0.0.0.255
        Current peer: 10.10.1.2
        Security association lifetime: 4608000 kilobytes/3600
seconds
        PFS (Y/N): N
        Transform sets={
                labset,
        }
        Interfaces using crypto map labmap:
                FastEthernet0/1
```

- **show crypto isakmp sa**

RA :

```
RA#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot
status
10.10.2.2       10.10.1.2       QM_IDLE           1031    0
ACTIVE


IPv6 Crypto ISAKMP SA
```

RB :

```
RB#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot
status
10.10.1.2       10.10.2.2       QM_IDLE           1000    0
ACTIVE


IPv6 Crypto ISAKMP SA
```

- **show crypto ipsec sa**

RA :

```
RA#show crypto ipsec sa

interface: FastEthernet0/1
    Crypto map tag: labmap, local addr 10.10.1.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (10.10.10.0/255.255.255.252/0/0)
   remote  ident (addr/mask/prot/port): (192.168.0.0/255.255.255.0/0/0)
   current_peer 10.10.2.2 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 1, #pkts encrypt: 1, #pkts digest: 0
   #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 1, #recv errors 0

     local crypto endpt.: 10.10.1.2, remote crypto endpt.:10.10.2.2
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/1
     current outbound spi: 0x287C5C78(679238776)

     inbound esp sas:
      spi: 0x020E2742(34481986)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2006, flow_id: FPGA:1, crypto map: labmap
        sa timing: remaining key lifetime (k/sec): (4525504/3157)
        IV size: 16 bytes
        replay detection support: N
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
  spi: 0x287C5C78(679238776)
    transform: esp-3des esp-sha-hmac ,
    in use settings ={Tunnel, }
    conn id: 2007, flow_id: FPGA:1, crypto map: labmap
    sa timing: remaining key lifetime (k/sec): (4525504/3157)
    IV size: 16 bytes
    replay detection support: N
    Status: ACTIVE

 outbound ah sas:

 outbound pcp sas:
```

RB :

```
RB>en
RB#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
10.10.1.2       10.10.2.2       QM_IDLE           1000    0 ACTIVE


IPv6 Crypto ISAKMP SA


RB#show crypto ipsec sa

interface: FastEthernet0/1
    Crypto map tag: labmap, local addr 10.10.2.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.0.0/255.255.255.0/0/0)
   remote  ident (addr/mask/prot/port): (10.10.10.0/255.255.255.252/0/0)
   current_peer 10.10.1.2 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
   #pkts decaps: 1, #pkts decrypt: 1, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 0, #recv errors 0

     local crypto endpt.: 10.10.2.2, remote crypto endpt.:10.10.1.2
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/1
     current outbound spi: 0x020E2742(34481986)

     inbound esp sas:
      spi: 0x287C5C78(679238776)
      transform: esp-3des esp-sha-hmac ,
      in use settings ={Tunnel, }
      conn id: 2006, flow_id: FPGA:1, crypto map: labmap
      sa timing: remaining key lifetime (k/sec): (4525504/2983)
      IV size: 16 bytes
      replay detection support: N
      Status: ACTIVE

   inbound ah sas:

   inbound pcp sas:

   outbound esp sas:
    spi: 0x020E2742(34481986)
      transform: esp-3des esp-sha-hmac ,
      in use settings ={Tunnel, }
      conn id: 2007, flow_id: FPGA:1, crypto map: labmap
      sa timing: remaining key lifetime (k/sec): (4525504/2983)
      IV size: 16 bytes
      replay detection support: N
      Status: ACTIVE

   outbound ah sas:

   outbound pcp sas:
```

18. Compare the SPI SAS (inbound and outbound) between RA and RB.

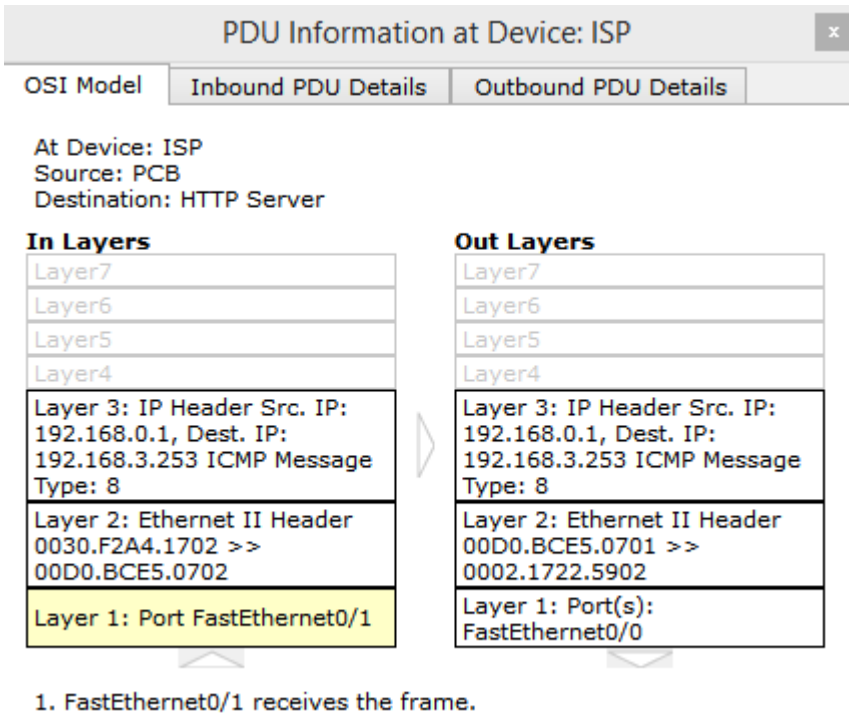
We have :

	RA	**RB**
SPI SAS inbound	0x020E2742	0x287C5C78
SPI SAS outbound	0x287C5C78	0x020E2742

We can notice that the RA SPI SAS inbound is equal to the RB SPI SAS outbound and the RB SPI inbound is equal to the RA SPI SAS outbound.

19. Be sur the SA IPSec are established, Use the simulation mode of Packet Tracer, "edit filters" check just ICMP, ping HHTP Server from PCB, click to "capture/Forward" up to have a message at the Internet Router. Click to the message at the ISP Router, copy screenshot hereafter for OSI Model, Inbound PDU Details and Outbound PDU Details.

OSI Model :



Inbound PDU :

Ethernet II

0	4	8	14	19 Bytes
PREAMBLE: 101010...1011		DEST MAC: 00D0.BCE5.0702	SRC MAC: 0030.F2A4.1702	
TYPE: 0x800	DATA (VARIABLE LENGTH)			FCS: 0x0

IP

0	4	8	16	19	31Bits
4	IHL	DSCP: 0x0	TL: 20		
ID: 0x49			0x0	0x0	
TTL: 255		PRO: 0x32	CHKSUM		
SRC IP: 10.10.2.2					
DST IP: 10.10.1.2					
OPT: 0x0					0x0
DATA (VARIABLE LENGTH)					

ENCAPSULATING SECURITY PAYLOAD

0	8	16	31Bits
ESP SPI: 1654998265			
ESP SEQUENCE: 34			
ESP DATA ENCRYPTED WITH 3DES			
ESP DATA AUTHENTICATED WITH SHA			

IP

0	4	8	16	19	31Bits
4	IHL	DSCP: 0x0	TL: 28		
ID: 0x25			0x0	0x0	
TTL: 254		PRO: 0x1	CHKSUM		
SRC IP: 192.168.0.1					
DST IP: 192.168.3.253					
OPT: 0x0					0x0
DATA (VARIABLE LENGTH)					

ICMP

0	8	16	31Bits
TYPE: 0x8	CODE: 0x0	CHECKSUM	
ID: 0x8		SEQ NUMBER: 35	

Outbound PDU :

Ethernet II

0	4	8	14	19 Bytes
PREAMBLE: 101010...1011		DEST MAC: 0002.1722.5902	SRC MAC: 00D0.BCE5.0701	
TYPE: 0x800	DATA (VARIABLE LENGTH)		FCS: 0x0	

IP

0	4	8	16	19	31Bits
4	IHL	DSCP: 0x0	TL: 20		
ID: 0x49			0x0	0x0	
TTL: 254		PRO: 0x32	CHKSUM		
SRC IP: 10.10.2.2					
DST IP: 10.10.1.2					
OPT: 0x0				0x0	
DATA (VARIABLE LENGTH)					

ENCAPSULATING SECURITY PAYLOAD

0	8	16	31Bits
ESP SPI: 1654998265			
ESP SEQUENCE: 34			
ESP DATA ENCRYPTED WITH 3DES			
ESP DATA AUTHENTICATED WITH SHA			

IP

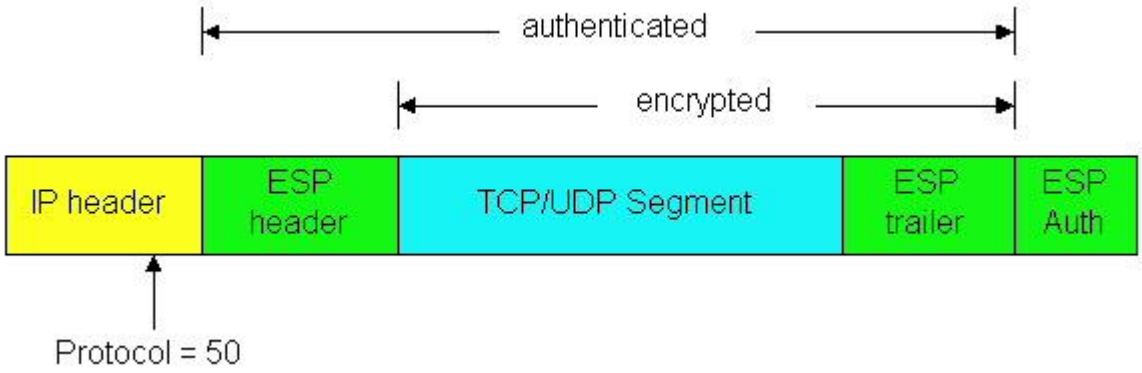
0	4	8	16	19	31Bits
4	IHL	DSCP: 0x0	TL: 28		
ID: 0x25			0x0	0x0	
TTL: 254		PRO: 0x1	CHKSUM		
SRC IP: 192.168.0.1					
DST IP: 192.168.3.253					
OPT: 0x0				0x0	
DATA (VARIABLE LENGTH)					

ICMP

0	8	16	31Bits
TYPE: 0x8	CODE: 0x0	CHECKSUM	
ID: 0x8		SEQ NUMBER: 35	

o Explain different headers of the packet in Inbound PDU Details and Outbound PDU Details.

We can observe that the IP of the destination and sources only appear in Inbound PDU Details and Outbound PDU details. We can also see that the ESP protocol encapsulate the TCP header and his data thanks to the IPSEC tunnel : it allows the encryption of the data as we can see on the picture :



Source : http://userpages.umbc.edu