# Explanation

**1. ISP Router**

* **Purpose:** Acts as the middleman between the Main and Sub branches.
* **Interfaces:**
  + Serial0/2/0 connects to MainBranch.
  + Serial0/2/1 connects to SubBranch.
* **BGP:**
  + External routing with Main (65001) and Sub (65002).
  + Advertises its own networks to the branches.

**2. Main Branch Router**

* **Purpose:** Main internal network (192.168.100.0/24) and connects to ISP.
* **Interfaces:**
  + Gig0/0 → internal LAN.
  + Serial0/2/0 → link to ISP.
  + Tunnel0 → secure GRE tunnel to Sub branch.
* **BGP:**
  + Talks to ISP (65000) for external routes.
  + Advertises its own public/point-to-point networks.
* **OSPF:**
  + Handles internal LAN routing only (192.168.100.0/24).
  + Keeps internal routes separate from BGP.
* **GRE Tunnel:**
  + Creates a virtual point-to-point link to Sub branch over the ISP network.
* **IPSec:**
  + Encrypts traffic through GRE tunnel for security.
  + Uses pre-shared key and AES + SHA for encryption/authentication.
  + Access-list 100 specifies what traffic is encrypted (here, 192.168.0.0/16).

**3. Sub Branch Router**

* **Purpose:** Sub-branch internal network (192.168.120.0/24) and connection to Main branch.
* **Interfaces:**
  + Gig0/0 → internal LAN.
  + Serial0/2/0 → link to ISP.
  + Tunnel0 → secure GRE tunnel to Main branch.
* **BGP:**
  + Talks to ISP (65000) for external routes.
  + Advertises its own public/point-to-point networks.
* **OSPF:**
  + Handles internal LAN routing only (192.168.120.0/24).
* **GRE Tunnel:**
  + Creates virtual point-to-point link to Main branch over the ISP network.
* **IPSec:**
  + Encrypts traffic through GRE tunnel.
  + Uses same pre-shared key and AES + SHA.
  + Access-list 100 defines encrypted traffic.

**How It Works Together**

1. Main and Sub branches communicate securely over the GRE tunnel with IPSec encryption.
2. Internal LANs use OSPF to route internally only; ISP never sees your private LANs.
3. ISP handles BGP, connecting the branches and enabling external routing.
4. Access-lists ensure only internal LAN traffic goes through IPSec.

# Routers configuration

## First interface configuration

Router main >>>>

hostname MainBranch

interface Gig0/0

ip address 192.168.100.1 255.255.255.0

no shutdown

interface Serial0/2/0

ip address 10.0.0.1 255.255.255.252

no shutdown

router isp >>>>>

hostname ISP

interface Serial0/2/0

ip address 10.0.0.2 255.255.255.252

clock rate 64000

no shutdown

interface Serial0/2/1

ip address 10.0.0.5 255.255.255.252

clock rate 64000

no shutdown

sub router

hostname SubBranch

interface Gig0/0

ip address 192.168.120.1 255.255.255.0

no shutdown

interface Serial0/2/0

ip address 10.0.0.6 255.255.255.252

no shutdown

## BGP (ISP↔Main↔Sub)

Isp router

router bgp 65000

bgp router-id 1.1.1.1

neighbor 10.0.0.1 remote-as 65001

neighbor 10.0.0.6 remote-as 65002

network 10.0.0.0 mask 255.255.255.252

network 10.0.0.4 mask 255.255.255.252

Main Router

router bgp 65001

bgp router-id 2.2.2.2

neighbor 10.0.0.2 remote-as 65000

network 10.0.0.0 mask 255.255.255.252

Sub router

router bgp 65002

bgp router-id 3.3.3.3

neighbor 10.0.0.5 remote-as 65000

network 10.0.0.4 mask 255.255.255.252

# making the gre

## making the ospf internal

main router

router ospf 1

router-id 1.1.1.1

network 192.168.100.0 0.0.0.255 area 0

network 172.16.0.0 0.0.0.3 area 0

sub router

router ospf 1

router-id 2.2.2.2

network 192.168.120.0 0.0.0.255 area 0

network 172.16.0.0 0.0.0.3 area 0

# making ipsec

main router

crypto isakmp policy 10

encryption aes

hash sha

authentication pre-share

group 2

lifetime 86400

exit

crypto isakmp key cisco address 10.0.0.6

crypto ipsec transform-set MYSET esp-aes esp-sha-hmac

crypto map MYMAP 10 ipsec-isakmp

set peer 10.0.0.6

set transform-set MYSET

match address 100

exit

access-list 100 permit ip 192.168.0.0 0.0.255.255 192.168.120.0 0.0.0.255

interface Serial0/2/0

crypto map MYMAP

sub router

crypto isakmp policy 10

encryption aes

hash sha

authentication pre-share

group 2

lifetime 86400

exit

crypto isakmp key cisco address 10.0.0.1

crypto ipsec transform-set MYSET esp-aes esp-sha-hmac

crypto map MYMAP 10 ipsec-isakmp

set peer 10.0.0.1

set transform-set MYSET

match address 100

exit

access-list 100 permit ip 192.168.120.0 0.0.0.255 192.168.0.0 0.0.255.255

interface Serial0/2/0

crypto map MYMAP