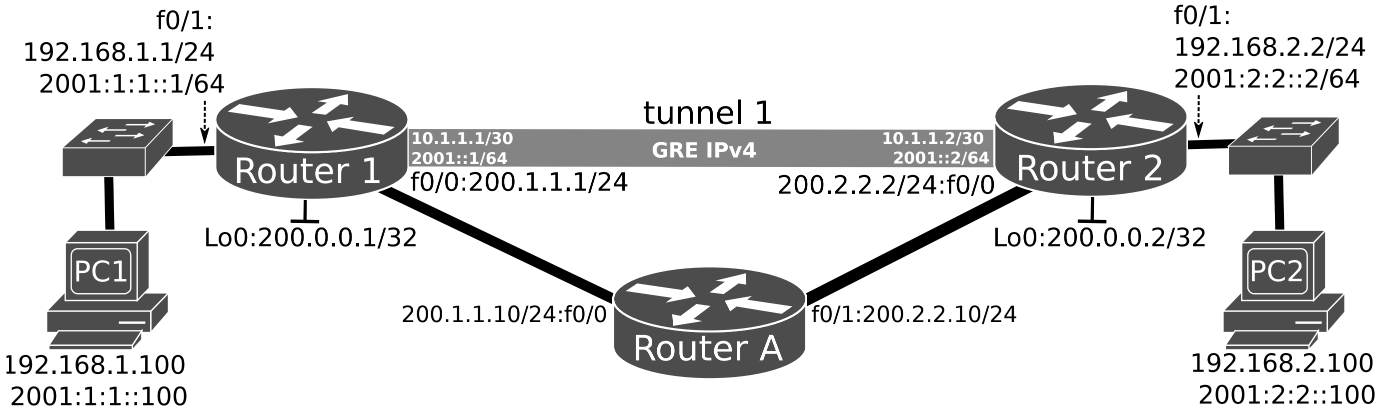
universidade de aveiro
theoria poiesis praxis

Segurança em Redes de Comunicações

Overlay IP and IPsec Networks

GRE IPv4 Tunnel / Overlay Network



With Static Routing

1. Configure the IPv4 and IPv6 addresses and activate OSPF for the underlying IPv4 network (including Loopback interfaces' addresses). To activate IPv6 routing, configure Loopback, IP address, and activate OSPF (process 1) in Router 1 for the underlying network by interface:

```
Router1(config)# ipv6 unicast-routing
Router1(config)# interface Loopback 0
Router1(config-if)# ip address 200.0.0.1 255.255.255.255
Router1(config-if)# ip ospf 1 area 0
Router1(config)# interface FastEthernet0/0
Router1(config-if)# ip address 200.1.1.1 255.255.255.0
Router1(config-if)# ip ospf 1 area 0
Router1(config-if)# no shut down
Router1(config)# interface FastEthernet0/1
Router1(config-if)# ip address 192.168.1.1 255.255.255.0
Router1(config-if)# ipv6 address 2001:1:1::1/64
Router1(config-if)# no shut down
```

Perform the equivalent configurations on Routers A (does not require IPv6 routing) and Router 2.

>> Verify the IPv4 routing tables (`show ip route`). Router2’s Loopback should be visible from Router 1, and vice-versa

Configure an GRE IPv4 tunnel (with overlay networks 10.1.1.0/30 and 2001::/64). On Router 1:

```
Router1(config)# interface Tunnel1
Router1(config-if)# ip address 10.1.1.1 255.255.255.252
Router1(config-if)# ipv6 address 2001::1/64
Router1(config-if)# tunnel source Loopback0
Router1(config-if)# tunnel destination 200.0.0.2
Router1(config-if)# tunnel mode gre ip
```

Configure also the overlay network routing with IPv4 and IPv6 static routes to the remote private networks (PC networks):

```
Router1(config)# ip route 192.168.2.0 255.255.255.0 Tunnel1
Router1(config)# ipv6 route 2001:2:2::/64 Tunnel1
```

Perform the equivalent configuration on Router2.

Verify the IPv4 and IPv6 routing tables. From PC1 ping PC2 (using IPv4 and IPv6 addresses) while capturing packets on links R1-RA and RA-R2.

>>Analyze the dual IP headers (of overlay and underlying networks, respectively.

Note: tunnel end points virtual interfaces (VTI) do not require the same ID number, however, good configuration guidelines strongly recommend it.

With Route Maps

2. Replace the IPv4 and IPv6 static routes by Route Maps. On Router 1:

```
Router1(config)# no ip route 192.168.2.0 255.255.255.0 Tunnel1
Router1(config)# no ipv6 route 2001:2:2::/64 Tunnel 1
!
Router1(config)# ipv6 access-list L101
Router1(config-ipv6-acl)# sequence 20 permit ipv6 2001:1:1::/64 2001:2:2::/64
Router1(config)# access-list 100 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
!
Router1(config)# route-map routeT1 permit 10
Router1(config-route-map)# match ip address 100
Router1(config-route-map)# set ip next-hop 10.1.1.2
Router1(config)# route-map route6T1 permit 10
Router1(config-route-map)# match ipv6 address L101
Router1(config-route-map)# set ipv6 next-hop 2001::2
!
Router1(config)# interface FastEthernet0/1
Router1(config-if)# ip policy route-map routeT1            ! IPv4 policy routing activation
Router1(config-if)# ipv6 policy route-map route6T1         ! IPv6 policy routing activation
```

Perform the equivalent configuration on Router2.

>> Verify the IPv4 and IPv6 routing tables (note the absence of routes to the remote private networks).

>> From PC1 ping PC2 (using IPv4 and IPv6 addresses) while capturing packets on links R1-RA and RA-R2.

>> Analyze the route-map statistics (`show route-map routeT1`).

With Dynamic Routing

3. Replace the IPv4 and IPv6 Route Maps with Dynamic Routing by activating a second OSPF and OSPFv3 process (process 2) within the overlay network (tunnel network and private networks), on Router 1:

```
Router1(config)#interface FastEthernet0/1
Router1(config-if)# no ip policy route-map routeT1
Router1(config-if)# no ipv6 policy route-map route6T1
!
Router1(config)#interface Tunnel1
Router1(config-if)# ip ospf 2 area 0
Router1(config-if)# ipv6 ospf 2 area 0
Router1(config)# interface FastEthernet0/1
Router1(config-if)# ip ospf 2 area 0
Router1(config-if)# ipv6 ospf 2 area 0
```

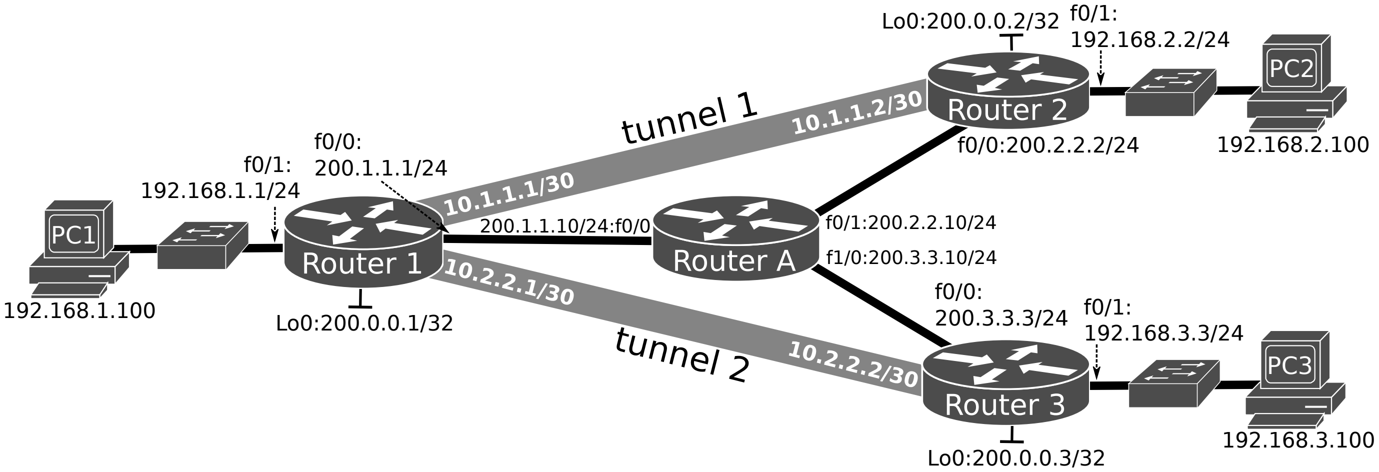
Perform the equivalent configuration on Router2.

>> Verify the IPv4 and IPv6 routing tables.

>> From PC1 ping PC2 (using IPv4 and IPv6 addresses) while capturing packets on links (R1-RA and RA-R2).

>> Analyze the exchanged OSPF and OSPFv3 packets exchanged over the overlay network with dual IP headers (networks 10.1.1.0/30 and fe80::/10).

Overlay Network with Partial Mesh GRE IPv4 Tunnels



4. Connect Router 3 to the network and update OSPF process 1, add an new private network (PC3 network) with address 192.168.3.0/24 and Router3 as gateway, and configure an additional tunnel (Tunnel2) between Router1 and Router3 (network 10.2.2.0/30) to create a partial mesh of IPv4 tunnels to extend the overlay network.

Update the overlay network OSPF routing process to include the new overlay link (Tunnel2), on Router1:

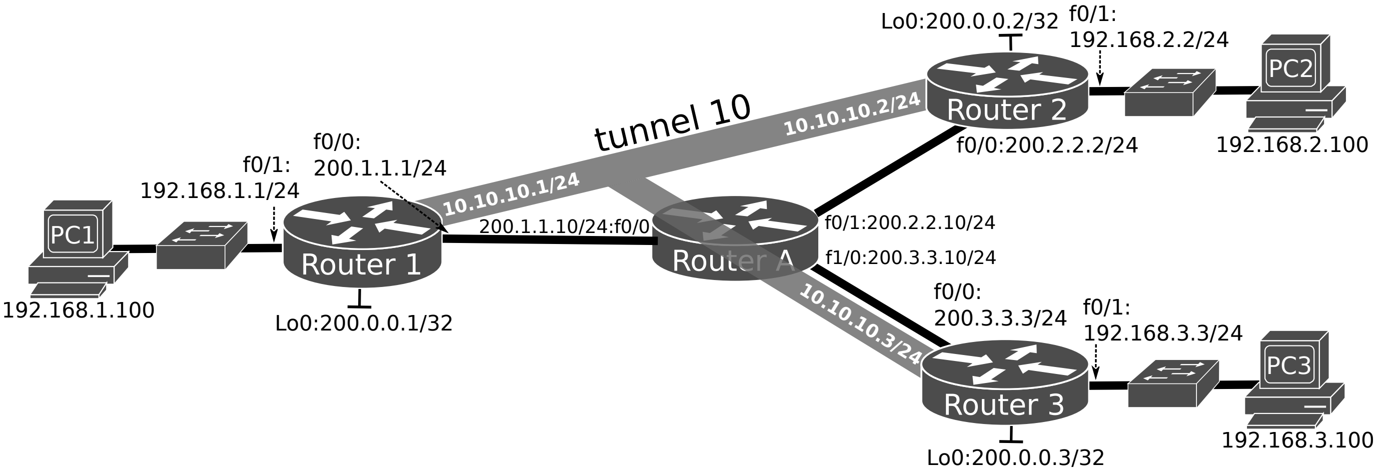
```
Router1(config)# interface Tunnel2
Router1(config-if)# ip ospf 2 area 0
```

On Router3:

```
Router1(config)# interface Tunnel2
Router1(config-if)# ip ospf 2 area 0
Router1(config)# interface FastEthernet0/1
Router1(config-if)# ip ospf 2 area 0
```

Verify the IPv4 routing tables. From PC3 ping PC2 (using IPv4 addresses) while capturing packets on links R1-RA and RA-R2. Analyze the captured packets and explain the duplicated packets. Explain the main disadvantage of having a tunnel partial mesh overlay network.

IPv4-IPv4 Multipoint Tunnel with NHRP and Static Routing



5. Shutdown Tunnel1 and Tunnel2 where configured:

```
Router1(config)# interface Tunnel1
Router1(config-if)# shutdown
Router1(config)# interface Tunnel2
Router1(config-if)# shutdown
```

Configure an IPv4-IPV4 Multipoint GRE Tunnel (Tunnel10) with NHRP (network-id 1 and key 1) in a Hub-Spokes architecture where Router1 assumes the hub role. On Router1 (Hub):

```
Router1(config)# interface Tunnel10
Router1(config-if)# ip address 10.10.10.1 255.255.255.0
Router1(config-if)# ip nhrp network-id 1
Router1(config-if)# tunnel source Loopback0
Router1(config-if)# tunnel mode gre multipoint
Router1(config-if)# tunnel key 1
```

On Router2 and Router3 (Spokes):

```
Router2(config)# interface Tunnel10
Router2(config-if)# ip address 10.10.10.2 255.255.255.0          !Router2
                    (#ip address 10.10.10.3 255.255.255.0            !Router3)
Router2(config-if)#ip nhrp network-id 1
Router2(config-if)#ip nhrp nhs 10.10.10.1
Router2(config-if)#ip nhrp map 10.10.10.1 200.0.0.1
Router2(config-if)#tunnel source Loopback0
Router2(config-if)#tunnel mode gre multipoint
Router2(config-if)#tunnel key 1
```

Configure static routing:

```
Router1(config)# ip route 192.168.2.0 255.255.255.0 10.10.10.2
Router1(config)# ip route 192.168.3.0 255.255.255.0 10.10.10.3
```

Perform the equivalent configuration on Router2 and Router3.

>> Verify IPv4-IPv4 NHRP mappings with: `#show ip nhrp`

>> Verify the IPv4 routing tables.

From PC3 ping PC2 (using IPv4 addresses) while capturing packets on links R1-RA and RA-R2.

>> Re-verify IPv4-IPv4 NHRP mappings. Explain the differences.

>> Analyze the NHRP packets and explain the absence of duplicated ICMP packets after a few tries.

>> Explain the main advantage of having a multipoint tunnel with NHRP overlay network.

IPv4-IPv4 Multipoint Tunnel with NHRP and Dynamic Routing

6. Remove all static routing configurations. As configured on experiments 1 and 3, the underlying network already has an OSPF routing process (process 1) and the private networks interfaces already have an OSPF process active (process 2). Additional commands on Router1 (Hub):

```
Router1(config)# interface Tunnel10
Router1(config-if)# ip ospf 2 area 0
Router1(config-if)# ip nhrp map multicast dynamic
Router1(config-if)# ip ospf network broadcast
Router1(config-if)# ip ospf priority 2
```

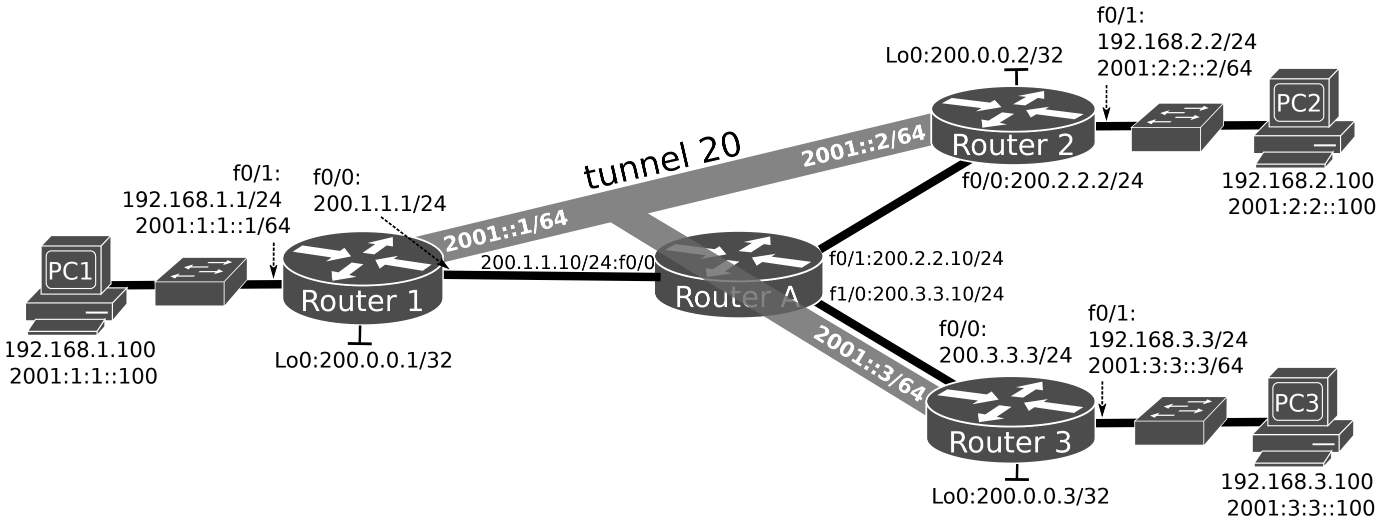
Additional commands on Router2 and Router3 (Spokes):

```
Router2(config)# interface Tunnel10
Router2(config-if)# ip ospf 2 area 0
Router2(config-if)# ip nhrp map multicast 200.0.0.1
Router2(config-if)# ip ospf network broadcast
Router2(config-if)# ip ospf priority 0
```

>> Verify the IPv4 routing tables and IPv4-IPv4 NHRP mappings. Re-test the overall connectivity between the private networks.

>> Analyze the NHRP packets. Re-verify IPv4-IPv4 NHRP mappings.

(Optional) IPv6-IPv4 Multipoint Tunnel with NHRP and Dynamic Routing



As configured on experiments 1 and 3, the underlying network already has an OSPFv2 routing process (process 1). Add OSPFv3 configurations at Router 3 for the PCs' networks. Configure a new IPv6-IPV4 Multipoint GRE Tunnel (Tunnel20) with NHRP (network-id 2 and key 2) in a Hub-Spokes architecture where Router1 assumes the hub role. On Router1 (Hub):

```
Router1(config)# interface Tunnel20
Router1(config-if)# ipv6 address 2001::1/64
Router1(config-if)# ipv6 nhrp network-id 2
Router1(config-if)# ipv6 nhrp map multicast dynamic
Router1(config-if)# tunnel source Loopback0
Router1(config-if)# tunnel mode gre multipoint
Router1(config-if)# tunnel key 2
Router1(config-if)# ipv6 ospf 2 area 0
Router1(config-if)# ipv6 ospf network broadcast
Router1(config-if)# ipv6 ospf priority 2
```

On Router2 and Router3 (Spokes):

```
Router2(config)# interface Tunnel20
```

```
Router2(config-if)# ipv6 address 2001::2/64     ! Router 2
                    (# ipv6 address 2001::3/64      ! Router 3)
Router2(config-if)# ipv6 nhrp nhs 2001::1
Router2(config-if)# ipv6 nhrp map 2001::1/64 200.0.0.1
Router2(config-if)# ipv6 nhrp map multicast 200.0.0.1
Router2(config-if)# ipv6 nhrp network-id 2
Router2(config-if)# tunnel source Loopback0
Router2(config-if)# tunnel mode gre multipoint
Router2(config-if)# tunnel key 2
Router2(config-if)# ipv6 ospf network broadcast
Router2(config-if)# ipv6 ospf priority 0
Router2(config-if)#ipv6 ospf 2 area 0
```

Verify IPv6-IPv4 NHRP mappings with:

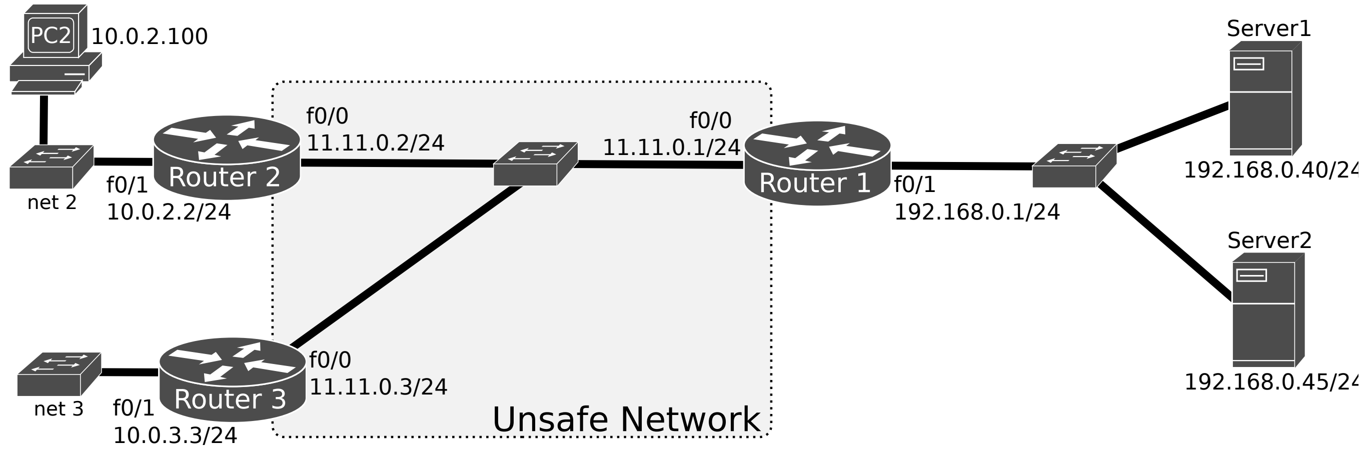
```
Router2# show ipv6 nhrp
```

>> Verify the IPv6 routing tables. Re-test the overall connectivity between the private networks.

>> Analyze the NHRP packets. Re-verify IPv6-IPv4 NHRP mappings.

IPSec Tunneling

1. Using GNS3, configure a network according to the following figure. Use two VPCS to emulate the two servers 192.168.0.40 and 192.168.0.45. Configure IPv4 addresses and routing (OSPF) for the public/unsafe network and test the existence of full connectivity between routers before initiating the IPsec configuration.



2. Consider that network 11.11.0.0/24 is unsafe. Therefor, all important traffic must be transported securely using an IPSec tunnel. Consider all IP communication between network 10.0.2.0/24 and Server2 as important traffic, all other traffic can be transmitted unencrypted through network 11.11.0.0/24. Router2 configuration (IPSec only) is the following:

```
 Router2(config)# crypto isakmp policy 30        ! The number defines the order of preference
 Router2(config-isakmp)# authentication pre-share                  ! Auth. with password
 Router2(config)# crypto isakmp key labcom address 11.11.0.1            ! Passw. with Router1
 Router2(config)# crypto ipsec transform-set authT ah-sha-hmac                        ! AH
 Router2(config)# crypto ipsec transform-set cipherT esp-des               ! ESP with DES
 Router2(config)# crypto ipsec transform-set auth_ciphT ah-sha-hmac esp-des  ! AH+ESP
 Router2(config)# crypto ipsec profile ARipsec              ! Defines tunnel type/protocols
 Router2(ipsec-profile)# set transform-set authT cipherT  auth_ciphT     !Order def. prefs.
---
 Router2(config)# interface Tunnel 0
 Router2(config-if)# ip unnumbered FastEthernet0/0
 Router2(config-if)# tunnel source 11.11.0.2
 Router2(config-if)# tunnel destination 11.11.0.1
 Router2(config-if)# tunnel mode ipsec ipv4
 Router2(config-if)# tunnel protection ipsec profile ARipsec
 Router2(config)# ip route 192.168.0.45 255.255.255.255 Tunnel 0           ! Route to Server 2
```

Configure Router1 using a similar and compatible (crypto) IPsec configuration and define the Tunnel:

```
 Router1(config)# interface Tunnel 0
 Router1(config-if)# ip unnumbered FastEthernet0/0
 Router1(config-if)# tunnel source 11.11.0.1
 Router1(config-if)# tunnel destination 11.11.0.2
 Router1(config-if)# tunnel mode ipsec ipv4
 Router1(config-if)# tunnel protection ipsec profile ARipsec
 Router1(config)# ip route 10.0.2.0 255.255.255.0 Tunnel 0                 ! Return route
```

Note: the underline words are user-defined names. Execute (in Router 1 and 2) the commands:

```
 # show crypto isakmp policy
 # show crypto ipsec transform-set
 # show crypto map
```

>> Explain the information returned by the routers.

3. Disable the IPsec tunnel interface in Router 2:

```
Router2(config)# interface Tunnel0
Router2(config-if)# shutdown
```

Start a capture on network 11.11.0.0/24 and re-enable the IPsec tunnel interface:

```
Router2(config)# interface Tunnel0
Router2(config-if)# no shutdown
```

>>Analyze the captured ISAKMP packets.

4. Start a capture on network 11.11.0.0/24. From PC2 ping both servers (192.168.0.40 and 192.168.0.45). Explain the differences between the two ICMP flows. Which is the IPSec protection mechanisms (AH, ESP or AH+ESP) been used for the traffic between network 10.0.2.0/24 and Server2?

5. Change the routers configuration (IPSec profiles) in order to use the two remaining protection mechanisms.

```
 Router2(config)# crypto ipsec profile ARipsec
 Router2(ipsec-profile)# set transform-set cipherT  authT  auth_ciphT
 ------
 Router2(ipsec-profile)#set transform-set auth_ciphT  authT  cipherT
```

Clear the tunnel IPsec active connections with commands: `shutdown`, `no shutdown`.

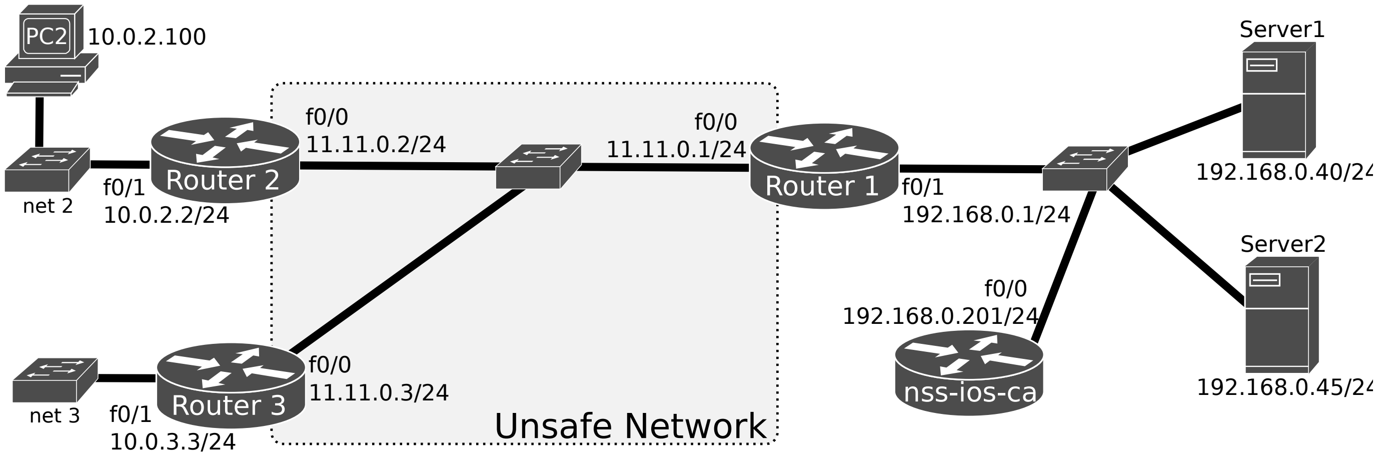
Test the configurations by pinging Server2 from PC2 and capturing the traffic flowing between Router2 and Router1.

>> Explain the differences between the 3 IPSec protection protocols.

IOS Certification Authority

In all Routers: disable the option “Automatically delete NVRAM and disk files” in Configure->Memories and disks

7. Configure the IP addresses, routers 1,2 and 3 host names (using the command `hostname <name>`) and routing of the network depicted in the following figure.



8. Configure Router nss-ios-ca as a Certification Authority.

Verify if the clock router is correct (`#show clock`), if not set it up:

```
Router# clock set <hh:mm:ss day month year>  !ex: 12:10:00 1 May 2021
Router(config)# clock timezone GMT 0
```

Configure the router’s name and deploy the CA:

```
Router(config)# hostname nss-ios-ca
nss-ios-ca(config)# ip http server
nss-ios-ca(config)# crypto key generate rsa general-keys label nss-ios-ca modulus 1024 exportable
nss-ios-ca(config)# crypto key export rsa nss-ios-ca pem url nvram: 3des labcomlabcom
nss-ios-ca(config)# crypto pki server nss-ios-ca
nss-ios-ca(cs-server)# database level names
nss-ios-ca(cs-server)# issuer-name CN = nss-ios-ca, O = University of Aveiro
nss-ios-ca(cs-server)# lifetime crl 24
nss-ios-ca(cs-server)# lifetime certificate 365
nss-ios-ca(cs-server)# lifetime ca-certificate 750
nss-ios-ca(cs-server)# no shutdown
```

Check CA server and certificates with the commands:

```
nss-ios-ca# show crypto pki server
nss-ios-ca# show crypto pki certificates
nss-ios-ca# dir nvram:
nss-ios-ca# more nvram:<file>
```

9. In Routers 1 and 2, verify if the clock router is correct (#show clock), if not set it up:

```
Router# clock set <hh:mm:ss day month year>  !ex: 12:10:00 1 May 2021
Router(config)# clock timezone GMT 0
```

Enroll Routers 1 and 2 with the CA and import certificates.

```
Router1(config)# ip domain name labcom.ua.pt
Router1(config)# ip host nss-ios-ca 192.168.0.201
Router1(config)# crypto key generate rsa general-keys modulus 1024
Router1(config)# crypto pki trustpoint nss-ios-ca
Router1(ca-trustpoint)# enrollment url http://nss-ios-ca:80
Router1(ca-trustpoint)# exit
Router1(config)# crypto pki authenticate nss-ios-ca      ! check fingerprint, say yes
Router1(config)# crypto pki enroll nss-ios-ca
                                                  ! any password (used for revoking), yes to request
```

Check certificates with the commands:

```
Router1# show crypto pki certificates
Router1# dir nvram:
```

Repeat similar configurations in Router2 with two exceptions:

The communication with CA should be made using a secure tunnel, therefore add a static route to force traffic to CA via the IPsec tunnel to force traffic to go through the previously configured IPsec tunnel.

```
Router2(config)# ip route 192.168.0.201 255.255.255.255 Tunnel 0
```

The router should not try to obtain the CRL every time it requires the use of a certificate (may not exist a secure connection to the CA).

```
Router2(config)# crypto pki trustpoint nss-ios-ca
Router2(ca-trustpoint)# revocation-check crl none
!this command makes the router to first try to obtain the CRL but if it fails it continues.
```

10. At the CA, manual approve the routers enrollment and certificates:

```
nss-ios-ca# show crypto pki server nss-ios-ca requests
        !for IOS older version 12.x       nss-ios-ca# crypto pki server nss-ios-ca info requests
nss-ios-ca# crypto pki server nss-ios-ca grant <ReqID>
```

Re-check certificates at the routers with the commands:

```
show crypto pki certificate
dir nvram:
```

Wait (1-2 minutes) until Routers 1 and 2 obtain a valid (available) certificate.

IPSec Tunnel with PKI authentication

11. Re-configure the IPsec tunnel to use with a ISAKMP policy with lower precedence (first choice) that uses PKI authentication with Digital Certificates (RSA-signatures). In booth Router1 and Router2 add:

```
Router(config)# crypto isakmp policy 10
Router(config-isakmp)# encr 3des
                              !default authentication uses Digital Certificates (rsig), so no command is necessary
Router(config-isakmp)# group 2
```

Check the details of the IPsec ISAKMP SA with:

```
# show crypto isakmp sa detail
```

Clear all IPsec active connections with command `clear crypto sa` and disable/enable the IPsec tunnel at Router 2. Re-check the details of the IPsec ISAKMP SA (namely Auth mode)-

Start a packet capture at the central network (11.11.0.0) and test the IPsec tunnel at Router 2 with the command:

```
# ping 192.168.0.45
```

Check the details of the IPsec ISAKMP SA with:

```
# show crypto isakmp sa detail
```

>> What can you conclude how the information is exchanged between routers in this scenario?

Remove the IPsec tunel (Tunnel 0) in both end-points.

Dynamic Multipoint VPNs (DMVPN) with hub-and-spoke design

12. Establish a DMVPN with a Hub-and-spokes design between Routers 1, 2 and 3. Where Router 1 is the hub and the others the spokes. Use network 10.100.0.0/24 for the tunnel interfaces network. Active a second OSPF process for the overlay network. To configure Router 1 as DMVPN Hub, perform the following commands:

```
Router1(config)# interface FastEthernet0/1
Router1(config-if)# ip ospf 2 area 0
Router1(config)# interface Tunnel 1
Router1(config-if)# ip address 10.100.0.1 255.255.255.0
Router1(config-if)# ip nhrp authentication nss-auth
Router1(config-if)# ip nhrp map multicast dynamic
Router1(config-if)# ip nhrp network-id 123
Router1(config-if)# ip nhrp holdtime 600
Router1(config-if)# ip ospf network broadcast
Router1(config-if)# tunnel source FastEthernet0/0
Router1(config-if)# tunnel mode gre multipoint
Router1(config-if)# tunnel key 12345
Router1(config-if)# tunnel protection ipsec profile ARipsec
Router1(config-if)# ip ospf 2 area 0
```

To configure Router 2 as a DMVPN Spoke, perform the following commands:

```
Router2(config)# interface FastEthernet0/1
Router2(config-if)# ip ospf 2 area 0
Router2(config)# interface Tunnel 1
Router2(config-if)# ip address 10.100.0.2  255.255.255.0
Router2(config-if)# ip nhrp authentication nss-auth
Router2(config-if)# ip nhrp nhs 10.100.0.1                   !hub definition
Router2(config-if)# ip nhrp map 10.100.0.1 11.11.0.1
Router2(config-if)# ip nhrp map multicast 11.11.0.1
Router2(config-if)# ip nhrp network-id 123
Router2(config-if)# ip nhrp holdtime 600
```

```
Router2(config-if)# ip ospf network broadcast
Router2(config-if)# tunnel source FastEthernet0/0
Router2(config-if)# tunnel destination 11.11.0.1
Router2(config-if)# tunnel key 12345
Router2(config-if)# tunnel protection ipsec profile ARipsec
Router2(config-if)# ip ospf 2 area 0
```

Perform a similar configuration in Router 3. Check the routing tables, start a packet capture at the central network (11.11.0.0) and perform pings between the routers. Analyze the captured packets and using the following commands verify the NHRP mapping tables and established secure connections:

```
# show dmvpn            !MAY NOT EXIST IN SOME IOS VERSIONS
# show ip nhrp
# show crypto sockets
# show crypto map
```

>> What can you conclude how the information is exchanged between Routers 2 and 3 in a DMVPN with an Hub-and-spoke design?

(optional) DMVPN with a mesh spoke-to-spoke design

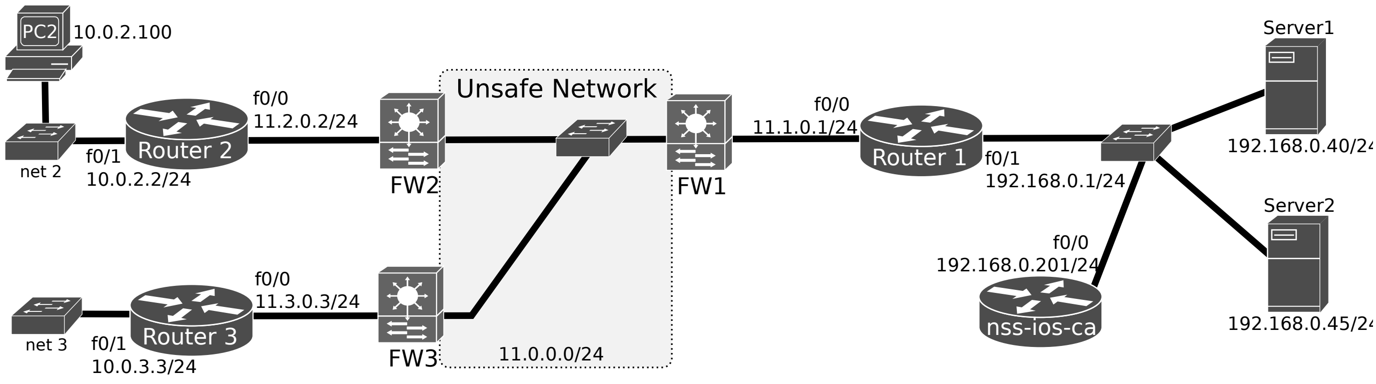
13. Establish a DMVPN with a spoke-to-spokes design between Routers 1, 2 and 3. Where Router 1 is the hub and the others the spokes. Router 1 configuration is the same as in experiment 7. In Routers 2 and 3 the tunnel mode should be GRE Multipoint:

```
Router2(config)# interface Tunnel 0
Router2(config-if)# no tunnel destination 11.11.0.1
Router2(config-if)# tunnel mode gre multipoint
```

Perform a similar configuration in Router 3. Do a shutdown/no shutdown cycle in the tunnels of all routers to reset them. Check the routing tables, start a packet capture at the central network (11.11.0.0) and perform pings between the routers. Analyze the captured packets and verify the NHRP mapping tables and established secure connections.

>>What can you conclude now how the information is exchanged between Routers 2 and 3 with an spoke-to-spoke design?

(optional) Firewalls' Policies



14. Assume that a firewall is controlling the traffic flow between the internal and the external/unsafe network. Create the necessary zones and flow control policies :

- To allow the establishment of the site-to-site VPN connections;

- To allow the exchange of data through the established site-to-site VPN connections.