Final Practice : Autonomous Systems

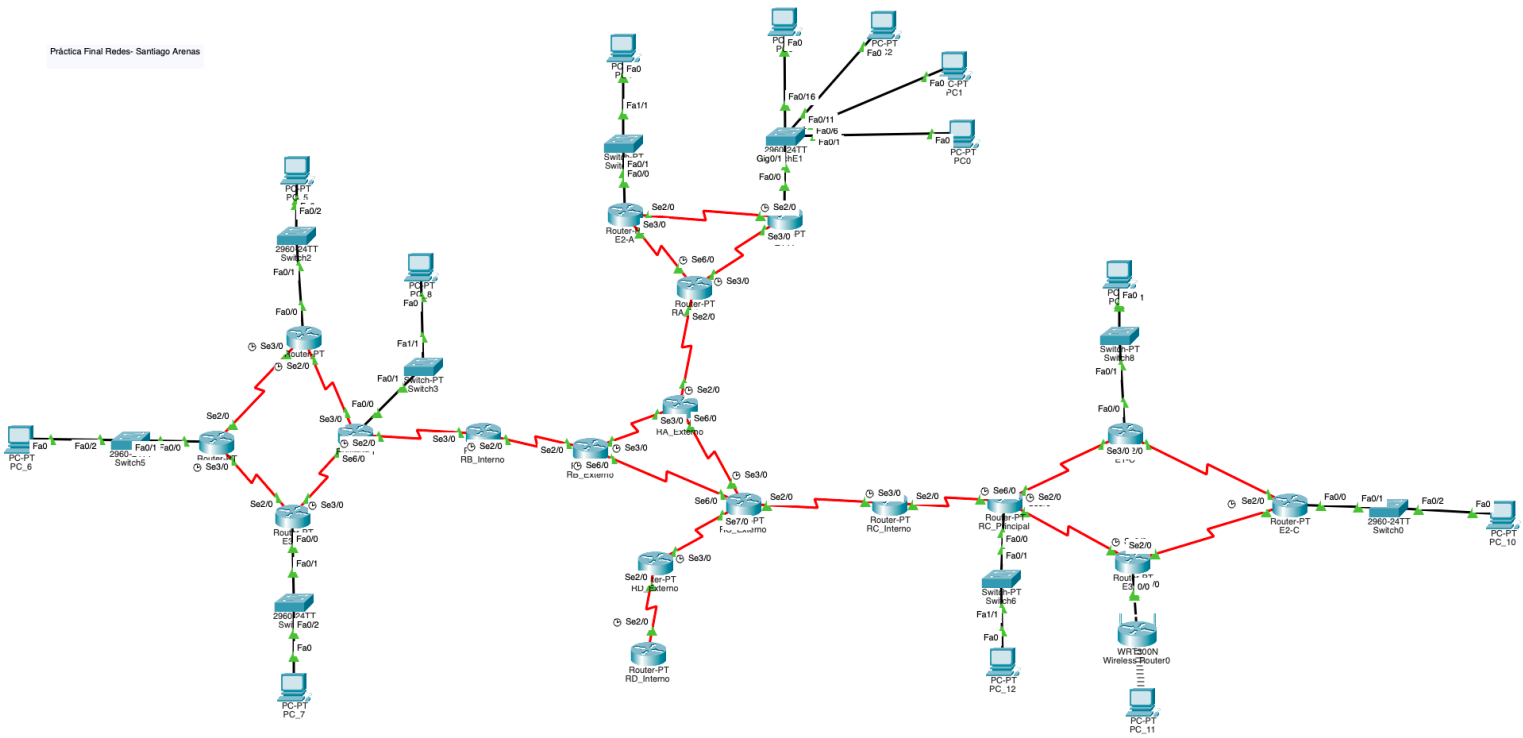
Santiago Arenas Martín - España | Network Architecture | 2024

Introduction

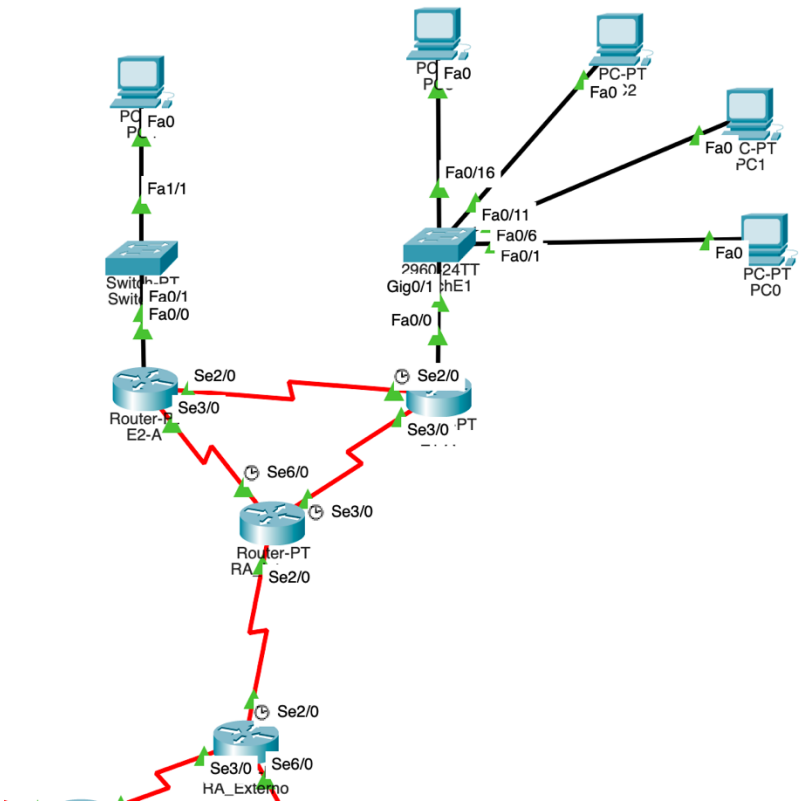
In this final practice, we have been tasked with designing a network that meets certain requirements. We must create a global network composed of four autonomous systems, implement internal routing protocols, and respect traffic limitations using access control lists (ACLs).

We will apply the knowledge gained in class to configure Layer 2 and 3 devices, set ACL constraints, and configure system-wide routing to ensure connectivity between all devices except those with ACL restrictions. We will use variable length masks (VLSM) and classless routing between domains (CIDR), choosing the optimal path based on the number of hops.

These four systems will be interconnected through their border routers, with the Autonomous C System acting as the interconnection core. Routing will be optimized to minimize the number of hops.



Development of the Practice



Autonomous System A

Autonomous System A is composed of two companies that implement OSPF. This protocol is efficient and scalable, ideal for large networks due to its ability to know the topology and select the shortest path . In this topology, an internal router A will connect the two companies, while an external router A will handle the external connections.

Company 1

Four Class C addresses (range 192.0.0.0 – 223.255.255.0) are required, resulting in a total of 1024 hosts/IP addresses. We'll use a /22 mask and the 199.1.0.0/22 network address, dividing the network into four departments:

• 199.1.0.0/24 (VLAN 2; Interfaces Fa0/1 - 5)• 199.1.1.0/24 (VLAN 3; Interfaces Fa0/6 - 10)• 199.1.2.0/24 (VLAN 4; Interfaces Fa0/11 - 15)• 199.1.3.0/24 (VLAN 5; Interfaces Fa0/16 - 20)

Each company will have its VLAN assigned. The IP addresses assigned to the hosts are:

PC	IP Address	Gateway	Mask
PC – 0	199.1.0.0	255.255.255.0	199.1.0.1
PC – 1	199.1.1.0	255.255.255.0	199.1.1.1
PC – 2	199.1.2.0	255.255.255.0	199.1.2.1
PC – 3	199.1.3.0	255.255.255.0	199.1.3.1
PC – 4	199.1.8.0	255.255.248.0	199.1.5.1

Company 2

This company has direct access from its main router to a LAN with 2048 IP addresses, equivalent to eight Class C addresses. We will use the public address 199.1.8.0/21.

The routing protocol used is OSPF.

Router-to-router networks use the following IP addresses:

- 10.0.1.0/24
- 10.0.2.0/24
- 10.0.3.0/24
- 10.0.4.0/24

Setup in Packet Tracer

1. Creation of all VLANs, assignment to the interfaces that appear in the range.
2. Internal router configuration. Here it is assigned encapsulation followed by the VLAN number.

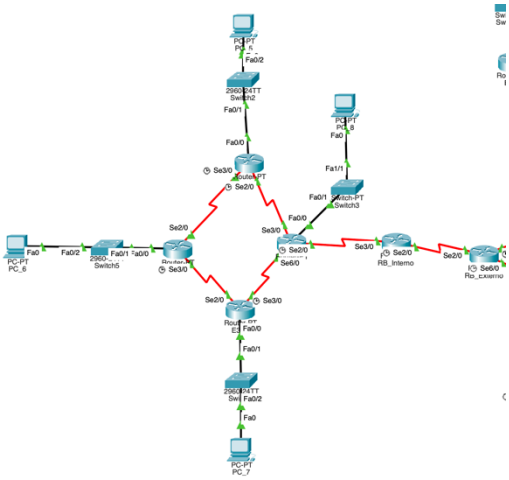
```
Router(config-subif)#interface fa0/0.4
Router (config-subif)#encapsulation dotlq 4
Router (config-subif)#ip address 199.1.2.1 255.255.255.0
```

3. Configuration of the router of the second company, to which you only have to assign the specified IP address.
4. Configuring networks between routers, each interface with your network.

Subsequently, the OSPF must be configured, which consists of two steps, a previous one where loopback 0 is configured on all the interfaces of the routers present in the autonomous system, assigning them IP addresses from 1.1.1.1 to 4.4.4.4, with masks 255.255.255.255. Then OSPF is configured, entering codes such as the external router A:

```
Router(config)#router ospf 1
Router (config-router)#network 10.0.3.0 0.0.0.255 area 0
Router (config-router) #exit
Router (config)#exit
```

For the other routers, you must declare the networks to which you are directly connected to network area 0.



Autonomous System B

For this autonomous system, we use the address range 200.0.0.0 – 200.0.127.0. Four subnets are created with 32
IP addresses each, or in other words, a network with a /27 mask:

• Department 1: 200.0.8.0/27• Department 2: 200.0.8.32/27• Department 3: 200.0.8.64/27• Department 4: 200.0.8.96/27

Router-to-router networks use the following IP addresses:

• 200.0.8.128/27• 200.0.8.160/27• 200.0.8.192/27• 200.0.8.224/27

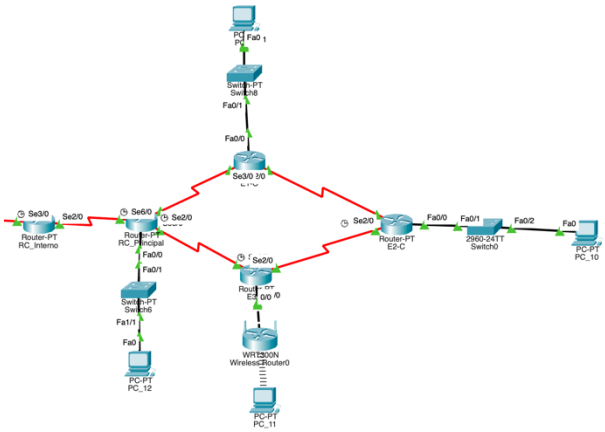
The RIP v1 routing protocol is used, which is simple to implement and maintain. The IP addresses assigned to PCs are:

PC	IP Address	Gateway	Mask
PC – 5	200.0.8.2	255.255.255.224	200.0.8.1
PC – 6	200.0.8.34	255.255.255.224	200.0.8.33
PC – 7	200.0.8.66	255.255.255.224	200.0.8.65
PC – 8	200.0.8.98	255.255.255.224	200.0.8.97

Inter-router addresses use the ranges 192.168.0.0/24 and 192.168.1.0/24.

Setup in Packet Tracer

3. Configuring RIP v1 on enterprise routers.
2. Configuration of networks between routers that are not part of the company.
3. Implementation of RIP v1 between the edge, internal and main router .
4. Implementation of an ACL on the main router that allows only HTTP or TELNET traffic from outside the company network
.



Autonomous System C

This system uses the same address scheme as Autonomous System B, with the difference that the connections between the routers use the 10.0.0.0 network.

One of the routers is connected to an access point for a private Wi-Fi network with 256 addresses. There are no ACL restrictions between the subnets and the outside.

The networks assigned to the departments are:

• Department 1: 201.0.8.0/27• Department 2: 201.0.8.32/27• Department 3: 201.0.8.64/27• Department 4: 201.0.8.96/27

Connections between routers use subnets:

• 10.0.0.0/30• 10.0.0.4/30• 10.0.0.8/30• 10.0.0.12/30

The connections between the main, internal, and external router use the subnets:

• 192.168.2.0/30• 192.168.2.4/30

The IP addresses assigned to PCs are:

PC	IP Address	Gateway	Mask
PC – 9	201.0.8.2	255.255.255. 224	201.0.8.1
PC – 10	201.0.8.34	255.255.255. 224	201.0.8.33
PC – 11	192.168.0.2	255.255.255. 224	192.168.0.1
PC – 12	201.0.8.98	255.255.255. 224	201.0.8.97

The RIP v2 routing protocol is used, which allows classless addresses to be used.

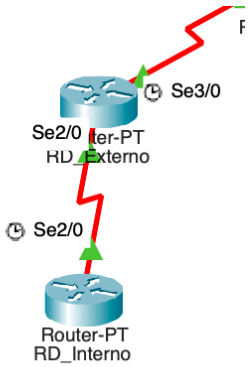
Wi-Fi network

Department 3 connects via Wi-Fi to the private network 192.168.1.0/24, which has the required 256 addresses . Devices are connected via IP assignment by DHCP.

Setup in Packet Tracer

1. RIP v2 configuration (disabling auto-summarization).
2. Setting up the Wi-Fi network on the Fa0/1 interface and the private network on the Fa0/0.
3. Enabling classless routing.

Autonomous System D



In this node router will be connected an internal router. The internal router will have a virtual interface with a loopback network with 64,536 addresses (with a /16 mask). The router to this network will be configured statically using the 220.0.0.0/30 network for the link between routers. However, the addresses we will assign will be 171.1.0.0/16.

Routing must be done statically, with internal router D having the address 220.0.0.2 for the interface that connects it to the other router and, with loopback 0, housing all the addresses of 171.1.0.0/16.

Cross-network configuration

The BGP protocol is used between them. To do this, the networks between the routers are defined, which will be the following:

- 175.1.0.0/30
- 175.1.0.4/30
- 175.1.0.8/30
- 175.1.0.12/30

Once the IP addresses have been assigned to the ports between the routers, the numbers of the autonomous systems are assigned, which has been decided as follows:

HS TO → 1

SA B → 2

SA C → 3

HS D → 4

An example of what a configuration might look like is as follows:

Router (config)#router bgp 1

Router (config-router)#neighbor 175.1.0.2 remote-as 2

Router (config-router)#neighbor 175.1.0.5 remote-as 3

Router (config-router)#redistribute connected

Router (config-router)#redistribute ospf 1

First it is declared that router A is the boundary of SA A, then the neighbors and where they are accessible are declared and, finally, that any traffic coming from OSPF is redirected there. The networks inside the router must also be declared with their corresponding mask.

Finally, the router gateways must be configured. The internal ones have to be redirected to the external ones, while the external ones have to point towards the external router of SA C, since it is the one with the most declared networks, although it could be made to point to whichever one it is. The external router of SA C points with its default to that of SA B.

Connectivity test

To check that the model works according to all the restrictions, we perform the following pings between autonomous systems.

We start with a ping between AS A and AS B, specifically from PC2 to PC_5. As we can see, the ICMP protocol returns "unreachable host", which, according to the established ACLs, demonstrates its correct behavior since only http and telnet traffic are supported in AS B.

```
C:\>ping 200.0.8.2

Pinging 200.0.8.2 with 32 bytes of data:

Reply from 192.168.0.1: Destination host unreachable.
Reply from 192.168.0.1: Destination host unreachable.
Reply from 192.168.0.1: Destination host unreachable.
Reply from 192.168.0.1: Destination host unreachable.

Ping statistics for 200.0.8.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Next, a ping between AS A and AS C, specifically from PC1 to PC9. In this case, there is connectivity according to the specifications.

```
C:\>ping 199.1.3.2

Pinging 199.1.3.2 with 32 bytes of data:

Reply from 199.1.3.2: bytes=32 time=78ms TTL=120
Reply from 199.1.3.2: bytes=32 time=132ms TTL=120
Reply from 199.1.3.2: bytes=32 time=8ms TTL=120
Reply from 199.1.3.2: bytes=32 time=110ms TTL=120
```

Finally, we make two pings to confirm that the ACLs of the autonomous system A are working. VLAN 2, corresponding to department 1, must not have connectivity to the outside other than web traffic. Therefore, we do a first ping to check that there is no connectivity with the outside world and then another to make sure that there is connectivity with the other departments.

```
C:\>ping 201.0.8.1

Pinging 201.0.8.1 with 32 bytes of data:

Reply from 199.1.0.1: Destination host unreachable.
Reply from 199.1.0.1: Destination host unreachable.
Reply from 199.1.0.1: Destination host unreachable.
Reply from 199.1.0.1: Destination host unreachable.

Ping statistics for 201.0.8.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Conclusion

The implementation of these four autonomous systems in a global network has demonstrated the importance of proper planning and detailed configuration of routing protocols. Each stand-alone system was configured to meet specific requirements, using different protocols and network configurations to ensure optimal and secure connectivity. The practice has been a valuable exercise in the application of network theories and techniques in a realistic scenario that allows all the content learned in this course to be valued.