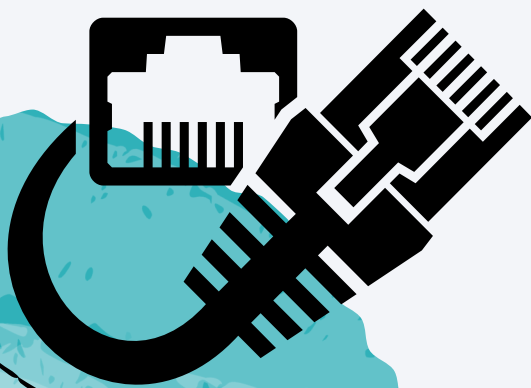


DISEÑO LÓGICO
E
INTERCONEXIÓN
DE LANs



| | |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| 1. Configurar IPs dinámicas sólo en los PCs ubicados en la escuela de BCN, el resto de dispositivos tendrán IP estática. | 2 |
| 2. Configurar en el router rtBCN desde el CLI..... | 4 |
| A) Configuración básica:..... | 4 |
| B) Enrutamiento: | 7 |
| C) Líneas de entrada: | 7 |
| D) El servicio DHCP:..... | 8 |
| 3. Configurar en el resto de los routers desde el CLI únicamente: | 10 |
| A) Nombre..... | 10 |
| B) Interfaces. | 10 |
| C) Enrutamiento dinámico RIPv2. | 12 |
| D) Líneas de entrada. | 12 |
| 4. Conectar los dispositivos de la red interna en rtBCN (PCs, servidores, APs) a la vlan correspondiente. | 13 |
| 5. Configurar los conmutadores de planta swPlanta1 y swPlanta2 desde el CLI: | 13 |
| A) Configuración básica:..... | 13 |
| B) Configuración de VLAN's: | 15 |
| C) Configuración de puertos:..... | 17 |
| 6. Realizar las siguientes copias:..... | 19 |
| 7. Configurar el resto de dispositivos para proporcionar conectividad (Access points y swAula201). | 23 |
| 8. PAT y NAT..... | 26 |
| A) Configurar el PAT en el router rtBCN, de manera que: | 26 |
| B) Comprobar el funcionamiento PAT:..... | 28 |
| D) Configurar NAT en el router rtBCN para que el servidor srvBCNExtern sea accesible desde el exterior con la IP pública 44.44.44.200/24..... | 29 |
| E) Comprobar el funcionamiento NAT desde el pcISP en el web browser acceder al srvBCNExtern mediante la IP pública http://44.44.44.200. | 29 |
| 9. Para que la red interna de la escuela sea segura se deberían configurar ACLs en el rtBCN pero para que el estudiante pueda detectar de manera más fácil sus errores previos al correcto funcionamiento, se implementarían las ACLs en el rtMataro. | 30 |
| A) De la red externa y DMZ a la red interna..... | 30 |
| B) De la red externa a la DMZ..... | 31 |
| C) De la red interna a la red externa y a la DMZ. | 31 |
| 10. Comprobar que se obtiene un esquema final como el de la figura siguiente: | 34 |

1. Configurar IPs dinámicas sólo en los PCs ubicados en la escuela de BCN, el resto de dispositivos tendrán IP estática.

| DISPOSITIVO | TIPO DE ASIGNACIÓN | VLAN | RED | RANGO DE IP'S DINÁMICAS | IP ESTÁTICA | GATEWAY | MÁSCARA DE RED | DNS |
|-----------------------------------------------------------------------------------------------|--------------------|------------|--------------------|------------------------------|-----------------|-----------------|-----------------|---------|
| <i>Pcs Escuela BCN (PcProfe1, PcAlumno1, PCAlumno2, Portatil Alumno1, Portatil Invitado1)</i> | Dinámica | 11, 22, 33 | 172.20.X.0/24 | 172.20.11.11 - 172.20.11.249 | | Según VLAN | 255.255.255.0 | 8.8.8.8 |
| <i>Server-PT srvAdmons</i> | Estática | 11 | 172.20.11.0/24 | | 172.20.11.2 | 172.20.11.1 | 255.255.255.0 | 8.8.8.8 |
| <i>Server-PT srvAlumnos</i> | Estática | 22 | 172.20.22.0/24 | | 172.20.22.2 | 172.20.22.1 | 255.255.255.0 | 8.8.8.8 |
| <i>Server_PT srvTFTP</i> | Estática | 99 | 172.20.99.0/24 | | 172.20.99.4 | 172.20.99.1 | 255.255.255.0 | 8.8.8.8 |
| <i>Server-PT srvDNS</i> | Estática | | 55.55.55.0/24 | | 55.55.55.4 | 55.55.55.1 | 255.255.255.0 | 8.8.8.8 |
| <i>Server-PT srvBCNExt</i> | Estática | | 10.33.33.160/28 | | 10.33.33.174 | 10.33.33.161 | 255.255.255.240 | 8.8.8.8 |
| <i>Server-PT srvWebMataroExt</i> | Estática | DMZ | 192.168.222.160/27 | | 192.168.222.163 | 192.168.222.161 | 255.255.255.224 | 8.8.8.8 |

Producto 3: Diseño lógico e interconexión de LANs

| | | | | | | | | |
|--------------------------------------------|----------|-----|--------------------|--|-----------------|-----------------|-----------------|---------|
| Server-PT srvFTPMataroExt | Estática | DMZ | 192.168.222.160/27 | | 192.168.222.164 | 192.168.222.161 | 255.255.255.224 | 8.8.8.8 |
| Server-PT srvMataroInt | Estática | | 192.168.20.0/24 | | 192.168.20.5 | 192.168.20.1 | 255.255.255.0 | 8.8.8.8 |
| Switch swPlanta1 | Estática | 99 | 172.20.99.0/24 | | 172.20.99.2 | 172.20.99.1 | 255.255.255.0 | 8.8.8.8 |
| Switch swPlanta2 | Estática | 99 | 172.20.99.0/24 | | 172.20.99.3 | 172.20.99.1 | 255.255.255.0 | 8.8.8.8 |
| Switch swAula201 | Estática | 22 | 172.20.22.0/24 | | 172.20.22.4 | 172.20.22.1 | 255.255.255.0 | 8.8.8.8 |
| Switch swDMZ | Estática | DMZ | 192.168.222.160/27 | | 192.168.222.162 | 192.168.222.161 | 255.255.255.224 | 8.8.8.8 |
| Switch swMataro | Estática | | 192.168.20.0/24 | | 192.168.20.2 | 192.168.20.1 | 255.255.255.0 | 8.8.8.8 |
| Switch swISP | Estática | | 55.55.55.0/24 | | 55.55.55.2 | 55.55.55.1 | 255.255.255.0 | 8.8.8.8 |
| PC-PT pcISP | Estática | | 55.55.55.0/24 | | 55.55.55.3 | 55.55.55.1 | 255.255.255.0 | 8.8.8.8 |
| PC-PT pcMataro1 | Estática | | 192.168.20.0/24 | | 192.168.20.3 | 192.168.20.1 | 255.255.255.0 | 8.8.8.8 |
| PC-PT pcMataro2 | Estática | | 192.168.20.0/24 | | 192.168.20.4 | 192.168.20.1 | 255.255.255.0 | 8.8.8.8 |

2. Configurar en el router rtBCN desde el CLI.

A) Configuración básica:

Para configurar el router 'rtBCN' en Cisco Packet Tracer se debe acceder al CLI (Command Line Interface) del router y ejecutar los siguientes comandos:

I. *Nombre.*

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname rtBCN
rtBCN(config)#
```

II. *Contraseña para pasar a modo privilegiado (class).*

```
rtBCN(config)#enable secret class
rtBCN(config)#
```

III. *Mensaje de entrada: #Acceso restringido al router rtBCN#.*

```
rtBCN(config)#banner motd #Acceso restringido al router rtBCN#
rtBCN(config)#
```

IV. *Asociación del nombre de otros dispositivos con sus IPs.*

Para mejorar la gestión de la red y facilitar el acceso a dispositivos importantes, se configurará una tabla de resolución de nombres en este router mediante el comando 'ip host' que asocia un nombre fácil de recordar con la dirección IP estática de los dispositivos más cercanos:

```
rtBCN(config)#ip host srvBNCExt 10.33.33.174
rtBCN(config)#ip host rtISP 44.44.44.2
rtBCN(config)#ip host swPlantal 172.20.99.2
rtBCN(config)#end
rtBCN#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
rtBCN#
```

Una vez terminado de asociar los nombres a las direcciones IP se sale del modo configuración global y se guardan los cambios para que estos se mantengan incluso después del reinicio del router.

V. Interfaces y subinterfaces con descripción.

Cada interfaz se ha de configurar con una IP específica, una descripción clara que identifique su propósito y la conexión, y se activará para permitir la transmisión de datos. Además, las subinterfaces para VLANs se configurarán con su respectiva encapsulación y dirección IP correspondiente a la VLAN a la que sirven. Por último, se guardarán los cambios en la configuración de inicio para asegurar que las interfaces se inicialicen con estos ajustes en caso de reinicio del dispositivo.

Comenzaremos configurando la **Interfaz Gi0/1 conectada al 'srvBCNExt'**:

```
Acceso restringido al router rtBCN

rtBCN>ena
Password:
rtBCN#config t
Enter configuration commands, one per line.  End with CNTL/Z.
rtBCN(config)#interface GigabitEthernet0/1
rtBCN(config-if)#ip address 10.33.33.174 255.255.255.240
rtBCN(config-if)#no shutdown

rtBCN(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed
state to up

rtBCN(config-if)#description Conexion al servidor externo BCNExt
rtBCN(config-if)#exit
rtBCN(config)#
```

Pasaremos a configurar la **Interfaz Gi0/0 para las VLANs** conectada a los switches de Planta:

```
rtBCN(config)#interface GigabitEthernet0/0
rtBCN(config-if)#no ip address
rtBCN(config-if)#description Troncal para las VLANs
rtBCN(config-if)#no shutdown
```

Posteriormente configuraremos las VLANs:

```
rtBCN(config)#interface GigabitEthernet0/0.11
rtBCN(config-subif)#encapsulation dot1Q 11
rtBCN(config-subif)#
rtBCN(config-subif)#ip address 172.20.11.1 255.255.255.0
rtBCN(config-subif)#no shutdown
rtBCN(config-subif)#description VLAN 11 - Personal
rtBCN(config-subif)#exit
rtBCN(config)#
```

Producto 3: Diseño lógico e interconexión de LANs

```
rtBCN(config)#interface GigabitEthernet0/0.22
rtBCN(config-subif)#encapsulation dot1Q 22
rtBCN(config-subif)#ip address 172.20.22.1 255.255.255.0
rtBCN(config-subif)#no shutdown
rtBCN(config-subif)#description VLAN 22 - Alumnos
rtBCN(config-subif)#exit
rtBCN(config)#
```

```
rtBCN(config)#interface GigabitEthernet0/0.33
rtBCN(config-subif)#encapsulation dot1Q 33
rtBCN(config-subif)#ip address 172.20.33.1 255.255.255.0
rtBCN(config-subif)#no shutdown
rtBCN(config-subif)#description VLAN 33 - Wifi-Invitados
rtBCN(config-subif)#exit
rtBCN(config)#
```

```
rtBCN(config)#interface GigabitEthernet0/0.99
rtBCN(config-subif)#encapsulation dot1Q 99
rtBCN(config-subif)#ip address 172.20.99.1 255.255.255.0
rtBCN(config-subif)#no shutdown
rtBCN(config-subif)#description VLAN 99 - Administracion
rtBCN(config-subif)#exit
rtBCN(config)#
```

Por último, configuraremos la **Interfaz Serial s0/0/0** conectada al router 'rtISP':

```
rtBCN(config)#interface Serial0/0/0
rtBCN(config-if)#ip address 44.44.44.2 255.255.255.0
rtBCN(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
rtBCN(config-if)#description Conexin WAN hacia ISP
rtBCN(config-if)#exit
rtBCN(config)#
```

Guardamos correctamente toda la configuración:

```
rtBCN(config)#exit
rtBCN#
%SYS-5-CONFIG_I: Configured from console by console

rtBCN#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
rtBCN#
```

A través del comando siguiente comprobamos todas las interfaces configuradas en el router, su estado y las direcciones IP configuradas:

```
rtBCN#show ip interface brief
Interface                IP-Address      OK? Method Status
Protocol
GigabitEthernet0/0       unassigned      YES unset  administratively down down
GigabitEthernet0/0.11    172.20.11.1     YES manual  administratively down down
GigabitEthernet0/0.22    172.20.22.1     YES manual  administratively down down
GigabitEthernet0/0.33    172.20.33.1     YES manual  administratively down down
GigabitEthernet0/0.99    172.20.99.1     YES manual  administratively down down
GigabitEthernet0/1       10.33.33.174    YES manual  up          up
GigabitEthernet0/2       unassigned      YES unset  administratively down down
Serial0/0/0              44.44.44.2      YES manual  down        down
Serial0/0/1              unassigned      YES unset  administratively down down
Vlan1                    unassigned      YES unset  administratively down down
rtBCN#
```

B) Enrutamiento:

I. Enrutamiento dinámico RIPv2.

En primer lugar, vamos a especificar que vamos a usar RIPv2, que es la segunda versión del Protocol Routing Information Protocol (RIP):

```
rtBCN(config)#router rip
rtBCN(config-router)#version 2
rtBCN(config-router)#
```

Ya dentro del modo de configuración RIP, vamos a especificar qué redes queremos anunciar mediante RIP. Esto permitirá al router enviar actualizaciones de enrutamiento que incluyan esas redes a otros routers que también estén configurados para RIP:

```
rtBCN(config-router)#network 172.20.11.0
rtBCN(config-router)#network 172.20.22.0
rtBCN(config-router)#network 172.20.33.0
rtBCN(config-router)#network 172.20.99.0
rtBCN(config-router)#network 10.33.33.0
rtBCN(config-router)#network 44.44.44.0
rtBCN(config-router)#
```

Por defecto, RIPv2 realiza actualizaciones automáticas, pero podemos usar el siguiente comando para modificar el comportamiento y así evitar que RIP resuma las redes a su clase mayor, lo cual es un comportamiento predeterminado en RIPv1 pero no en RIPv2:

```
rtBCN(config-router)#no auto-summary
rtBCN(config-router)#exit
```

C) Líneas de entrada:

Para asegurar el acceso seguro al router, se configurará la línea de consola para requerir una contraseña, de forma que se prevenga el acceso no autorizado a la configuración del router a través de la interfaz física de la consola. Además, se habilitará el acceso remoto a través del Telnet para los usuarios 'admin' y 'operador' asignando una contraseña común 'dit' para ambos. Esto permitirá que los usuarios autorizados gestionen el router de forma remota. Para cada línea VTY, que permite las conexiones de Telnet, configuraremos también el router para requerir la verificación de usuario, lo que aumenta la seguridad del dispositivo y protege contra accesos no autorizados.

I. Vía telnet mediante usuarios: admin y operador con pwd dit.


```
rtBCN(config)#line vty 0 4
rtBCN(config-line)#password dit
rtBCN(config-line)#login
rtBCN(config-line)#username admin password dit
rtBCN(config)#username operador password dit
rtBCN(config)#username admin password dit
rtBCN(config)#line vty 0 4
rtBCN(config-line)#login local
rtBCN(config-line)#transport input telnet
rtBCN(config-line)#end
rtBCN#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
rtBCN#
```

II. Vía consola con password común: cisco.

```
rtBCN#config t
Enter configuration commands, one per line. End with CNTL/Z.
rtBCN(config)#line console 0
rtBCN(config-line)#password cisco
rtBCN(config-line)#login
rtBCN(config-line)#end
rtBCN#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
rtBCN#
```

D) El servicio DHCP:

Se va a proceder a configurar el servicio DHCP en el router para asignar automáticamente direcciones IP a los dispositivos dentro de las VLANs 11, 22 y 33. Para ello se creará para cada VLAN un pool de DHCP que especifica el rango de direcciones IP a asignar, la dirección del router por defecto (Gateway) y el servidor DNS. Posteriormente se excluirán un rango de direcciones IP altas para evitar conflictos con dispositivos que pueden requerir direcciones IP fijas o estáticas.

Este enfoque de configuración del DHCP asegura una administración eficiente de las direcciones IP dentro de la red y reduce la complejidad administrativa al eliminar la necesidad de asignaciones manuales de direcciones IP para los dispositivos de los usuarios.

I. Crear tres consolas: colavlan11, colavlan22 y colavlan33.

```

Acceso restringido al router rtBCN

User Access Verification

Password:

rtBCN>ena
Password:
rtBCN#config t
Enter configuration commands, one per line.  End with CNTL/Z.
rtBCN(config)#ip dhcp pool colavlan11
rtBCN(dhcp-config)# network 172.20.11.0 255.255.255.0
rtBCN(dhcp-config)#default-router 172.20.11.1
rtBCN(dhcp-config)# dns-server 8.8.8.8

rtBCN(config)#ip dhcp pool colavlan22
rtBCN(dhcp-config)#network 172.20.22.0 255.255.255.0
rtBCN(dhcp-config)#default-router 172.20.22.1
rtBCN(dhcp-config)#dns-server 8.8.8.8
rtBCN(dhcp-config)#exit
rtBCN(config)#

rtBCN(config)#ip dhcp pool colavlan33
rtBCN(dhcp-config)#network 172.20.33.0 255.255.255.0
rtBCN(dhcp-config)#default-router 172.20.33.1
rtBCN(dhcp-config)#dns-server 8.8.8.8
rtBCN(dhcp-config)#exit
rtBCN(config)#

```

II. En cada cola se asignarán IPs a partir de la .11 y excluyendo a partir de la .250.

```

rtBCN(config)#ip dhcp excluded-address 172.20.11.1 172.20.11.10
rtBCN(config)#ip dhcp excluded-address 172.20.11.250 172.20.11.254
rtBCN(config)#ip dhcp excluded-address 172.20.22.1 172.20.22.10
rtBCN(config)#ip dhcp excluded-address 172.20.22.250 172.20.22.254
rtBCN(config)#ip dhcp excluded-address 172.20.33.1 172.20.33.10
rtBCN(config)#ip dhcp excluded-address 172.20.33.250 172.20.33.254

```

Con el comando 'show run' podemos verificar que este paso se ha configurado correctamente:

```

rtBCN#show run
Building configuration...

Current configuration : 2899 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname rtBCN
!
!
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCil
!
!
ip dhcp excluded-address 172.20.11.1 172.20.11.10
ip dhcp excluded-address 172.20.11.250 172.20.11.254
ip dhcp excluded-address 172.20.22.1 172.20.22.10
ip dhcp excluded-address 172.20.22.250 172.20.22.254
ip dhcp excluded-address 172.20.33.1 172.20.33.10
ip dhcp excluded-address 172.20.33.250 172.20.33.254
!
ip dhcp pool colavlan11
network 172.20.11.0 255.255.255.0
default-router 172.20.11.1
dns-server 8.8.8.8
ip dhcp pool colavlan22
network 172.20.22.0 255.255.255.0
default-router 172.20.22.1
dns-server 8.8.8.8
ip dhcp pool colavlan33
network 172.20.33.0 255.255.255.0
default-router 172.20.33.1
dns-server 8.8.8.8
!
!

```

3. Configurar en el resto de los routers desde el CLI únicamente:

A) Nombre.

- **ROUTER rtISP:**

```
Router>en
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname rtISP
rtISP(config)#
```

- **ROUTER rtMataro:**

```
Router>ena
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname rtMataro
rtMataro(config)#
```

B) Interfaces.

- **ROUTER rtISP:**

- En primer lugar, vamos a **asociar el nombre de los otros dispositivos y su dirección IP:**

```
rtISP(config)#ip host rtMataro 77.77.77.2
rtISP(config)#ip host swISP 55.55.55.2
rtISP(config)#ip host rtBCN 44.44.44.3
rtISP(config)#end
rtISP#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
rtISP#
```

Aquí hacemos la **comprobación** de la correcta asociación:

```
rtISP#show host
Default Domain is not set
Name/address lookup uses domain service
Name servers are 255.255.255.255

Codes: UN - unknown, EX - expired, OK - OK, ?? - revalidate
       temp - temporary, perm - permanent
       NA - Not Applicable None - Not defined

Host          Port  Flags      Age Type  Address(es)
rtBCN         None (perm, OK)  0  IP    44.44.44.3
rtMataro      None (perm, OK)  0  IP    77.77.77.2
swISP         None (perm, OK)  0  IP    55.55.55.2
rtISP#
```

- **Posteriormente procedemos a configurar las interfaces:**

```
rtISP(config)#interface s0/0/0
rtISP(config-if)#ip address 44.44.44.2 255.255.255.0
rtISP(config-if)#description Enlace con rtBCN
rtISP(config-if)#no shutdown

rtISP(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
end
rtISP#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
rtISP#
```

```
rtISP(config)#interface Gi0/0
rtISP(config-if)#ip address 55.55.55.1 255.255.255.0
rtISP(config-if)#description Conexion a swISR
rtISP(config-if)#no shutdown
```

```
rtISP(config-if)#interface s0/0/1
rtISP(config-if)#exit
rtISP(config)#interface s0/0/1
rtISP(config-if)#ip address 77.77.77.1 255.255.255.0
rtISP(config-if)#description Conexion a rtMataro
rtISP(config-if)#no shutdown
```

- **ROUTER rtMataro:**

- Comenzamos *asociando el nombre de los otros dispositivos con su dirección IP:*

```
rtMataro(config)#ip host swMataro 192.168.20.2
rtMataro(config)#ip host swDMZ 192.168.222.162
rtMataro(config)#ip host rtISP 77.77.77.1
rtMataro(config)#end
rtMataro#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
rtMataro#
```

- **Posteriormente procedemos a configurar las interfaces:**

```
rtMataro(config)#interface s0/0/0
rtMataro(config-if)#ip address 77.77.77.1 255.255.255.0
rtMataro(config-if)#description Enlace con rtISP
rtMataro(config-if)#no shutdown

rtMataro(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
```

```
rtMataro(config)#interface Gi0/0
rtMataro(config-if)#ip address 192.168.20.1 255.255.255.0
rtMataro(config-if)#description Enlace con swMataro
rtMataro(config-if)#no shutdown

rtMataro(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
```

```
rtMataro(config)#interface Gi0/1
rtMataro(config-if)#ip address 192.168.222.161 255.255.255.224
rtMataro(config-if)#description Enlace con swDMZ
^
% Invalid input detected at '^' marker.

rtMataro(config-if)#description Enlace con swDMZ
rtMataro(config-if)#no shutdown

rtMataro(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
```

C) Enrutamiento dinámico RIPv2.

- **ROUTER rtISP:**

```
rtISP(config)#router rip
rtISP(config-router)#version 2
rtISP(config-router)#network 44.44.44.0
rtISP(config-router)#network 55.55.55.0
rtISP(config-router)#network 77.77.77.0
rtISP(config-router)#no auto-summary
rtISP(config-router)#exit
rtISP(config)#
```

- **ROUTER rtMataro:**

```
rtMataro(config)#router rip
rtMataro(config-router)#version 2
rtMataro(config-router)#network 77.77.77.0
rtMataro(config-router)#network 192.168.20.0
rtMataro(config-router)#network 192.168.222.160
rtMataro(config-router)#no auto-summary
rtMataro(config-router)#exit
```

D) Líneas de entrada.

- **ROUTER rtISP:**

```
rtISP(config)#line vty 0 4
rtISP(config-line)#password dit
rtISP(config-line)#login
rtISP(config-line)#exit
rtISP(config)#username operador password dit
rtISP(config)#username admin password dit
rtISP(config)#line vty 0 4
rtISP(config-line)#login local
rtISP(config-line)#transport input telnet
rtISP(config-line)#end
rtISP#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
rtISP#config t
Enter configuration commands, one per line. End with CNTL/Z.
rtISP(config)#line console 0
rtISP(config-line)#password cisco
rtISP(config-line)#login
rtISP(config-line)#end
rtISP#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
rtISP#
```

- **ROUTER rtMataro:**

```
rtMataro(config)#line vty 0 4
rtMataro(config-line)#password dit
rtMataro(config-line)#login
rtMataro(config-line)#exit
rtMataro(config)#username operador password dit
rtMataro(config)#username admin password dit
rtMataro(config)#line vty 0 4
rtMataro(config-line)#login local
rtMataro(config-line)#transport input telnet
rtMataro(config-line)#end
rtMataro#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
rtMataro#config t
Enter configuration commands, one per line. End with CNTL/Z.
rtMataro(config)#line console 0
rtMataro(config-line)#password cisco
rtMataro(config-line)#login
rtMataro(config-line)#end
rtMataro#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
rtMataro#
```

4. Conectar los dispositivos de la red interna en rtBCN (PCs, servidores, APs) a la vlan correspondiente.

Para llevar a cabo este paso y conectar los dispositivos a la red interna debemos realizar previamente una serie de configuraciones en los switches y en los dispositivos que se conectarán a esas VLANs. Esta configuración vamos a realizarla en el paso 5.

5. Configurar los conmutadores de planta swPlanta1 y swPlanta2 desde el CLI:

A) Configuración básica:

I. *Nombre del switch.*

- **Switch swPlanta1:**

```
Switch>ena
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname swPlanta1
```

- **Switch swPlanta2:**

```
Switch>ena
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname swPlanta2
```

II. Contraseña para pasar a modo privilegiado: class.

- **Switch swPlanta1:**

```
swPlanta1(config)#enable secret class
```

- **Switch swPlanta2:**

```
swPlanta2(config)#enable secret class
```

III. Mensaje de entrada: #Acceso restringido al switch ____#.

- **Switch swPlanta1:**

```
swPlanta1(config)#banner motd #Acceso restringido al switch swPlanta1#
```

- **Switch swPlanta2:**

```
swPlanta2(config)#banner motd #Acceso restringido al switch swPlanta2#
```

IV. Asociación del nombre del otro conmutador con su IP de administración.

- **Switch swPlanta1:**

```
swPlanta1(config)#ip host swPlanta2 172.20.99.3
```

- **Switch swPlanta2:**

```
swPlanta2(config)#ip host swPlanta1 172.20.99.2
```

V. Configuración de líneas de entrada igual que en rtBCN.

- **Switch swPlanta1:**

```
swPlanta1(config)#username admin password dit
swPlanta1(config)#username operador password dit
swPlanta1(config)#line vty 0 4
swPlanta1(config-line)#login local
swPlanta1(config-line)#transport input telnet
swPlanta1(config-line)#line console 0
swPlanta1(config-line)#password cisco
swPlanta1(config-line)#login
swPlanta1(config-line)#end
swPlanta1#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
swPlanta1#
```

- **Switch swPlanta2:**

```
swPlanta2(config)#username admin password dit
swPlanta2(config)#username operador password dit
swPlanta2(config)#line vty 0 4
swPlanta2(config-line)#login local
swPlanta2(config-line)#transport input telnet
swPlanta2(config-line)#line console 0
swPlanta2(config-line)#password cisco
swPlanta2(config-line)#login
swPlanta2(config-line)#end
swPlanta2#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
swPlanta2#
```

B) Configuración de VLAN's:

I. Creación y nombrado de VLANs.

- **Switch swPlanta1:**

```
Acceso restringido al switch swPlanta1

User Access Verification

Password:

swPlanta1>ena
Password:
swPlanta1#config t
Enter configuration commands, one per line. End with CNTL/Z.
swPlanta1(config)#vlan 11
swPlanta1(config-vlan)#name Personal
swPlanta1(config-vlan)#exit
swPlanta1(config)#vlan 22
swPlanta1(config-vlan)#name Alumnos
swPlanta1(config-vlan)#exit
swPlanta1(config)#vlan 33
swPlanta1(config-vlan)#name Wifi-Invitados
swPlanta1(config-vlan)#exit
swPlanta1(config)#vlan 99
swPlanta1(config-vlan)#name Administracion
swPlanta1(config-vlan)#exit
swPlanta1(config)#
```


- **Switch swPlanta2:**

```
Acceso restringido al switch swPlanta2

User Access Verification

Password:

swPlanta2>ena
Password:
swPlanta2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
swPlanta2(config)#vlan 11
swPlanta2(config-vlan)#name Personal
swPlanta2(config-vlan)#exit
swPlanta2(config)#vlan 22
swPlanta2(config-vlan)#name Alumnos
swPlanta2(config-vlan)#exit
swPlanta2(config)#vlan 33
swPlanta2(config-vlan)#name Wifi-Invitados
swPlanta2(config-vlan)#exit
swPlanta2(config)#vlan 99
swPlanta2(config-vlan)#name Administracion
swPlanta2(config-vlan)#exit
swPlanta2(config)#
```

II. Configuración de la IP de administración.

- **Switch swPlanta1:**

```
swPlanta1(config)#interface vlan 99
swPlanta1(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up

swPlanta1(config-if)#ip address 172.20.99.2 255.255.255.0
swPlanta1(config-if)#no shutdown
swPlanta1(config-if)#end
swPlanta1#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
swPlanta1#
```

- **Switch swPlanta2:**

```
swPlanta2(config)#interface vlan 99
swPlanta2(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up

swPlanta2(config-if)#ip address 172.20.99.3 255.255.255.0
swPlanta2(config-if)#no shutdown
swPlanta2(config-if)#end
swPlanta2#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
swPlanta2#
```

C) Configuración de puertos:

I. Configurar los puertos según la siguiente tabla:

| Puertos | Asignación | Red |
|-------------------|--------------------------|---------------|
| Fa0/1-0/5 | Enlaces troncales 802.1Q | |
| Fa0/6-0/12,Gi0/1 | VLAN 11: Personal | 172.X.11.0/24 |
| Fa0/13-0/19,Gi0/2 | VLAN 22: Alumnos | 172.X.22.0/24 |
| Fa0/20-0/23 | VLAN 33: Wifi-invitados | 172.X.33.0/24 |
| Fa0/24 | VLAN 99: Administracion | 172.X.99.0/24 |

II. Configurar seguridad estática en los puertos Giga, en caso de que se intente violar el puerto, éste se apagará.

Para realizar la configuración de los puertos de los conmutadores 'swPlanta1' y 'swPlanta2' vamos a configurar cada puerto a su VLAN correspondiente. Veamos como lo haremos:

• Switch swPlanta1:

```
swPlantal(config)#interface range fa0/1 - 5
swPlantal(config-if-range)#switchport mode trunk
swPlantal(config-if-range)#switchport trunk allowed vlan 11,22,33,99
swPlantal(config-if-range)#exit
swPlantal(config)#interface range fa0/6 - 12
swPlantal(config-if-range)#switchport mode access
swPlantal(config-if-range)#switchport access vlan 11
swPlantal(config-if-range)#exit
swPlantal(config)#interface range fa0/13 - 19
swPlantal(config-if-range)#switchport mode access
swPlantal(config-if-range)#switchport access vlan 22
swPlantal(config-if-range)#exit
swPlantal(config)#interface range fa0/20 - 23
swPlantal(config-if-range)#switchport mode access
swPlantal(config-if-range)#switchport access vlan 33
swPlantal(config-if-range)#exit
swPlantal(config)#interface fa0/24
swPlantal(config-if)#switchport mode access
swPlantal(config-if)#switchport access vlan 99
swPlantal(config-if)#exit

swPlantal(config)#interface gi0/1
swPlantal(config-if)#switchport mode access
swPlantal(config-if)#switchport access vlan 11
swPlantal(config-if)#switchport port-security
swPlantal(config-if)#switchport port-security maximum 1
swPlantal(config-if)#switchport port-security violation shutdown
swPlantal(config-if)#exit
swPlantal(config)#interface gi0/2
swPlantal(config-if)#switchport mode access
swPlantal(config-if)#switchport access vlan 22
swPlantal(config-if)#switchport port-security
swPlantal(config-if)#switchport port-security maximum 1
swPlantal(config-if)#switchport port-security violation shutdown
swPlantal(config-if)#exit
swPlantal(config)#end
swPlantal#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
swPlantal#
```

Con el comando 'show vlan' comprobamos:

```
swPlanta1#show vlan
```

| VLAN | Name | Status | Ports |
|------|--------------------|--------|----------------------------------------------------------------|
| 1 | default | active | Fa0/1, Fa0/2, Fa0/3, Fa0/4, Fa0/5 |
| 11 | Personal | active | Fa0/6, Fa0/7, Fa0/8, Fa0/9, Fa0/10, Fa0/11, Fa0/12, Gig0/1 |
| 22 | Alumnos | active | Fa0/13, Fa0/14, Fa0/15, Fa0/16, Fa0/17, Fa0/18, Fa0/19, Gig0/2 |
| 33 | Wifi-Invitados | active | Fa0/20, Fa0/21, Fa0/22, Fa0/23 |
| 88 | native | active | |
| 99 | Administracion | active | Fa0/24 |
| 1002 | fddi-default | active | |
| 1003 | token-ring-default | active | |
| 1004 | fddinet-default | active | |
| 1005 | trnet-default | active | |

| VLAN | Type | SAID | MTU | Parent | RingNo | BridgeNo | Stp | BrdgMode | Transl |
|------|------|--------|------|--------|--------|----------|-----|----------|--------|
| 1 | enet | 100001 | 1500 | - | - | - | - | - | 0 0 |
| 11 | enet | 100011 | 1500 | - | - | - | - | - | 0 0 |
| 22 | enet | 100022 | 1500 | - | - | - | - | - | 0 0 |

- **Switch swPlanta2:**

```
swPlanta2(config)#interface range fa0/1 - 5
swPlanta2(config-if-range)#switchport mode trunk
swPlanta2(config-if-range)#switchport trunk allowed vlan 11,22,33,99
swPlanta2(config-if-range)#exit
swPlanta2(config)#interface range fa0/6 - 12
swPlanta2(config-if-range)#switchport mode access
swPlanta2(config-if-range)#switchport access vlan 11
swPlanta2(config-if-range)#exit
swPlanta2(config)#interface range fa0/13 - 19
swPlanta2(config-if-range)#switchport mode access
swPlanta2(config-if-range)#switchport access vlan 22
swPlanta2(config-if-range)#exit
swPlanta2(config)#interface range fa0/20 - 23
swPlanta2(config-if-range)#switchport mode access
swPlanta2(config-if-range)#switchport access vlan 33
swPlanta2(config-if-range)#exit
swPlanta2(config)#interface fa0/24
swPlanta2(config-if)#switchport mode access
swPlanta2(config-if)#switchport access vlan 99
swPlanta2(config-if)#exit

swPlanta2(config)#interface gi0/1
swPlanta2(config-if)#switchport mode access
swPlanta2(config-if)#switchport access vlan 11
swPlanta2(config-if)#switchport port-security
swPlanta2(config-if)#switchport port-security maximum 1
swPlanta2(config-if)#switchport port-security violation shutdown
swPlanta2(config-if)#exit
swPlanta2(config)#interface gi0/2
swPlanta2(config-if)#switchport mode access
swPlanta2(config-if)#switchport access vlan 22
swPlanta2(config-if)#switchport port-security
swPlanta2(config-if)#switchport port-security maximum 1
swPlanta2(config-if)#switchport port-security violation shutdown
swPlanta2(config-if)#exit
swPlanta2(config)#end
swPlanta2#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
swPlanta2#
```

Comprobamos lo configurado con el comando 'show vlan':

```
swPlanta2#show vlan
```

| VLAN Name | Status | Ports |
|-------------------------|--------|-----------------------------------------------------|
| 1 default | active | Fa0/1, Fa0/2, Fa0/3, Fa0/4, Fa0/5 |
| 11 Personal | active | Fa0/6, Fa0/7, Fa0/8, Fa0/9, Fa0/10, Fa0/11, Fa0/12, |
| Gig0/1 | | |
| 22 Alumnos | active | Fa0/13, Fa0/14, Fa0/15, |
| Fa0/16 | | Fa0/17, Fa0/18, Fa0/19, |
| Gig0/2 | | |
| 33 Wifi-Invitados | active | Fa0/20, Fa0/21, Fa0/22, |
| Fa0/23 | | |
| 88 native | active | |
| 99 Administracion | active | Fa0/24 |
| 1002 fddi-default | active | |
| 1003 token-ring-default | active | |
| 1004 fddinet-default | active | |
| 1005 trnet-default | active | |

| VLAN Type | SAID | MTU | Parent | RingNo | BridgeNo | Stp | BrdgMode | Transl |
|-----------|------|--------|--------|--------|----------|-----|----------|--------|
| Trans2 | | | | | | | | |
| 1 | enet | 100001 | 1500 | - | - | - | - | 0 0 |
| 11 | enet | 100011 | 1500 | - | - | - | - | 0 0 |
| 22 | enet | 100022 | 1500 | - | - | - | - | 0 0 |

6. Realizar las siguientes copias:

1. Copiar la configuración inicial de los conmutadores de planta y del rtBCN en el srvTFTP.

Para realizar una copia de la configuración inicial de los conmutadores y del router 'rtBCN' en el servidor 'srvTFTP' haremos uso del comando 'copy running-config tftp' que almacenará la configuración en uso. Posteriormente introduciremos la dirección IP del host en el que se almacenará la configuración e indicaremos el nombre a ser asignado al archivo de configuración. Lo haremos de la siguiente forma:

- ROUTER rtBCN:

```
rtBCN#copy running-config tftp
Address or name of remote host []? 172.20.99.4
Destination filename [rtBCN-config]? rtBCN-ConfigIni-AnaBelen

Writing running-config...!!
[OK - 2528 bytes]

2528 bytes copied in 0 secs
rtBCN#
```

Producto 3: Diseño lógico e interconexión de LANs

- Switch swPlanta1:

```
swPlanta1#copy running-config tftp
Address or name of remote host []? 172.20.99.4
Destination filename [swPlanta1-config]? swPlanta1-ConfigIni-AnaBelen

Writing running-config....!!
[OK - 2874 bytes]

2874 bytes copied in 3.005 secs (956 bytes/sec)
swPlanta1#
```

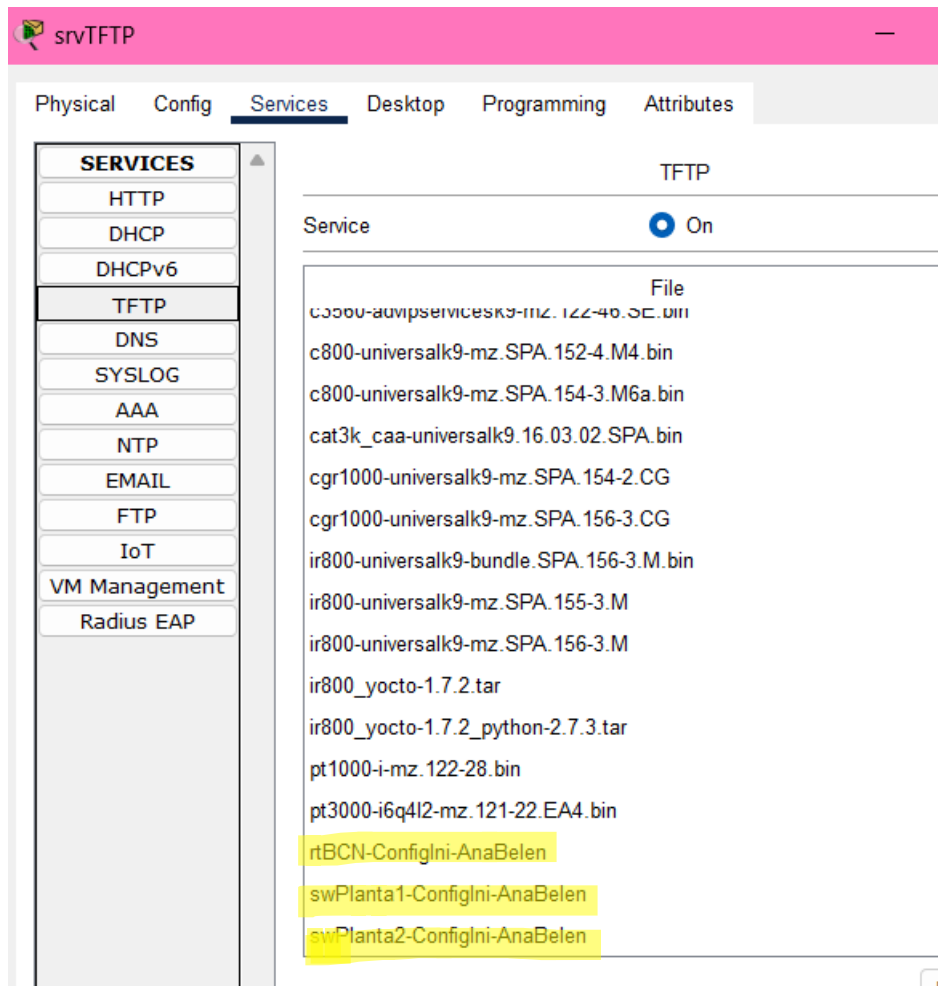
- Switch swPlanta2:

```
swPlanta2#copy running-config tftp
Address or name of remote host []? 172.20.99.4
Destination filename [swPlanta2-config]? swPlanta2-ConfigIni-AnaBelen

Writing running-config....!!
[OK - 2874 bytes]

2874 bytes copied in 3.007 secs (955 bytes/sec)
swPlanta2#
```

Comprobamos que las copias se enviaron correctamente al servidor 'srvTFTP':



III. Copiar el IOS del swPlanta2 en el srvTFTP con nombre: sw-tuNombre.

```
swPlanta2#show flash
Directory of flash:/

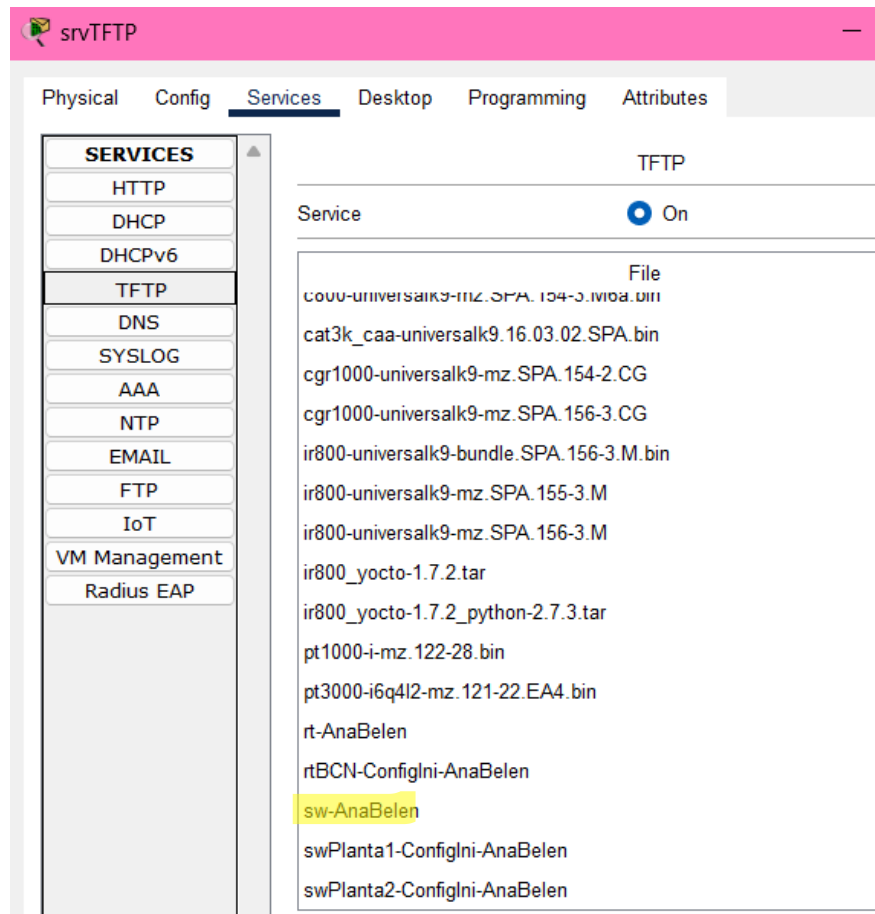
 1  -rw-      4414921      <no date>  c2960-lanbase-mz.122-25.FX.bin
 7  -rw-       2874      <no date>  config.text
 2  -rw-       856      <no date>  vlan.dat

64016384 bytes total (59597733 bytes free)
swPlanta2#copy flash: tftp:
Source filename []? c2960-lanbase-mz.122-25.FX.bin
Address or name of remote host []? 172.20.99.4
Destination filename [c2960-lanbase-mz.122-25.FX.bin]? sw-AnaBelen

Writing c2960-lanbase-mz.
122-25.FX.bin...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 4414921 bytes]

4414921 bytes copied in 0.122 secs (983227 bytes/sec)
swPlanta2#
```

Comprobamos que se copió correctamente en el 'srvTFTP':



The screenshot shows the 'srvTFTP' web interface. The 'Services' tab is selected, and the 'TFTP' service is turned 'On'. A list of files is displayed, including 'sw-AnaBelen', which is highlighted in yellow, indicating it was successfully uploaded.

| Service | File |
|---------|------------------------------------------|
| | c2960-universalk9-mz.SPA.124-3.JV108.bin |
| | cat3k_caa-universalk9.16.03.02.SPA.bin |
| | cgr1000-universalk9-mz.SPA.154-2.CG |
| | cgr1000-universalk9-mz.SPA.156-3.CG |
| | ir800-universalk9-bundle.SPA.156-3.M.bin |
| | ir800-universalk9-mz.SPA.155-3.M |
| | ir800-universalk9-mz.SPA.156-3.M |
| | ir800_yocto-1.7.2.tar |
| | ir800_yocto-1.7.2_python-2.7.3.tar |
| | pt1000-i-mz.122-28.bin |
| | pt3000-i6q4l2-mz.121-22.EA4.bin |
| | rt-AnaBelen |
| | rtBCN-ConfigIni-AnaBelen |
| | sw-AnaBelen |
| | swPlanta1-ConfigIni-AnaBelen |
| | swPlanta2-ConfigIni-AnaBelen |

IV. Copiar el IOS del rtBCN en el srvTFTP con el nombre: rt-tuNombre.

```
rtBCN#show flash:

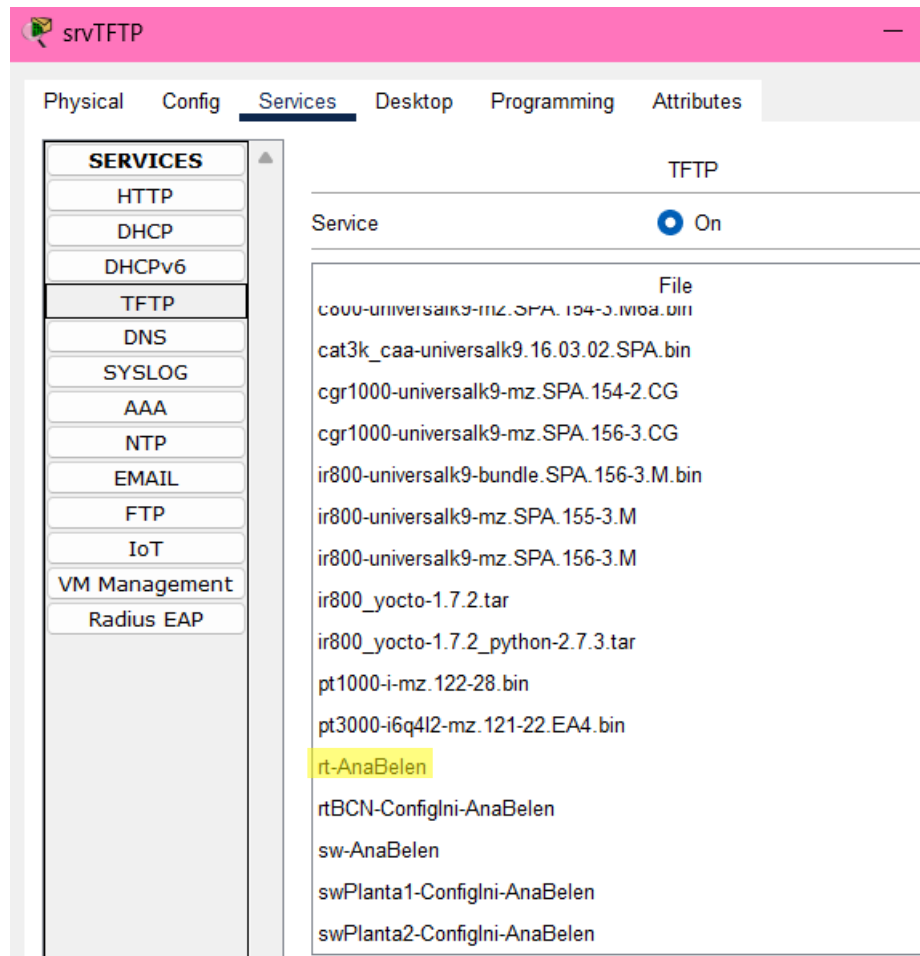
System flash directory:
File Length Name/status
 3 33591768 c2900-universalk9-mz.SPA.151-4.M4.bin
 2 28282 sigdef-category.xml
 1 227537 sigdef-default.xml
[33847587 bytes used, 221896413 available, 255744000 total]
249856K bytes of processor board System flash (Read/Write)

rtBCN#copy flash: tftp:
Source filename []? c2900-universalk9-mz.SPA.151-4.M4.bin
Address or name of remote host []? 172.20.99.4
Destination filename [c2900-universalk9-mz.SPA.151-4.M4.bin]? rt-AnaBelen

Writing c2900-universalk9-mz.SPA.
151-4.M4.bin...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 33591768 bytes]

33591768 bytes copied in 1.092 secs (3229850 bytes/sec)
rtBCN#
```

Comprobamos que se realizó la copiar correctamente:

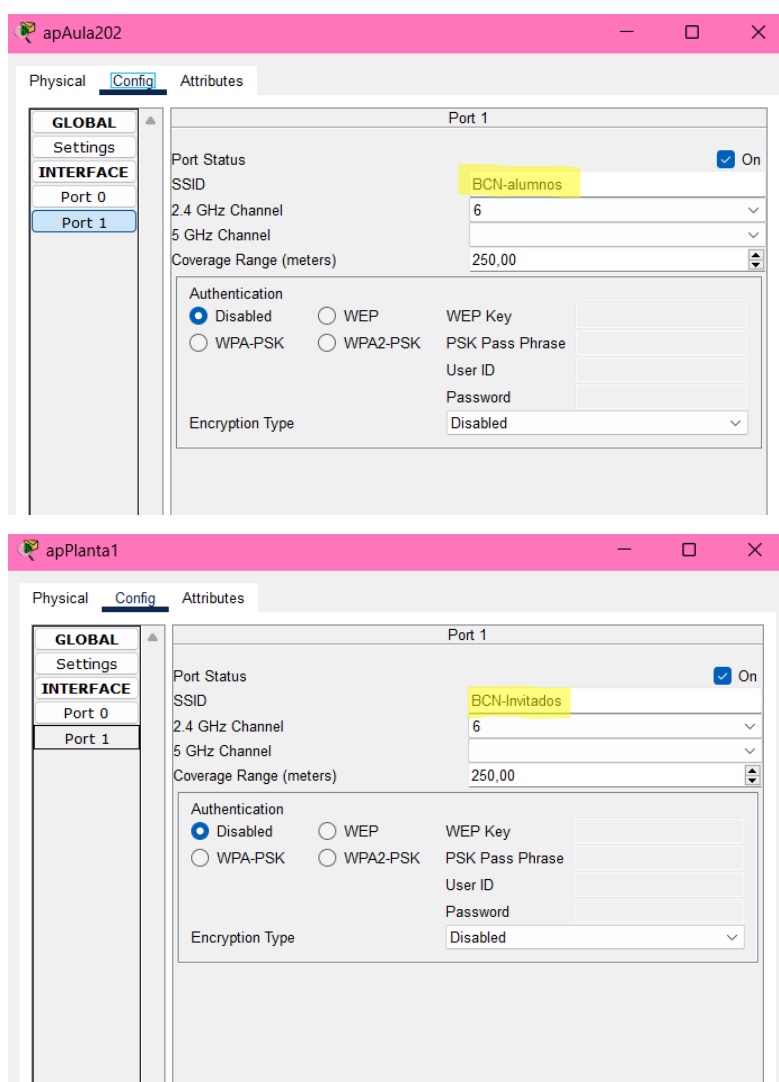


The screenshot shows the 'srvTFTP' web interface. The 'Services' tab is selected, and the 'TFTP' service is turned 'On'. A list of files is displayed, including 'c2900-universalk9-mz.SPA.151-4.M4.bin' and 'rt-AnaBelen', which is highlighted in yellow. Other files listed include 'cat3k_caa-universalk9.16.03.02.SPA.bin', 'cgr1000-universalk9-mz.SPA.154-2.CG', 'cgr1000-universalk9-mz.SPA.156-3.CG', 'ir800-universalk9-bundle.SPA.156-3.M.bin', 'ir800-universalk9-mz.SPA.155-3.M', 'ir800-universalk9-mz.SPA.156-3.M', 'ir800_yocto-1.7.2.tar', 'ir800_yocto-1.7.2_python-2.7.3.tar', 'pt1000-i-mz.122-28.bin', 'pt3000-i6q4l2-mz.121-22.EA4.bin', 'rtBCN-ConfigIni-AnaBelen', 'sw-AnaBelen', 'swPlanta1-ConfigIni-AnaBelen', and 'swPlanta2-ConfigIni-AnaBelen'.

7. Configurar el resto de dispositivos para proporcionar conectividad (Access points y swAula201).

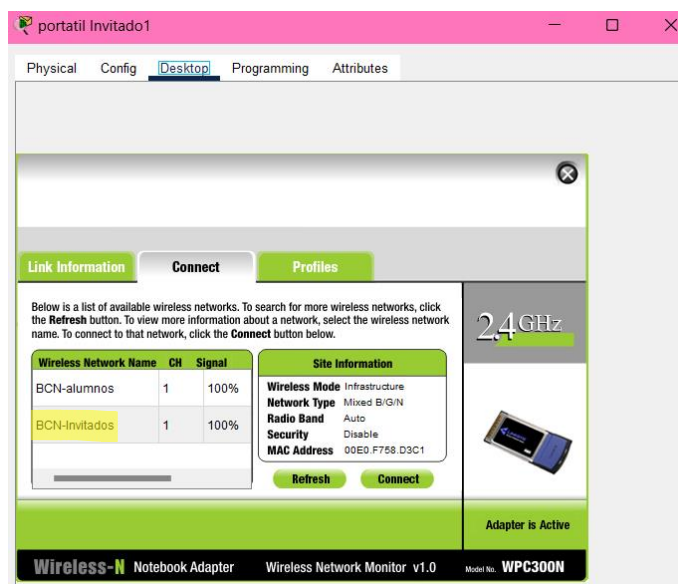
Comprobar la conectividad en toda la red. Es necesario comprobar que hay conectividad entre todos los PCs de la red antes de continuar configurando el apartado NAT y PAT.

Para **configurar los puntos de acceso**, vamos a asignar un SSID a cada uno de la siguiente forma:



Y posteriormente vamos a conectar los dispositivos portátiles:

Producto 3: Diseño lógico e interconexión de LANs



Ahora vamos a configurar el switch 'swAula201' de forma básica, pues este solo tiene conexión con la VLAN22 y está destinado a los alumnos, por lo que no es gestionable desde la red de administración:

```
Switch>ena
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname swAula201
swAula201(config)#

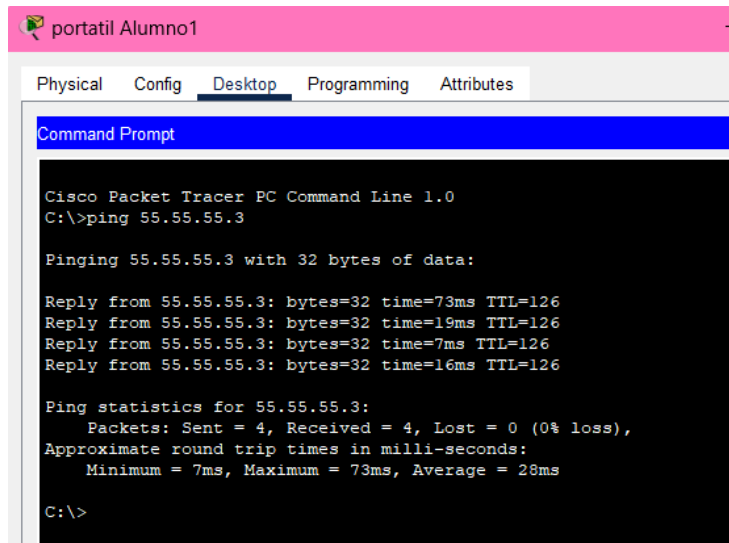
swAula201(config)#enable secret class

swAula201(config)#banner motd #Acceso restringido al swAula201#
```

Por último, realizaremos varias pruebas de conectividad en toda la red entre todos los PCs:

Producto 3: Diseño lógico e interconexión de LANs

- Ping desde 'portatil Alumnmo1' a 'pcMataro1':



The screenshot shows the 'portatil Alumnmo1' device in Cisco Packet Tracer. The 'Desktop' tab is selected, and a 'Command Prompt' window is open. The command 'ping 55.55.55.3' has been executed, resulting in four successful replies with 32 bytes of data. The ping statistics show 4 packets sent, 4 received, and 0% loss, with round trip times ranging from 7ms to 73ms.

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 55.55.55.3

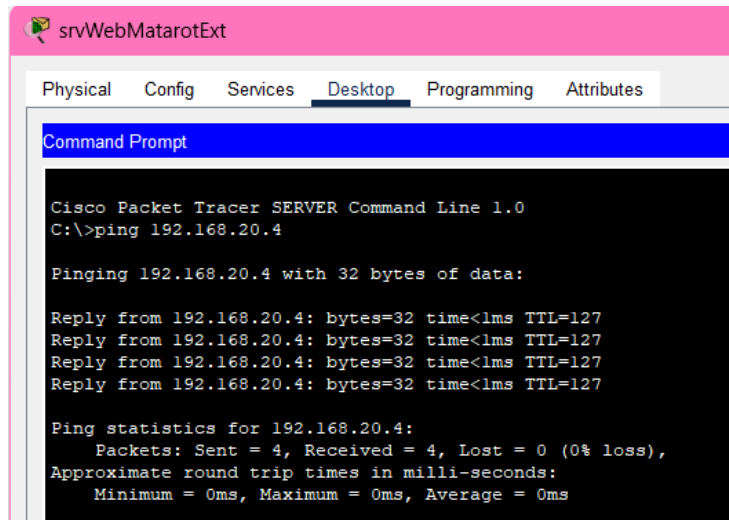
Pinging 55.55.55.3 with 32 bytes of data:

Reply from 55.55.55.3: bytes=32 time=73ms TTL=126
Reply from 55.55.55.3: bytes=32 time=19ms TTL=126
Reply from 55.55.55.3: bytes=32 time=7ms TTL=126
Reply from 55.55.55.3: bytes=32 time=16ms TTL=126

Ping statistics for 55.55.55.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 7ms, Maximum = 73ms, Average = 28ms

C:\>
```

- Ping desde 'srvMataroExt' a 'pcMataro2':



The screenshot shows the 'srvWebMatarotExt' device in Cisco Packet Tracer. The 'Desktop' tab is selected, and a 'Command Prompt' window is open. The command 'ping 192.168.20.4' has been executed, resulting in four successful replies with 32 bytes of data. The ping statistics show 4 packets sent, 4 received, and 0% loss, with round trip times all being 0ms.

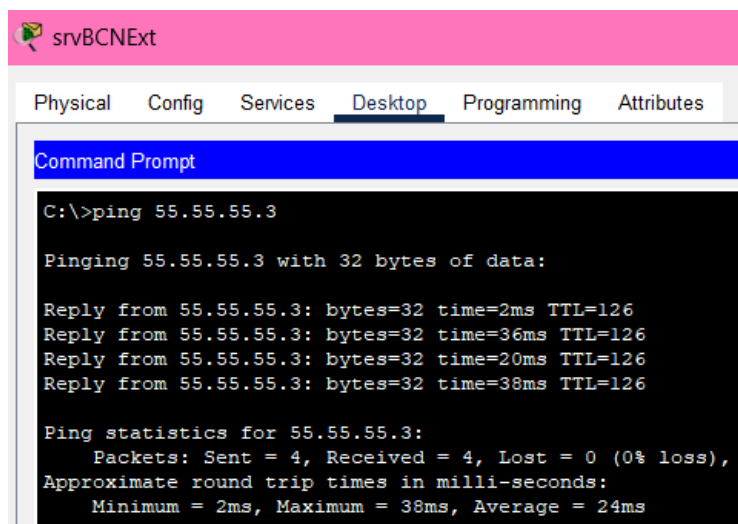
```
Cisco Packet Tracer SERVER Command Line 1.0
C:\>ping 192.168.20.4

Pinging 192.168.20.4 with 32 bytes of data:

Reply from 192.168.20.4: bytes=32 time<1ms TTL=127
Reply from 192.168.20.4: bytes=32 time<1ms TTL=127
Reply from 192.168.20.4: bytes=32 time<1ms TTL=127
Reply from 192.168.20.4: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.20.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

- Ping desde 'srvBCNExt' a 'pcISP':



The screenshot shows the 'srvBCNExt' device in Cisco Packet Tracer. The 'Desktop' tab is selected, and a 'Command Prompt' window is open. The command 'ping 55.55.55.3' has been executed, resulting in four successful replies with 32 bytes of data. The ping statistics show 4 packets sent, 4 received, and 0% loss, with round trip times ranging from 2ms to 38ms.

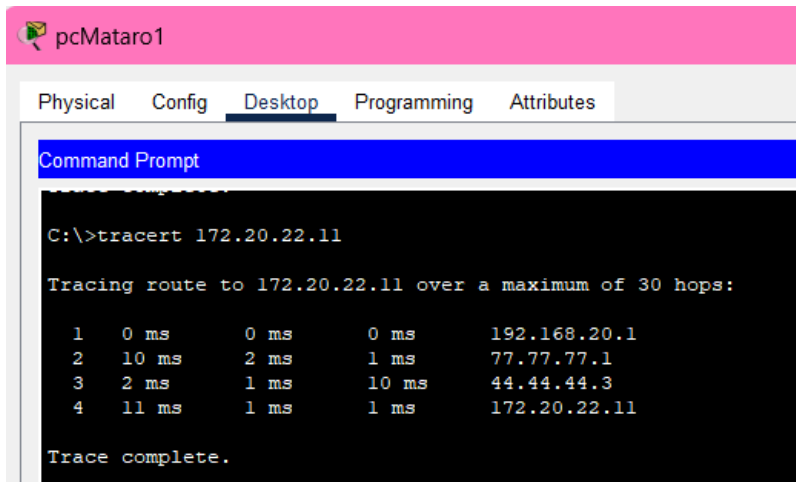
```
C:\>ping 55.55.55.3

Pinging 55.55.55.3 with 32 bytes of data:

Reply from 55.55.55.3: bytes=32 time=2ms TTL=126
Reply from 55.55.55.3: bytes=32 time=36ms TTL=126
Reply from 55.55.55.3: bytes=32 time=20ms TTL=126
Reply from 55.55.55.3: bytes=32 time=38ms TTL=126

Ping statistics for 55.55.55.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 38ms, Average = 24ms
```

- Por último, haremos una prueba de tracert desde 'pcMataro1' a 'pcAlumno2':



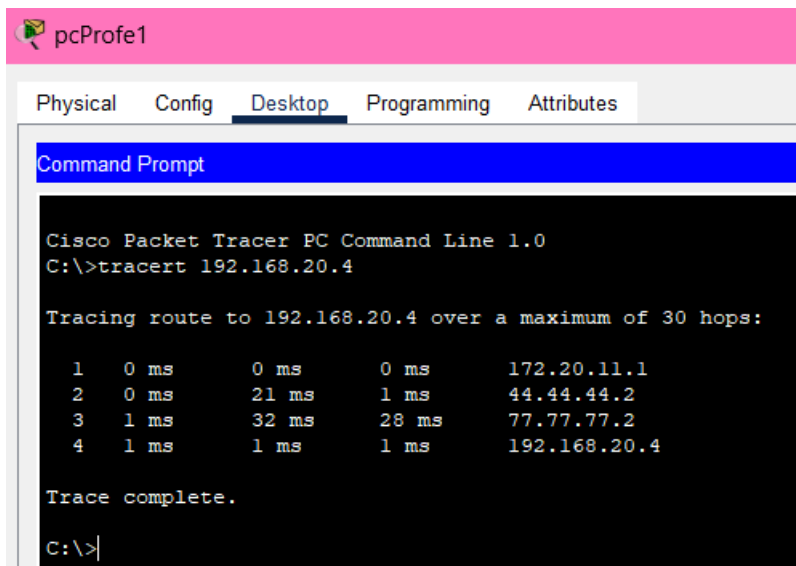
```
pcMataro1
Physical Config Desktop Programming Attributes
Command Prompt
C:\>tracert 172.20.22.11

Tracing route to 172.20.22.11 over a maximum of 30 hops:

  1  0 ms    0 ms    0 ms    192.168.20.1
  2  10 ms   2 ms    1 ms    77.77.77.1
  3  2 ms    1 ms    10 ms   44.44.44.3
  4  11 ms   1 ms    1 ms    172.20.22.11

Trace complete.
```

- Y otro tracert desde 'pcProfe1' a pcMataro2':



```
pcProfe1
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>tracert 192.168.20.4

Tracing route to 192.168.20.4 over a maximum of 30 hops:

  1  0 ms    0 ms    0 ms    172.20.11.1
  2  0 ms    21 ms   1 ms    44.44.44.2
  3  1 ms    32 ms   28 ms   77.77.77.2
  4  1 ms    1 ms    1 ms    192.168.20.4

Trace complete.
C:\>
```

8. PAT y NAT

A) Configurar el PAT en el router rtBCN, de manera que:

Para configurar el PAT en el router 'rtBCN' el primero paso que se hará será el definir la interfaz de salida de router hacia el internet como la interfaz externa para NAT mediante el comando 'ip nat outside' que le indicará al router que cualquier tráfico que pase por esta interfaz (s0/0/0) será considerado como proveniente de fuera de la red interna y se aplicará el NAT si es necesario. Lo haremos de la siguiente forma:

```
rtBCN(config)#interface s0/0/0
rtBCN(config-if)#ip nat outside
rtBCN(config-if)#
```

I. La vlan11 salgan con la IP pública 44.44.44.100/24.

Para configurar la red de la VLAN11 primero vamos a acceder a la interfaz virtual de la red y la vamos a configurar como red interna de la siguiente forma:

```
rtBCN(config)#interface gi0/0.11
rtBCN(config-subif)#ip nat inside
rtBCN(config-subif)#exit
```

Posteriormente, para permitir que múltiples dispositivos de la VLAN11 compartan una única dirección IP pública para acceder a Internet, vamos a configurar PAT, que es una forma de NAT, de la siguiente forma:

```
rtBCN(config)#ip nat inside source static 172.20.11.0 44.44.44.100
rtBCN(config)#access-list 100 permit ip 172.20.11.0 0.0.0.255 any
rtBCN(config)#exit
rtBCN#
%SYS-5-CONFIG_I: Configured from console by console
```

Con estos comandos hemos configurado la traducción de la dirección estática para la red interna 172.20.11.0 asignándole la dirección IP pública 44.44.44.100. También se ha creado la lista de acceso 100 en la que se almacenarán las reglas.

II. Las vlan22 y vlan33 salgan con las IPs públicas de la 44.44.44.101 a 44.44.44.103/24.

Similar al paso anterior, pero para las VLANS22 Y VLANS33, en primer lugar, vamos a establecer las interfaces como NAT interna:

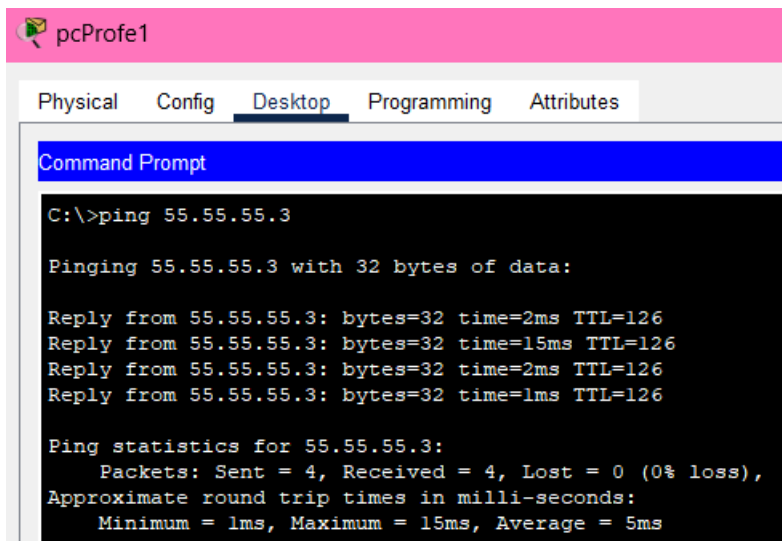
```
rtBCN(config)#interface gi0/0.22
rtBCN(config-subif)#ip nat inside
rtBCN(config-subif)#exit
rtBCN(config)#interface gi0/0.33
rtBCN(config-subif)#ip nat inside
rtBCN(config-subif)#exit
```

Posteriormente les asignaremos un rango de direcciones IP públicas de la siguiente forma:

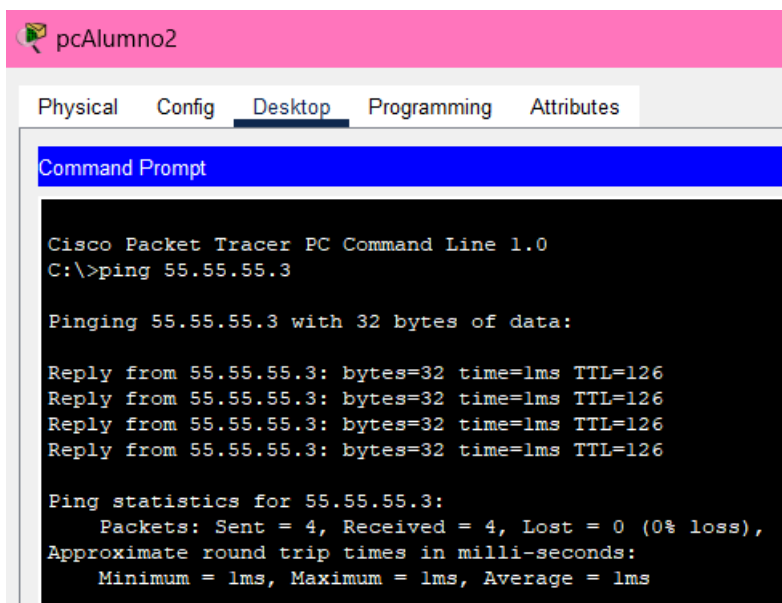
```
rtBCN(config)#ip nat pool public-ips 44.44.44.101 44.44.44.103 netmask 255.255.255.0
rtBCN(config)#ip nat inside source list 101 pool public-ips overload
rtBCN(config)#access-list 101 permit ip 172.20.22.0 0.0.0.255 any
rtBCN(config)#access-list 101 permit ip 172.20.33.0 0.0.0.255 any
rtBCN(config)#exit
rtBCN#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
```

B) Comprobar el funcionamiento PAT:

I. Ping des del pcProfe1 a pcISP.



III. Ping desde el pcAlumno2 a pcISP.



IV. Ejecutar el comando `sh ip nat translation` en `rtBCN` y verificar que se ha producido la traducción de IP privada a IP pública.

```
rtBCN#sh ip nat translation
Pro Inside global      Inside local      Outside local      Outside global
icmp 44.44.44.101:1    172.20.22.11:1    55.55.55.4:1       55.55.55.4:1
icmp 44.44.44.101:2    172.20.22.11:2    55.55.55.3:2       55.55.55.3:2
--- 44.44.44.100      172.20.11.0       ---                ---
```

Tras ejecutar dicho comando comprobamos que se ha producido la traducción de IP privada a IP pública correctamente.

D) Configurar NAT en el router `rtBCN` para que el servidor `srvBCNExtern` sea accesible desde el exterior con la IP pública `44.44.44.200/24`.

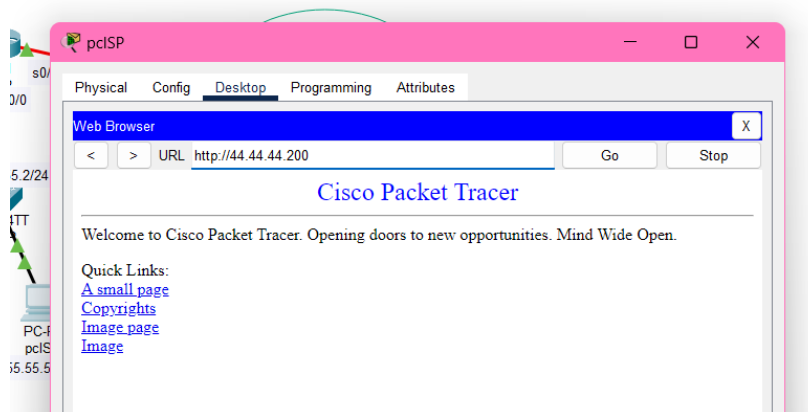
- En primer lugar, vamos a entrar en la configuración de la interfaz de red `G0/1` para aplicarle la configuración de IP nat inside como ya hemos hecho en ejercicios anteriores:

```
rtBCN(config)#int gi0/1
rtBCN(config-if)#ip nat inside
rtBCN(config-if)#exit
```

Por último, configuraremos el NAT estático para '`srvBCNExt`' para que sea accesible desde el exterior usando una dirección IP pública específica de la siguiente forma:

```
rtBCN(config)#ip nat inside source static 10.33.33.174 44.44.44.200
```

E) Comprobar el funcionamiento NAT desde el `pcISP` en el web browser acceder al `srvBCNExtern` mediante la IP pública <http://44.44.44.200>.



9. Para que la red interna de la escuela sea segura se deberían configurar ACLs en el rtBCN pero para que el estudiante pueda detectar de manera más fácil sus errores previos al correcto funcionamiento, se implementaran las ACLs en el rtMataro.

A) De la red externa y DMZ a la red interna.

ACL para que solo puedan entrar desde fuera las respuestas a las peticiones TCP originadas desde la red interna. De la misma manera solo podrán entrar desde fuera las respuestas a los pings originados desde dentro.

A tener en cuenta: Como el PT no soporta ACLs reflexivas no podremos asegurar los ataques que se produzcan a través del protocolo UDP.

Con el objetivo de permitir únicamente las respuestas a conexiones TCP iniciadas desde la red interna y las respuestas a pings que también hayan sido iniciados internamente, se creará la siguiente ACL:

```
rtMataro(config)#ip access-list extended ACL-DMZ-A-INT
rtMataro(config-ext-nacl)#permit tcp any 192.168.20.0 0.0.0.255 established
rtMataro(config-ext-nacl)#permit icmp any 192.168.20.0 0.0.0.255 echo-reply
rtMataro(config-ext-nacl)#deny ip any any
rtMataro(config-ext-nacl)#exit
rtMataro(config)#interface GigabitEthernet0/0
rtMataro(config-if)#ip access-group ACL-DMZ-A-INT out
rtMataro(config-if)#end
rtMataro#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
rtMataro#
```

Detalle de cada línea:

- Se usa el comando 'ip access-list extended' para crear una nueva ACL extendida llamada ACL-DMZ-A-INT.
- Se permiten las conexiones TCP establecidas a la gama de IP de mi red interna.
- Se permiten las respuestas ICMP echo-reply (respuestas a pings) a la gama de IP de mi red interna.
- Niega todo el tráfico para proporcionar seguridad por defecto.
- Aplica esta ACL a la interfaz que se enfrenta a la red interna en dirección de salida (out).

- Usa el comando 'ip access-group' en el modo de configuración de la interfaz.

B) De la red externa a la DMZ.

ACL para que solo se pueda entrar desde fuera para hacer un ping y para acceder al servicio HTTP del srvWebMataroExt.

Con el objetivo de permitir solo el acceso HTTP al servidor srvWebMataroExt y solicitudes ICMP echo (pings) desde la red externa. Lo haremos de la siguiente forma:

```
rtMataro(config)#ip access-list extended ACL-EXT-A-DMZ
rtMataro(config-ext-nacl)#permit tcp any host 192.168.222.163 eq www
rtMataro(config-ext-nacl)#permit icmp any host 192.168.222.163 echo
rtMataro(config-ext-nacl)#permit tcp any 192.168.20.0 0.0.0.255
rtMataro(config-ext-nacl)#permit icmp any 192.168.20.0 0.0.0.255
rtMataro(config-ext-nacl)#deny ip any any
rtMataro(config-ext-nacl)#exit
rtMataro(config)#interface s0/0/0
rtMataro(config-if)#ip access-group ACL-EXT-A-DMZ in
rtMataro(config-if)#end
rtMataro#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
rtMataro#
```

Detalle de cada línea:

- Se utiliza el comando 'ip Access-list extended' para crear una nueva ACL extendida llamada ACL-EXT-A-DMZ.
- Permite el tráfico TCP en el puerto HTTP (80) al IP del servidor 'srvWebMataroExt'.
- Permite las solicitudes ICMP echo (pings) al IP del servidor 'srvWebMataroExt'.
- Niega todo el resto del tráfico.
- Aplica esta ACL a la interfaz externa en dirección de entrada (in).

C) De la red interna a la red externa y a la DMZ.

Podrán acceder sin ninguna restricción

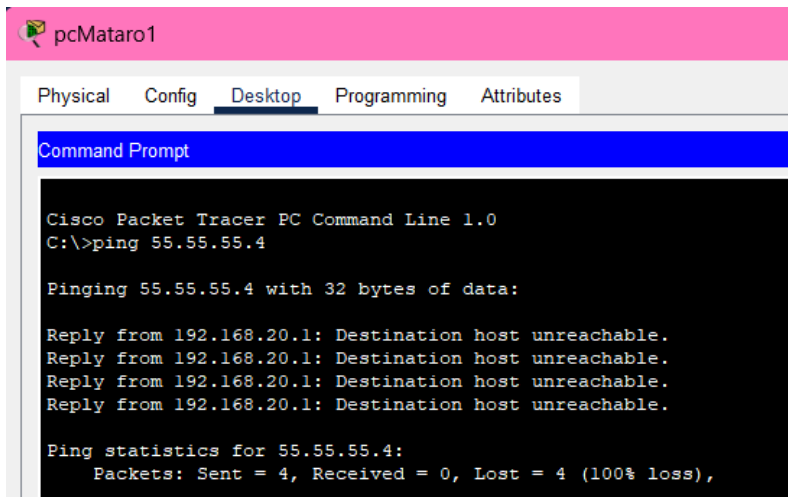
En este apartado creo que no es necesario implementar ninguna ACL para el tráfico de la red interna hacia la red externa y DMZ, debido a que el requisito es permitir la comunicación libre y sin restricciones desde la red interna hacia fuera. Al no aplicar una ACL en esta dirección, aseguramos que todos los dispositivos internos puedan acceder a los recursos externos y de la

Producto 3: Diseño lógico e interconexión de LANs

DMZ sin limitaciones, manteniendo la red abierta y funcional conforme a nuestras políticas de conectividad.

Vamos ahora a realizar algunas comprobaciones para ver que hemos configurado correctamente las ACLs:

- Ping desde la red interna ('pcMataro1') hacia la red externa ('srvDNS'):



```
pcMataro1
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 55.55.55.4

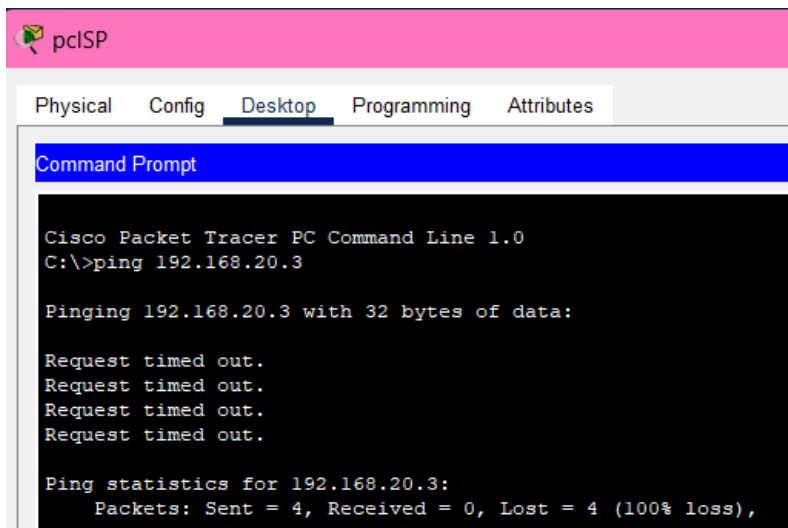
Pinging 55.55.55.4 with 32 bytes of data:

Reply from 192.168.20.1: Destination host unreachable.
Reply from 192.168.20.1: Destination host unreachable.
Reply from 192.168.20.1: Destination host unreachable.
Reply from 192.168.20.1: Destination host unreachable.

Ping statistics for 55.55.55.4:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

El ping se realiza con éxito.

- Ping desde la red externa ('pcISP') hacia la red interna ('pcMataro1'):



```
pcISP
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.20.3

Pinging 192.168.20.3 with 32 bytes of data:

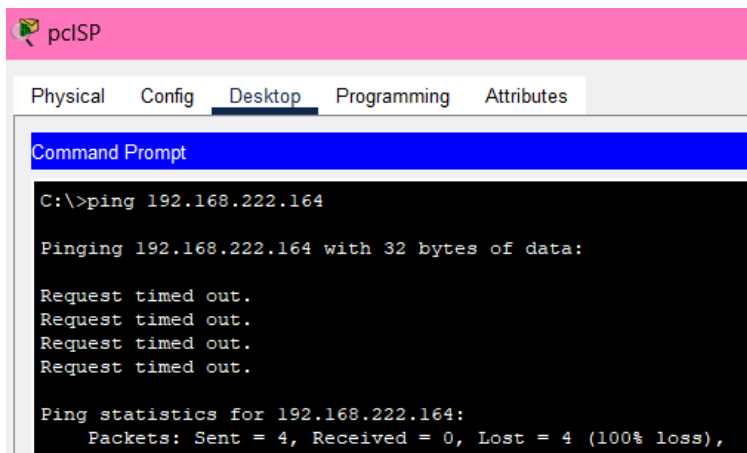
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.20.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

El ping falla como debe hacer pues se creó una ACL para no permitir comunicación.

Producto 3: Diseño lógico e interconexión de LANs

- Ping desde la red externa ('pcISP') hacia la red interna ('srvFTPMataroExt'):



```
pcISP
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 192.168.222.164

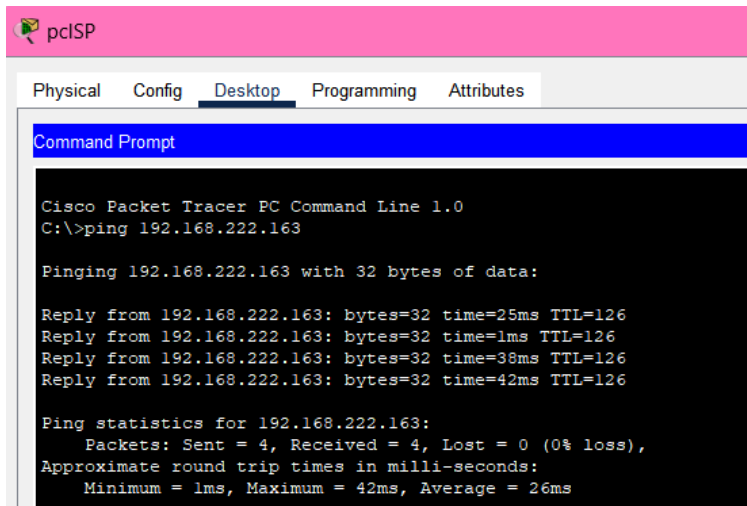
Pinging 192.168.222.164 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.222.164:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

El ping vuelve a fallar porque no se permite con la configuración de las ACLs esta conexión.

- Ping desde la red externa ('pcISP') hacia la red interna ('srvWebMataroExt'):



```
pcISP
Physical Config Desktop Programming Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.222.163

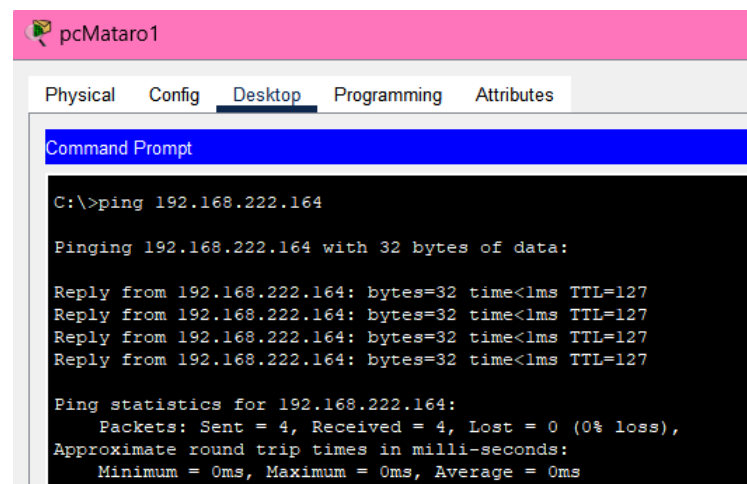
Pinging 192.168.222.163 with 32 bytes of data:

Reply from 192.168.222.163: bytes=32 time=25ms TTL=126
Reply from 192.168.222.163: bytes=32 time=1ms TTL=126
Reply from 192.168.222.163: bytes=32 time=38ms TTL=126
Reply from 192.168.222.163: bytes=32 time=42ms TTL=126

Ping statistics for 192.168.222.163:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 42ms, Average = 26ms
```

El ping se realiza correctamente.

- Ping dentro de la red interna desde 'pcMataro1' hacia 'srvFTPMataroExt':



```
pcMataro1
Physical Config Desktop Programming Attributes
Command Prompt
C:\>ping 192.168.222.164

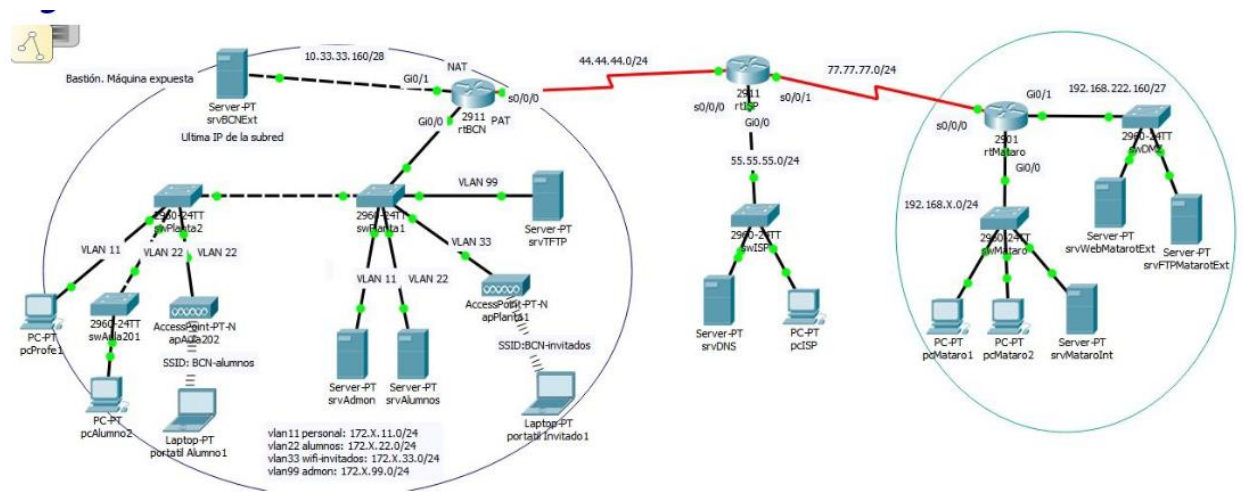
Pinging 192.168.222.164 with 32 bytes of data:

Reply from 192.168.222.164: bytes=32 time<1ms TTL=127
Reply from 192.168.222.164: bytes=32 time<1ms TTL=127
Reply from 192.168.222.164: bytes=32 time<1ms TTL=127
Reply from 192.168.222.164: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.222.164:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

El ping se realiza con éxito.

10. Comprobar que se obtiene un esquema final como el de la figura siguiente:



Producto 3: Diseño lógico e interconexión de LANs

