Preparador Informática

www.preparadorinformatica.com

PRÁCTICA 4bis

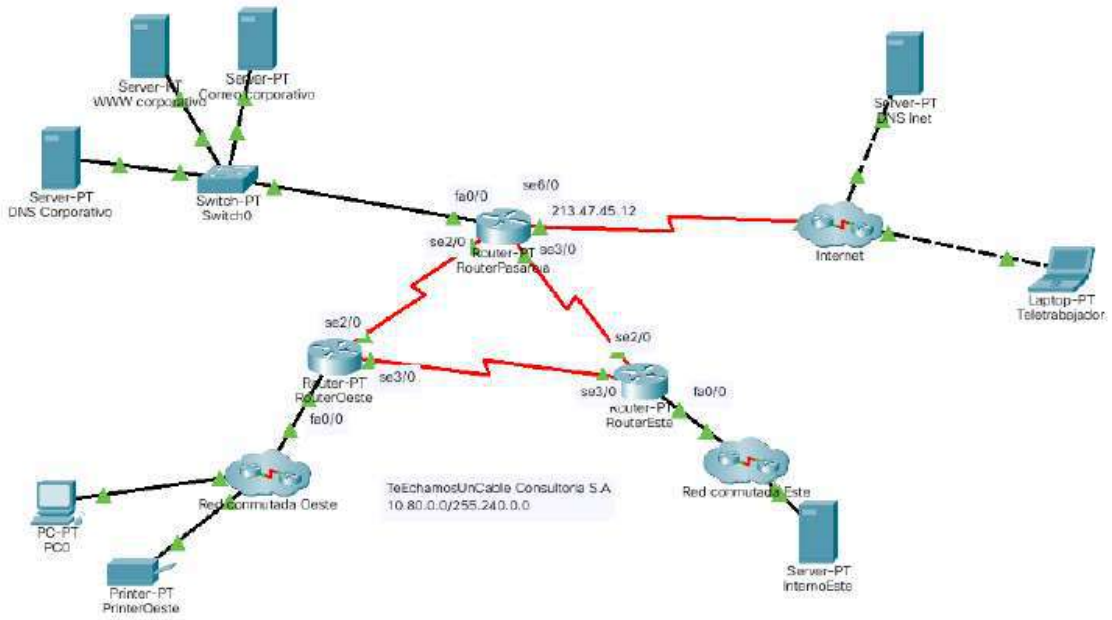
REDES

OPOSICIONES INFORMÁTICA 2021

MADRID

Ejercicio 1 – REDES *3,5 puntos*

La figura muestra la red de la corporación *TeEchamosUnCable Consultoría S.A.*



Se pide:

a) (*1,5 punto*) Partiendo de la red 10.80.0.0/255.240.0.0 establezca las subredes necesarias en toda la red privada propia de la corporación de forma que el tamaño de cada subred se ajuste a sus dimensiones reales y se economice el espacio de direccionamiento IP utilizado, propiciando la agrupación de rutas. Para ello, ha de tenerse en cuenta que tanto en la sede del este como en la del oeste se prevé un crecimiento máximo de hasta 500 puestos de trabajo. Igualmente prevé un crecimiento máximo de hasta 28 servidores en la DMZ (red del switch0).

Tenga en cuenta que:

i. De cada subred ha de especificarse: la dirección de red, máscara, dirección de difusión y el rango de direcciones IP disponibles para los equipos.

ii. Ha de asignarse una dirección IP estática a los interfaces de los routers, servidores y otros recursos compartidos en la red corporativa.

iii. En cada subred se reservarán las direcciones IP de valor inferior para los routers pertenecientes a ella.
   a. A la hora de elegir el valor concreto correspondiente a la parte de subred de una dirección IP, se deben escoger valores de subred contiguos y crecientes.
iv. Desarrolle el procedimiento de cálculo y justifique la estrategia de resolución, acompañándolo de las oportunas aclaraciones.

b) (*1,5 puntos*) Asumiendo que se ha configurado previamente el enrutamiento de forma estática dentro de la red corporativa, indique de forma ordenada, detallada y completa cómo procedería para la configuración de la función de traducción de direcciones y de reenvío de puertos en el *RouterPasarela*, del fabricante CISCO, de forma que permitiera:

i. (*0,75 puntos*) La salida de peticiones y entradas de respuestas desde clientes corporativos a servicios de Internet.
ii. (*0,75 puntos*) Que los servidores DNS, web y de correo corporativos atendieran peticiones de usuarios anónimos en Internet (no necesariamente teletrabajadores).

Para ello, ha de tenerse en consideración que la corporación tiene disponible la dirección IP pública estática, 213.47.45.12.

Desarrolle el procedimiento de configuración (explicitando los comandos y modos asociados) y justifique la estrategia de resolución, sirviéndose de las oportunas aclaraciones.

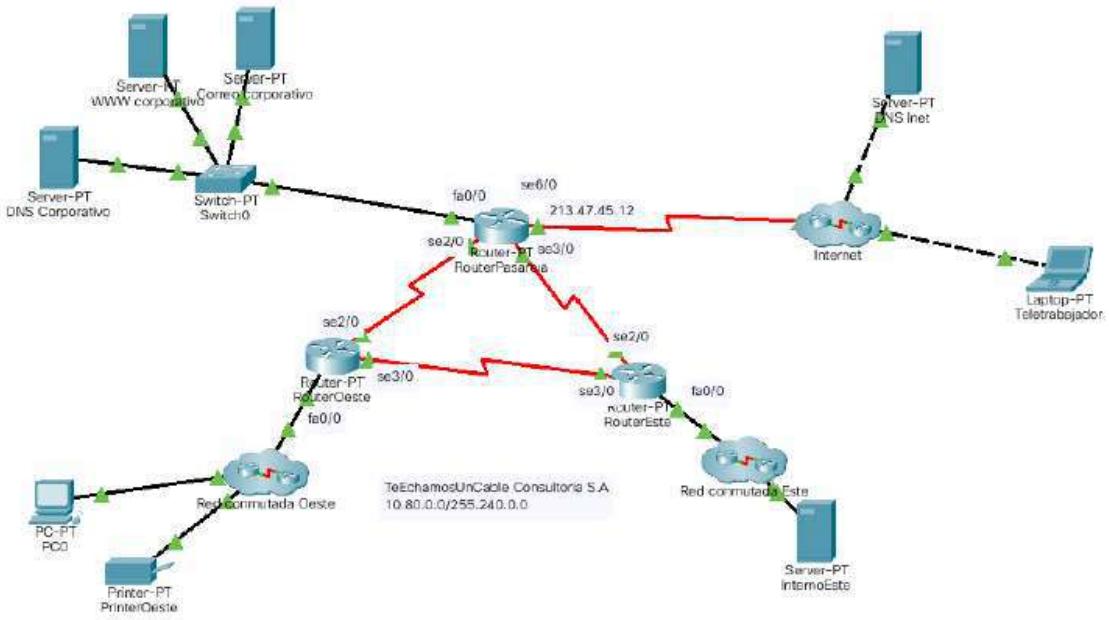
c) (*0,5 puntos*) La corporación permite que sus empleados que están teletrabajando accedan a los recursos internos de la red (servidores internos, carpetas compartidas, impresoras en red, etc.) de forma transparente: es decir, desde la perspectiva del usuario no hay apenas variación con respecto a cómo los mismos acceden a estos recursos desde puestos internos (es decir, conectados directamente en la intranet). Cada usuario cuenta con sus propias credenciales de acceso a la intranet, que coinciden con las requeridas para su conexión remota cuando teletrabaja. Concrete qué servicio/s, protocolo/s, recursos hardware, sistemas operativos, software, etc. Incorporaría como administrador de la red corporativa para permitir este acceso transparente de teletrabajadores.

SOLUCIÓN PROPUESTA

Ejercicio 1 – REDES

3,5 puntos

La figura muestra la red de la corporación *TeEchamosUnCable Consultoría S.A.*



Se pide:

a) (*1,5 punto*) Partiendo de la red 10.80.0.0/255.240.0.0 establezca las subredes necesarias en toda la red privada propia de la corporación de forma que el tamaño de cada subred se ajuste a sus dimensiones reales y se economice el espacio de direccionamiento IP utilizado, propiciando la agrupación de rutas. Para ello, ha de tenerse en cuenta que tanto en la sede del este como en la del oeste se prevé un crecimiento máximo de hasta 500 puestos de trabajo. Igualmente prevé un crecimiento máximo de hasta 28 servidores en la DMZ (red del switch0).

Tenga en cuenta que:

i. De cada subred ha de especificarse: la dirección de red, máscara, dirección de difusión y el rango de direcciones IP disponibles para los equipos.

ii. Ha de asignarse una dirección IP estática a los interfaces de los routers, servidores y otros recursos compartidos en la red corporativa.

iii. En cada subred se reservarán las direcciones IP de valor inferior para los routers pertenecientes a ella.
   a. A la hora de elegir el valor concreto correspondiente a la parte de subred de una dirección IP, se deben escoger valores de subred contiguos y crecientes.
iv. Desarrolle el procedimiento de cálculo y justifique la estrategia de resolución, acompañándolo de las oportunas aclaraciones.

Antes de comenzar con el subnetting de las redes, necesitamos conocer cuál es la máscara de red en formato decimal. Para ello, convertimos la máscara a binario y contamos los bits a 1, el resultado será la máscara en notación decimal:

11111111.1111 0000.00000000.00000000 → 255.240.0.0

En rojo se identifican los bits a 1 que identifican a la subred, por tanto, la máscara es una **/12**.

Necesitamos asignar un direccionamiento a cada una de las redes conmutadas, para ello, tendremos que realizar subnetting sobre el direccionamiento indicado (10.80.0.0/12). Existen dos tipos de subnetting, VLSM (Máscara de Subred de Longitud Variable) y FLSM (Máscara de Subred de Longitud Fija). Vamos a realizar subnetting basándonos en VLSM ya que las redes no son homogéneas respecto al número de hosts, por lo que nos interesa no desperdiciar el espacio de direcciones disponible. Además, el ejercicio especifica que las redes deben ser lo más ajustadas posibles al número de hosts que incluyen y el rango de direcciones libres después de la asignación debe ser el mayor posible.

Para comenzar con el subnetting necesitamos conocer el número de hosts que alberga cada subred, podemos verlo en la tabla siguiente, ordenada de mayor a menor número de hosts ya que la subdivisión de las redes debe comenzar por las redes de mayor tamaño. Además, debemos tener en cuenta que necesitaremos una dirección IP extra para las puertas de enlace (gateway) de cada subred que debemos sumar al número de hosts de cada una de ellas.
Las redes identificadas son las siguientes:

Subred	Número de hosts (IPs)	Observaciones
Subred A	500 + 1 (Router Este)	Red conmutada Este
Subred B	500 + 1 (Router Oeste)	Red conmutada Oeste
Subred C	28 + 1 (Router Pasarela)	Red DMZ
Subred D	2	Red Router Pasarela y Oeste
Subred E	2	Red Router Pasarela y Este
Subred F	2	Red Router Este y Oeste

Cálculos de la Subred A (Red conmutada Este)

Necesitamos conocer cuántos bits son necesarios para poder direccionar los 501 hosts de la subred. Podemos obtener los bits a través de la siguiente ecuación:

$$2^n - 2 \geq H$$

Donde ***n*** es el número de bits y ***H*** representa el número de hosts deseados, por lo tanto:

$$2^9 - 2 = 510 \geq 501; n = 9$$

Con 9 bits podemos direccionar un total de 510 hosts, por lo que son suficientes para los 501 que requiere la red.

A continuación, tenemos que calcular el número de bits de la nueva subred, podemos hacerlo utilizando la siguiente expresión:

$$R = (32 - p) - n$$

Donde 32 son los bits de una dirección IP, ***p*** es el prefijo de la red original, en nuestro caso, 12, y ***n*** son los bits de hosts necesarios que hemos obtenido en el paso anterior:

$$R = (32 - 12) - 9 = 11$$

Un total de 11 bits son los que necesitamos coger de la parte de hosts para obtener una red de 510 hosts. Una vez conocido este dato, la nueva red tendrá un prefijo de 23 bits, sumando 11 bits a los 12 que ya estaban asignados a la red original:

$$p = 12 + 11 = 23$$

La representación binaria sería la siguiente:

Máscara de la red original: **11111111.11100000.00000000.00000000** (255.240.0.0) = /12

Máscara de la nueva subred: **11111111.11111111.11111110.00000000** (255.255.254.0) = /23

El bloque de bits en **rojo** representa la parte de red, en **negro** los bits prestados de la parte de hosts y en **verde** los bits de hosts disponibles.

Para calcular el salto de red, es decir, la siguiente dirección de red contigua, se utiliza la siguiente expresión:

$$S = 256 - m$$

Donde ***m*** es el último octeto no nulo de la máscara en decimal. Por lo tanto, el valor del salto de red es **8**:

$$S = 256 - 254 = 2$$

La siguiente dirección de red se obtiene sumando 2 al último octeto de la dirección de red, es decir, la siguiente red a la 10.80.0.0/23 sería 10.80.2.0/23.

Ya tenemos todos los datos de la subred, los resumimos en la siguiente tabla:

Subred	Dirección de red	Hosts necesarios	Hosts disponibles	Rango hosts	Broadcast	Máscara
Subred A	10.80.0.0/23	501	510	10.80.0.1 – 10.80.1.254	10.80.1.255	255.255.254.0

Cálculos de la Subred B (Red conmutada Oeste)

A continuación, necesitamos calcular la red para la Subred B. Como estamos utilizando VLSM, tendremos que repetir el mismo procedimiento anterior, pero esta vez sobre la siguiente red contigua, 10.80.2.0/23.

1. Calculamos los bits necesarios para direccionar los hosts:

$$2^9 - 2 = 510 \geq 501; n = 9$$

2. Calculamos el número de bits de la subred:

$$R = (32 - 12) - 9 = 11$$

3. Calculamos la nueva mascara:

$$p = 12 + 11 = 23$$

Máscara de la nueva subred:

11111111.11111111.1111111**0.00000000** (255.255.254.0) = /23

4. Calculamos el salto de red:

$$S = 256 - 254 = 2$$

La siguiente red contigua será la 10.80.4.0/23

Los datos de la Subred B son:

Subred	Dirección de red	Hosts necesarios	Hosts disponibles	Rango hosts	Broadcast	Máscara
Subred B	10.80.2.0/23	501	510	10.80.2.1 – 10.80.3.254	10.80.3.255	255.255.254.0

Cálculos de la Subred C (Red DMZ)

A continuación, necesitamos calcular la red para la Subred C. Como estamos utilizando VLSM, tendremos que repetir el mismo procedimiento anterior, pero esta vez sobre la siguiente red contigua, 10.80.4.0/23.

5. Calculamos los bits necesarios para direccionar los hosts:

$$2^5 - 2 = 30 \geq 29; n = 5$$

6. Calculamos el número de bits de la subred:

$$R = (32 - 12) - 5 = 15$$

7. Calculamos la nueva mascara:

$$p = 12 + 15 = 27$$

Máscara de la nueva subred:

11111111.11111111.11111111.111**00000** (255.255.255.224) = /27

8. Calculamos el salto de red:

$$S = 256 - 224 = 32$$

La siguiente red contigua será la 10.80.4.32/27

Los datos de la Subred C son:

Subred	Dirección de red	Hosts necesarios	Hosts disponibles	Rango hosts	Broadcast	Máscara
Subred C	10.80.4.0/27	29	30	10.80.4.1 – 10.80.4.30	10.80.4.31	255.255.255.224

Cálculos de la Subred D (Red Router Pasarela y Oeste)

A continuación, necesitamos calcular la red para la Subred D. Como estamos utilizando VLSM, tendremos que repetir el mismo procedimiento anterior, pero esta vez sobre la siguiente red contigua, 10.80.4.32/27.

9. Calculamos los bits necesarios para direccionar los hosts:

$$2^2 - 2 = 2 \geq 2; n = 2$$

10. Calculamos el número de bits de la subred:

$$R = (32 - 12) - 2 = 18$$

11. Calculamos la nueva mascara:

$$p = 12 + 18 = 30$$

Máscara de la nueva subred:

11111111.11111111.11111111.111111**00** (255.255.255.252) = /30

12. Calculamos el salto de red:

$$S = 256 - 252 = 4$$

La siguiente red contigua será la 10.80.4.36/30

Los datos de la Subred D son:

Subred	Dirección de red	Hosts necesarios	Hosts disponibles	Rango hosts	Broadcast	Máscara
Subred D	10.80.4.32/30	2	2	10.80.4.33 – 10.80.4.34	10.80.4.35	255.255.255.252

Cálculos de la Subred E (Red Router Pasarela y Este)

A continuación, necesitamos calcular la red para la Subred E. Como estamos utilizando VLSM, tendremos que repetir el mismo procedimiento anterior, pero esta vez sobre la siguiente red contigua, 10.80.4.36/30.

13. Calculamos los bits necesarios para direccionar los hosts:

$$2^2 - 2 = 2 \geq 2; n = 2$$

14. Calculamos el número de bits de la subred:

$$R = (32 - 12) - 2 = 18$$

15. Calculamos la nueva mascara:

$$p = 12 + 18 = 30$$

Máscara de la nueva subred:

11111111.11111111.11111111.111111**00** (255.255.255.252) = /30

16. Calculamos el salto de red:

$$S = 256 - 252 = 4$$

La siguiente red contigua será la 10.80.4.40/30

Los datos de la Subred E son:

Subred	Dirección de red	Hosts necesarios	Hosts disponibles	Rango hosts	Broadcast	Máscara
Subred E	10.80.4.36/30	2	2	10.80.4.37 – 10.80.4.38	10.80.4.39	255.255.255.252

Cálculos de la Subred F (Red Router Este y Oeste)

A continuación, necesitamos calcular la red para la Subred F. Como estamos utilizando VLSM, tendremos que repetir el mismo procedimiento anterior, pero esta vez sobre la siguiente red contigua, 10.80.4.40/30.

17. Calculamos los bits necesarios para direccionar los hosts:

$$2^2 - 2 = 2 \geq 2; n = 2$$

18. Calculamos el número de bits de la subred:

$$R = (32 - 12) - 2 = 18$$

19. Calculamos la nueva mascara:

$$p = 12 + 18 = 30$$

Máscara de la nueva subred:

11111111.11111111.11111111.111111**00** (255.255.255.252) = /30

20. Calculamos el salto de red:

$$S = 256 - 252 = 4$$

La siguiente red contigua será la 10.80.4.44/30

Los datos de la Subred F son:

Subred	Dirección de red	Hosts necesarios	Hosts disponibles	Rango hosts	Broadcast	Máscara
Subred F	10.80.4.40/30	2	2	10.80.4.41 – 10.80.4.42	10.80.4.43	255.255.255.252

Una vez calculados todos los datos necesarios para completar la tabla especificada en el ejercicio, la presentamos con los datos identificativos de las redes:

Id Subred	Dirección de red	Prefijo	Máscara	Primera IP asignable	Última IP asignable	Broadcast
Subred A	10.80.0.0	23	255.255.254.0	10.80.0.1	10.80.1.254	10.80.1.255
Subred B	10.80.2.0	23	255.255.254.0	10.80.2.1	10.80.3.254	10.80.3.255
Subred C	10.80.4.0	27	255.255.255.224	10.80.4.1	10.80.4.30	10.80.4.31
Subred D	10.80.4.32	30	255.255.255.252	10.80.4.33	10.80.4.34	10.80.4.35
Subred E	10.80.4.36	30	255.255.255.252	10.80.4.37	10.80.4.38	10.80.4.39
Subred F	10.80.4.40	30	255.255.255.252	10.80.4.41	10.80.4.42	10.80.4.43

A continuación, se indica la asignación de direcciones IP estática a los interfaces de red de los routers, servidores y otros recursos compartidos en la red corporativa, siempre teniendo en cuenta los requisitos de asignación especificados en el enunciado:

Subred	Recurso	Interfaz	Dirección IP	Máscara	Gateway
Subred A	Router-PT RouterEste	Fa0/0	10.80.0.1	255.255.254.0	-
	Server-PT InternoEste	Eth0	10.80.0.2	255.255.254.0	10.80.0.1
Subred B	Router-PT RouterOeste	Fa0/0	10.80.2.1	255.255.254.0	-
	PC-PT PC0	Eth0	10.80.2.2	255.255.254.0	10.80.2.1
	Printer-PT PrinterOeste	Eth0	10.80.2.3	255.255.254.0	10.80.2.1
Subred C	Router-PT Router Pasarela	Fa0/0	10.80.4.1	255.255.255.224	-
	Server-PT DNS Corporativo	Eth0	10.80.4.2	255.255.255.224	10.80.4.1
	Server-PT WWW Corporativo	Eth0	10.80.4.3	255.255.255.224	10.80.4.1
	Server-PT Correo Corporativo	Eth0	10.80.4.4	255.255.255.224	10.80.4.1
Subred D	Router-PT Router Pasarela	Se2/0	10.80.4.33	255.255.255.252	-
	Router-PT RouterOeste	Se2/0	10.80.4.34	255.255.255.252	-
Subred E	Router-PT Router Pasarela	Se3/0	10.80.4.37	255.255.255.252	-
	Router-PT RouterEste	Se2/0	10.80.4.38	255.255.255.252	-
Subred F	Router-PT RouterOeste	Se3/0	10.80.4.41	255.255.255.252	-
	Router-PT RouterEste	Se3/0	10.80.4.42	255.255.255.252	-

Respecto al recurso de la subred C (Red DMZ) Switch-PT Switch0, suponemos que es un switch no gestionado y, por tanto, no tiene asignada una dirección IP de gestión.

b) (*1,5 puntos*) Asumiendo que se ha configurado previamente el enrutamiento de forma estática dentro de la red corporativa, indique de forma ordenada, detallada y completa cómo procedería para la configuración de la función de traducción de direcciones y de reenvío de puertos en el *RouterPasarela*, del fabricante CISCO, de forma que permitiera:

i. (*0,75 puntos*) La salida de peticiones y entradas de respuestas desde clientes corporativos a servicios de Internet.
ii. (*0,75 puntos*) Que los servidores DNS, web y de correo corporativos atendieran peticiones de usuarios anónimos en Internet (no necesariamente teletrabajadores).

Para ello, ha de tenerse en consideración que la corporación tiene disponible la dirección IP pública estática, 213.47.45.12.

Desarrolle el procedimiento de configuración (explicitando los comandos y modos asociados) y justifique la estrategia de resolución, sirviéndose de las oportunas aclaraciones.

Network Address Translation (NAT) es una función que permite la comunicación hacia Internet a múltiples hosts a través de una única dirección IP pública. Dado que no está permitido el uso de direcciones IP privadas en Internet, será necesario configurar NAT en el router pasarela para que los clientes corporativos puedan comunicarse con los servicios en Internet.

Existe varios tipos de NAT, nosotros utilizaremos PAT (Port Address Translation). PAT permite traducir las direcciones IP privadas a una única dirección IP privada, como suele ser el escenario más habitual en este tipo de configuraciones de red.

La configuración PAT requiere identificar las interfaces inside y outside del router Pasarela y generar una ACL con las subredes a las que se le aplicarán el PAT.

La configuración necesaria para permitir que los clientes corporativos puedan acceder a servicios de Internet a través del router Pasarela es la siguiente:

```
# Accedemos al modo privilegiado del router y entramos en configuración:
RouterPasarela>enable
RouterPasarela#configure terminal

# Configuramos una ACL con las subredes de los clientes corporativos, Red conmutada Este y Oeste:
RouterPasarela(config)#access-list 1 permit 10.80.0.0 0.0.1.255
RouterPasarela(config)#access-list 1 permit 10.80.2.0 0.0.1.255

# Asignamos la ACL al servicio nat configurado y a la interfaz externa que tiene configurada la IP pública:
RouterPasarela(config)#ip nat inside source list 1 interface Se6/0 overload

# Configuramos las interfaces internas (inside) con PAT:
RouterPasarela(config)#interface Se2/0
RouterPasarela(config-if)#ip nat inside
RouterPasarela(config-if)#exit
RouterPasarela(config)#interface Se3/0
RouterPasarela(config-if)#ip nat inside
RouterPasarela(config-if)#exit

# Configuramos la interfaz externa (outside) con PAT:
RouterPasarela(config)#interface Se6/0
RouterPasarela(config-if)#ip nat outside
RouterPasarela(config-if)#exit
RouterPasarela(config)#exit
```

A continuación, vamos a describir la configuración necesaria para que los servidores web, correo y dns corporativos sean accesibles desde Internet. Para publicar dichos servicios a través del router Pasarela, necesitaremos utilizar NAT estático con asignación de puertos. A través de esta configuración, los servicios internos serán publicados en Internet a través de la IP pública y en los puertos específicos que asignaremos.

Teniendo en cuenta las Configuraciones realizadas en el paso anterior, continuamos con la configuración necesaria para este escenario:

```
# Accedemos al modo privilegiado del router y entramos en configuración:
RouterPasarela>enable
RouterPasarela#configure terminal

# Configuramos la interfaz interna (inside):
RouterPasarela(config)#interface fa0/0
RouterPasarela(config-if)#ip nat inside
RouterPasarela(config-if)#exit

# Configuración de NAT estático para el servidor web, puerto 80/tcp:
RouterPasarela(config)# ip nat inside source static tcp 10.80.4.3 80 213.47.45.12 80

# Configuración de NAT estático para el servidor de correo, puerto 25/tcp:
RouterPasarela(config)# ip nat inside source static tcp 10.80.4.4 25 213.47.45.12 25

# Configuración de NAT estático para el servidor DNS, puerto 53/tcp y udp:
RouterPasarela(config)# ip nat inside source static tcp 10.80.4.2 53 213.47.45.12 53
RouterPasarela(config)# ip nat inside source static udp 10.80.4.2 53 213.47.45.12 53
```

c) (*0,5 puntos*) La corporación permite que sus empleados que están teletrabajando accedan a los recursos internos de la red (servidores internos, carpetas compartidas, impresoras en red, etc.) de forma transparente: es decir, desde la perspectiva del usuario no hay apenas variación con respecto a cómo los mismos acceden a estos recursos desde puestos internos (es decir, conectados directamente en la intranet). Cada usuario cuenta con sus propias credenciales de acceso a la intranet, que coinciden con las requeridas para su conexión remota cuando teletrabaja. Concrete qué servicio/s, protocolo/s, recursos hardware, sistemas operativos, software, etc. Incorporaría como administrador de la red corporativa para permitir este acceso transparente de teletrabajadores.

Para definir una infraestructura en la organización que permita la conexión de empleados en remoto (teletrabajo), será necesario definir los requisitos mínimos para dicha infraestructura:

1. Los empleados utilizarán la misma contraseña que emplean en los servicios corporativos para la conexión a red de teletrabajo.
2. Acceso a todos los recursos de forma transparente

Teniendo en cuenta los requisitos previos identificados en el enunciado del ejercicio, necesitaremos, al menos, los siguientes servicios:

- **VPN de acceso remoto**: Los empleados necesitan conectarse de forma remota a la intranet de la organización a través de una VPN. Es la tecnología actualmente utilizada para conectar dos sedes entre sí o un empleado con la sede. Existen multitud de fabricantes que proporcionan dicha tecnología conforme a los

requerimientos de la organización. La VPN debe proporcionar una comunicación segura y cifrada de extremo a extremo y controlar el acceso de los empleados a través de un sistema de autorización y autenticación.
El acceso a la red de la organización deberá integrar la VPN con los servicios de directorio, por ejemplo, Active Directory de Microsoft. A través de Active Directory la VPN podrá autenticar a los usuarios remotos empleando las cuentas de usuario corporativas.
Además, los empleados deberán instalar en sus PCs un cliente del fabricante de la VPN utilizada para conectarse con el terminador de túneles de la organización. Algunos fabricantes de VPN son: Fortigate, PaloAlto, OpenVPN, Cisco.

- **Active Directory**: Los servicios de directorio de Microsoft facilitan, entre otras cosas, la integración de todos los sistemas y servicios básicos de la organización, como, por ejemplo, recursos compartidos, autorización de acceso, autenticación de usuarios, etc. Por ello, si la organización ha implementado un Active Directory, la VPN podría integrarse para derivar la autenticación de los usuarios remotos con las cuentas corporativas, no necesitando una nueva contraseña para tal fin. Este sistema de autenticación podría reforzarse con sistemas multifactor.
  Los servicios de directorio activo se ejecutan sobre sistemas Microsoft Windows Server.

- **Routers, switches, firewalls**: Para realizar la comunicación entre todas las redes, es necesario el uso de dispositivos de red que permitan la comunicación de los servicios necesarios de la organización, como los recursos compartidos, dns, correo, ftp, www, etc.
  Algunos fabricantes de dispositivos de networking son: Cisco, HPE, Huawei, Juniper.