EXCMO. AYUNTAMIENTO DE JUMILLA
C.I.F. P 3002200-H
Cánovas del Castillo, 35
30520 **JUMILLA** (Murcia)

PROCESO SELECCIÓN TÉCNICO/A INFORMÁTICO/A 2019.

EJERCIO PRACTICO: REDES y FIREWALLs.

DESCRIPCION DEL ESCENARIO:

Partimos del escenario representado en el diagrama de red lógico que aparece en la figura 1.

Nuestra red está distribuida en una serie de redes internas a nivel 3 que tenemos separadas e interconectadas mediante switches de nivel 3 (switches con capacidad de routing). Cada una de las redes de nivel 3 está asignada a una vlan de nivel 2.

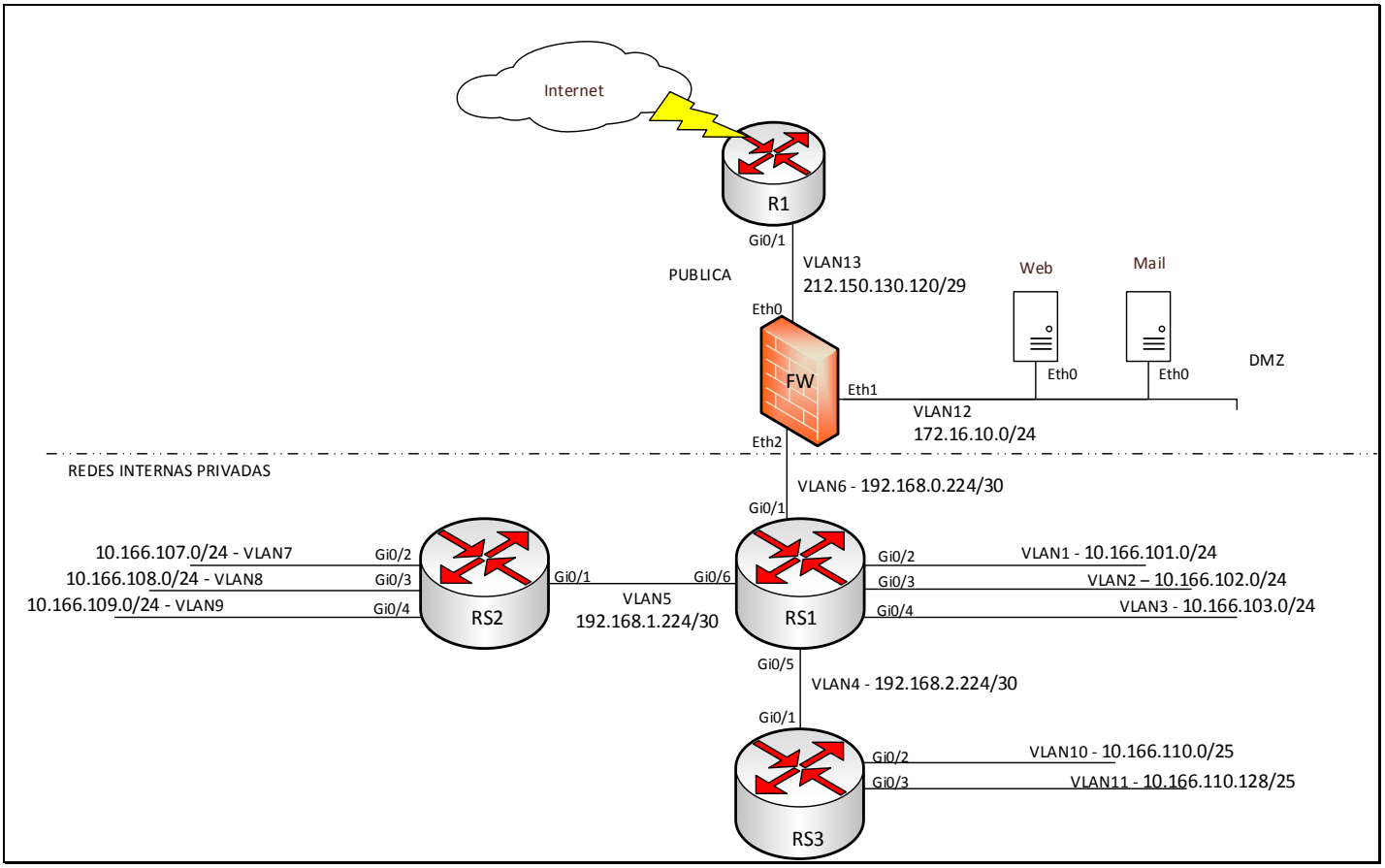
El operador de telecomunicaciones que tenemos contratado pone a nuestra disposición un router privado con un rango de ip's públicas que nos permiten tener presencia y conectividad con Internet. A dicho router tenemos conectado nuestro propio firewall que proporciona la seguridad perimetral de nuestra organización.

El firewall tiene tres interfaces, la Eth0 conectada contra el router del operador con el direccionamiento público, la Eth1 conectada a la vlan utilizada como nuestra DMZ, y la Eth2 conectada a nuestras redes internas privadas.

Los tres switches que aparecen identificados como RS1, RS2 y RS3 son switches de nivel 3, y por lo tanto realizan las funciones de switching y routing simultáneamente.

Las redes internas que están asignadas de la Vlan 1 a la Vlan 11 se utilizan para conectar equipos diversos (pc's, impresoras, cámaras de seguridad, teléfonos IPde usuario, impresoras, etc.) o bien como redes de interconexión entre los routers internos.

Figura 1.- Diagrama de red lógico de nuestra organización



El direccionamiento a nivel 3 y la vlan asignada a cada red se recoge en la tabla siguiente:

VLAN	COMENTARIO	DIRECCIONAMIENTO
13	Red publica	212.150.130.120/29
12	DMZ	172.16.10.0/24
6	Conexión FW con redes internas	192.168.0.224/30
5	Conexión RS1 – RS2	192.168.1.224/30
4	Conexión RS1 – RS3	192.168.2.224/30
1	Red interna 1	10.166.101.0/24
2	Red interna 2	10.166.102.0/24
3	Red interna 3	10.166.103.0/24
7	Red interna 7	10.166.107.0/24
8	Red interna 8	10.166.108.0/24
9	Red interna 9	10.166.109.0/24
10	Red interna 10	10.166.110.0/25
11	Red interna 11	10.166.110.128/25

J.1.- (1 punto) Para la Red pública asociada a nivel 2 a la VLAN 13, indica:

Ip asignada a la dirección de de red: 212.150.130.120

Ip asignada a la dirección de broadcast: 212.150.130.127

Mascará de red en formado x.x.x.x con x = valores entre 0 y 255: 255.255.225.248

Primera dirección ip útil del rango de red: 212.150.130.121

Ultima dirección ip útil del rango de red: 212.150.130.126

J.2.- (1 punto) Para la Red de interconexión RS1 - RS2 asociada a nivel 2 a la VLAN 5, indica:

Ip asignada a la dirección de de red: 192.168.1.224

Ip asignada a la dirección de broadcast: 192.168.1.227

Mascará de red en formado x.x.x.x con x = valores entre 0 y 255: 255.255.255.252

Primera dirección ip útil del rango de red: 192.168.1.225

Ultima dirección ip útil del rango de red: 192.168.1.226

J.3.- (1 punto) Para la Red interna 10 asociada a nivel 2 a la VLAN 10, indica:

Ip asignada a la dirección de de red: 10.166.110.0

Ip asignada a la dirección de broadcast: 10.166.110.127

Mascará de red en formado x.x.x.x con x = valores entre 0 y 255: 255.255.255.128

Primera dirección ip útil del rango de red: 10.166.110.1

Ultima dirección ip útil del rango de red: 10.166.110.126

J.4.- (1 punto) Para la Red interna 11 asociada a nivel 2 a la VLAN 11, indica:

Ip asignada a la dirección de de red: 10.166.110.128

Ip asignada a la dirección de broadcast: 10.166.110.255

Mascará de red en formado x.x.x.x con x = valores entre 0 y 255: 255.255.255.128

Primera dirección ip útil del rango de red: 10.166.110.129

Ultima dirección ip útil del rango de red: 10.166.110.254

Nos centramos ahora en el firewall. Se trata de un equipo que corre un sistema operativo Linux con una capa software por encima que le permite actuar de router y firewall de nivel 7.

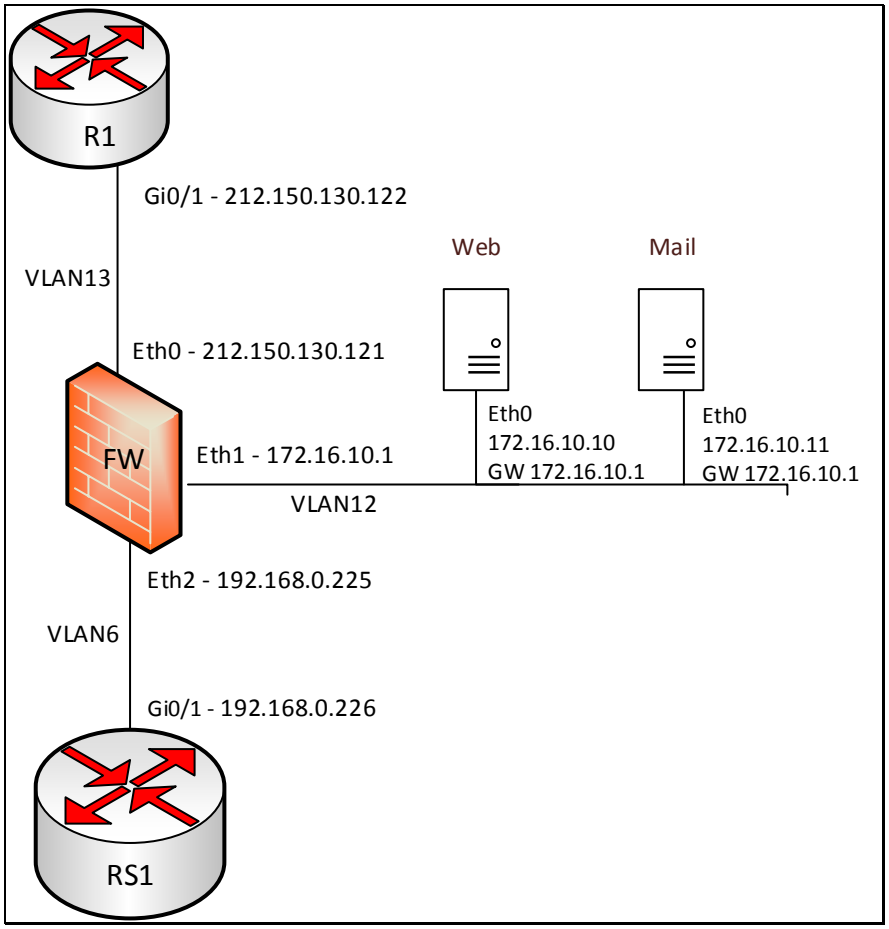
En la interfaz Eth0 tiene asignada la ip 212.150.130.121.

En la interfaz Eth1 tiene asignada la ip 172.16.10.1

En la interfaz Eth2 tiene asignada la ip 192.168.0.225

El Gateway por defecto del firewall es la ip del router R1 del operador en la VLAN13 que tiene accesible a través de su interfaz Gi0/1, la 212.150.130.122, y tiene accesible todas las redes internas de nuestra organización a través de la IP del router/switch RS1 en la VLAN6 a la que se conecta por la interfaz Gi0/1, que es la 192.168.0.226. Los detalles se muestran en la figura 2, que es un detalle ampliado de la figura 1.

Figura 2.- Detalle del Firewall Perimetral



J.5.- (4 puntos) Completa en la siguiente tabla la información de configuración de rutas estáticas que mostraría el comando "netstat –rn" de manera que el firewall a nivel 3 tenga conectividad con Internet, con la DMZ y con todas y cada una de las redes internas de nuestra organización.

Destino	Pasarela	Genmask	Interfaz
212.150.130.120	0.0.0.0	255.255.255.248	eth0
172.16.10.0	0.0.0.0	255.255.255.0	eth1
192.168.0.224	0.0.0.0	255.255.255.252	eth2
0.0.0.0	212.150.130.122	0.0.0.0	eth0
10.166.101.0	192.168.0.226	255.255.255.0	eth2
10.166.102.0	192.168.0.226	255.255.255.0	eth2
10.166.103.0	192.168.0.226	255.255.255.0	eth2
192.168.1.224	192.168.0.226	255.255.255.252	eth2
10.166.107.0	192.168.0.226	255.255.255.0	eth2
10.166.108.0	192.168.0.226	255.255.255.0	eth2
10.166.109.0	192.168.0.226	255.255.255.0	eth2
192.168.2.224	192.168.0.226	255.255.255.252	eth2
10.166.110.0	192.168.0.226	255.255.255.128	eth2
10.166.110.128	192.168.0.226	255.255.255.128	eth2

Como hemos indicado el software de firewall que corre en este equipo es de nivel 7. A parte tiene la capacidad de realizar NAT (Network Address Translation) para asignar o mapear ip's públicas del rango de red que nos ofrece el operador de telecomunicaciones contra equipos de nuestras redes internas.

Para aprovechar el uso de las ip's públicas que tenemos disponibles, queremos emplear una misma IP para mapear el tráfico contra nuestro servidor Web y nuestro servidor Mail. El servidor Web escucha en el puerto asociado al protocolo HTTP, mientras que el servidor Mail tiene abiertos el protocolo SMTP para envío y recepción de mensajes y el HTTPS para acceso a la interfaz Web de usuario.

Cuando un equipo desde Internet intente acceder a la ip publica 212.150.130.123 contra el puerto asociado al protocolo HTTP, nuestro firewall debe mapearlo contra la ip privada y el puerto de nuestro servidor web en la DMZ.

Cuando un equipo desde Internet intente acceder a la ip publica 212.150.130.123 contra el puerto asociado al protocolo SMTP o HTTPS, nuestro firewall debe mapearlo contra la ip privada y el puerto de nuestro servidor Mail en la DMZ.

Cuando nuestros servidores Web y Mail envían tráfico contra internet, deben hacerlo usando la misma ip pública, la 212.150.130.123

Cuando la comunicación es a nivel interno, es decir, cuando nos conectamos a los servidores desde cualquiera de nuestras redes internas, o cuando los servidores de la DMZ generan tráfico contra equipos de nuestra red interna, no se aplica ningún tipo de NAT, se usa la IP privada de cada servidor directamente.

J.6.- (3 puntos) Complete la tabla de NAT que tendría que usar nuestro firewall para conseguir el mapeo de los servicios indicados.

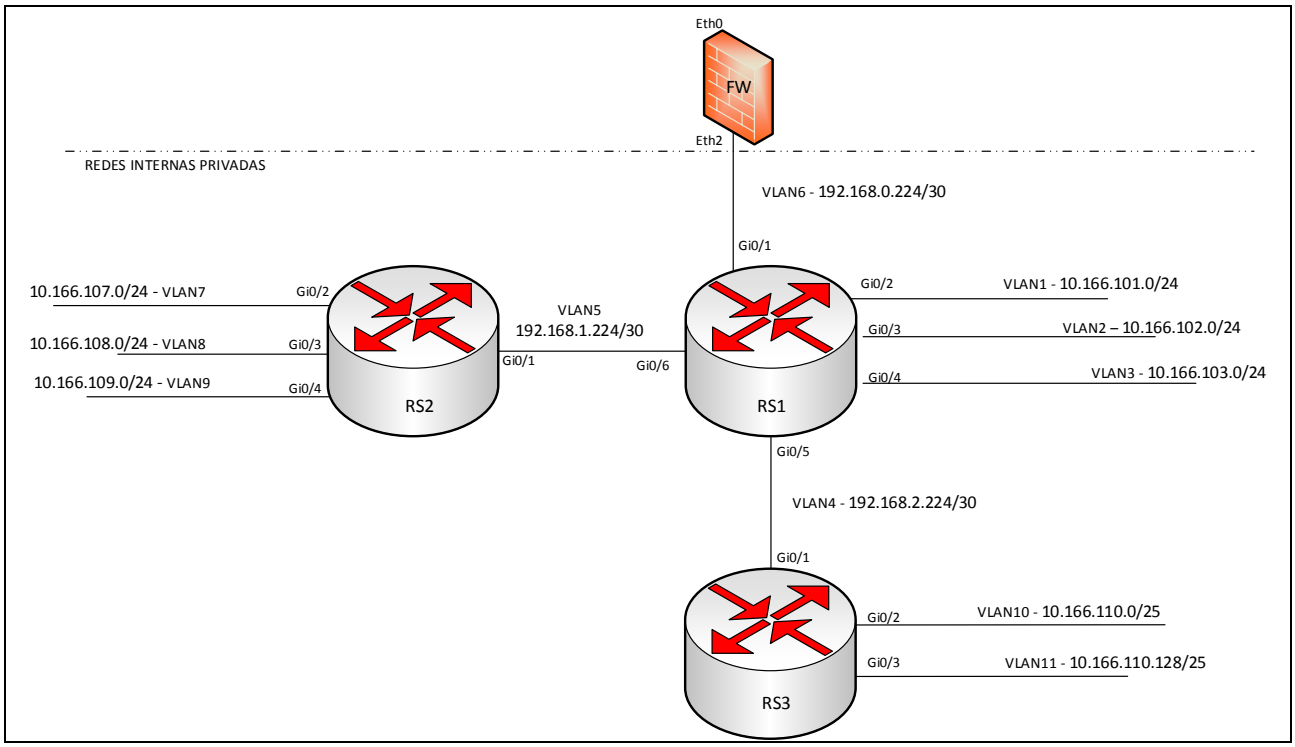
Notas:

- Any -> representa a cualquier dirección IP, ya sea pública o privada
- = Original -> Indica que la ip se mantiene tal cual iba en el paquete original
- RedesInternas -> Es un grupo que recoge el direccionamiento IP de todas las redes internas de nuestra organización.
- Las reglas de NAT se aplican en orden secuencial, del 1 al 9. Se coge el paquete original y se testea si cumple la condición establecida de origen, destino y puerto de la columna "Paquete Original". Si coincide, se la aplica la traducción especificada en la columna "Paquete traducido" y finalizamos. Si no coincide, pasamos a la siguiente regla y así sucesivamente.

	Paquete Original			Paquete traducido		
Orden	IP Origen	IP destino	Puerto tcp	IP Origen	IP destino	Puerto tcp
1	* Any	212.150.130.123	25	= Original	172.16.10.11	25
2	* Any	212.150.130.123	443	= Original	172.16.10.11	443
3	* Any	212.150.130.123	80	= Original	172.16.10.10	80
4	172.16.10.11	RedesInternas	25	= Original	= Original	25
5	172.16.10.11	RedesInternas	443	= Original	= Original	443
6	172.16.10.10	RedesInternas	80	= Original	= Original	80
7	172.16.10.11	* Any	25	212.150.130.123	= Original	25
8	172.16.10.11	* Any	443	212.150.130.123	= Original	443
9	172.16.10.10	* Any	80	212.150.130.123	= Original	80

Estamos ahora en la configuración de los Routers/Switch de nuestra infraestructura de red. Se trata de equipos que corren un sistema tipo Cisco IOS.

Figura 3.- Detalle de los equipos de red



Si ejecutamos el comando "show running-config" en el equipo RS1, el resultado que arroja es el siguiente:

```
!
interface GigabitEthernet0/1
 description ConexionFW
 switchport access vlan 6
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet0/2
description ConexionVlan1
switchport mode access
spanning-tree portfast
!
interface GigabitEthernet0/3
description ConexionVlan2
switchport access vlan 2
switchport mode access
spanning-tree portfast
!
interface GigabitEthernet0/4
description ConexionVlan3
switchport access vlan 3
switchport mode access
spanning-tree portfast
!
interface GigabitEthernet0/5
description ConexionRS3
switchport access vlan 4
switchport mode access
spanning-tree portfast
!
interface GigabitEthernet0/6
description ConexionRS2
switchport access vlan 5
switchport mode access
spanning-tree portfast
!
interface Vlan1
ip address 10.166.101.1 255.255.255.0
!
interface Vlan2
ip address 10.166.102.1 255.255.255.0
!
interface Vlan3
ip address 10.166.103.1 255.255.255.0
!
interface Vlan4
ip address 192.168.2.225 255.255.255.252
!
interface Vlan5
ip address 192.168.1.225 255.255.255.252
!
interface Vlan6
ip address 192.168.0.226 255.255.255.252
!
ip route 0.0.0.0 0.0.0.0 192.168.0.225
ip route 10.166.110.0 255.255.255.128 192.168.2.226
ip route 10.166.110.128 255.255.255.128 192.168.2.226
ip route 10.166.107.0 255.255.255.0 192.168.1.226
```

ip route 10.166.108.0 255.255.255.0 192.168.1.226
ip route 10.166.109.0 255.255.255.0 192.168.1.226
!

J.7.- (3 puntos) Partiendo de esta base, asumiendo que los routers/switch solo tienen las interfaces que aparecen en la figura 3, completa como quedaría la ejecución del comando "show running-config" en los equipos RS2 y RS3

Configuración RS2:

!
interface GigabitEthernet0/1
description ConexionRS1
switchport access vlan 5
switchport mode access
spanning-tree portfast
!
interface GigabitEthernet0/2
description ConexionVlan7
switchport access vlan 7
switchport mode access
spanning-tree portfast
!
interface GigabitEthernet0/3
description ConexionVlan8
switchport access vlan 8
switchport mode access
spanning-tree portfast
!
interface GigabitEthernet0/4
description ConexionVlan9
switchport access vlan 9
switchport mode access
spanning-tree portfast
!
interface Vlan5
ip address 192.168.1.226 255.255.255.252
!
interface Vlan7
ip address 10.166.107.1 255.255.255.0
!
interface Vlan8
ip address 10.166.108.1 255.255.255.0
!
interface Vlan9
ip address 10.166.109.1 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 192.168.1.225
!

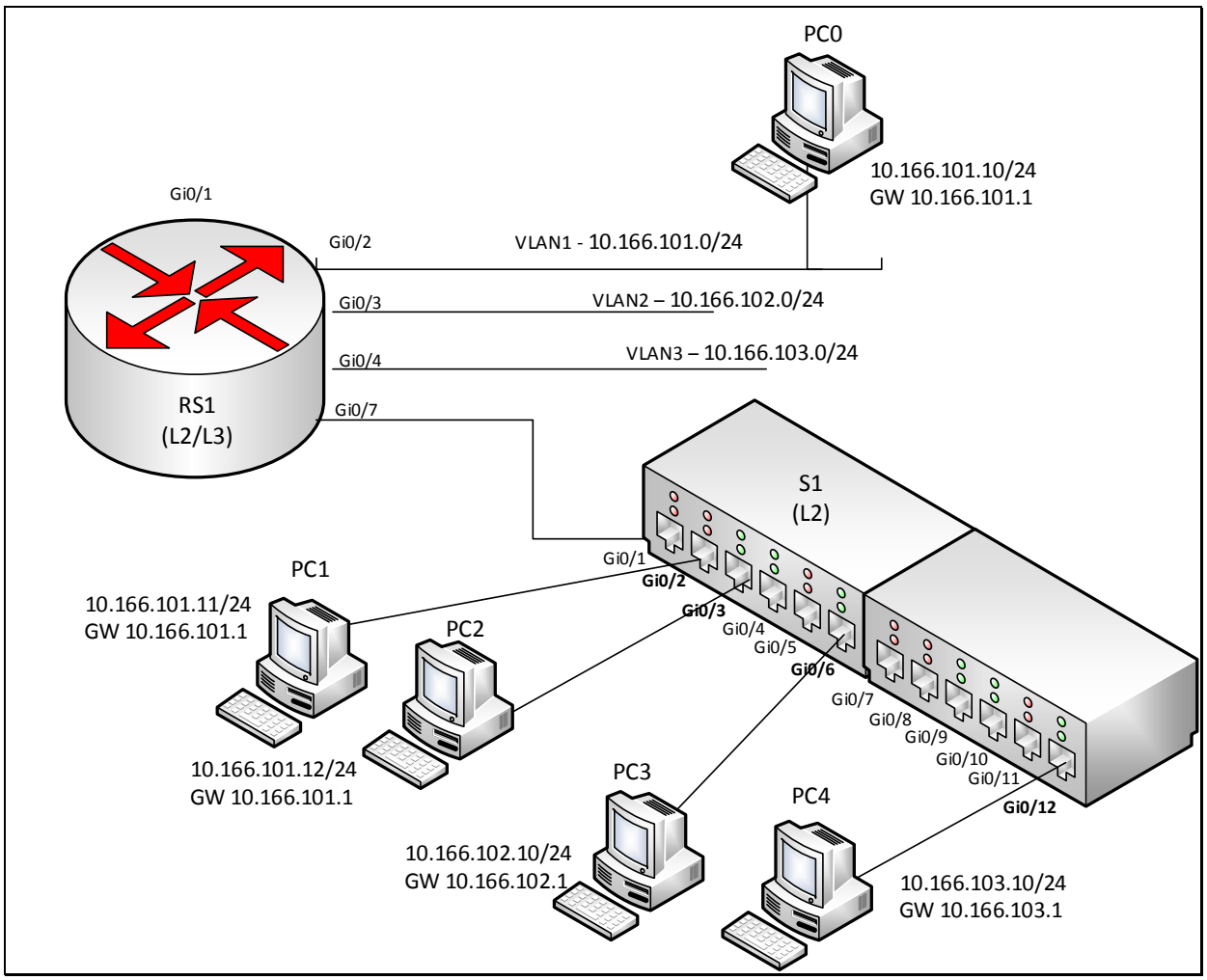
Configuración RS3:

```
!
interface GigabitEthernet0/1
 description ConexionRS1
 switchport access vlan 4
 switchport mode access
spanning-tree portfast
!
interface GigabitEthernet0/2
description ConexionVlan10
switchport access vlan 10
switchport mode access
spanning-tree portfast
!
interface GigabitEthernet0/3
description ConexionVlan11
switchport access vlan 11
switchport mode access
spanning-tree portfast
!
interface Vlan4
ip address 192.168.2.226 255.255.255.252
!
interface Vlan10
ip address 10.166.110.1 255.255.255.128
!
interface Vlan11
ip address 10.166.110.129 255.255.255.128
!
ip route  0.0.0.0  0.0.0.0  192.168.2.225
!
```

Queremos ampliar las interfaces de red disponibles para el equipo RS1, de manera que podamos conectar nuevos dispositivos de usuario (PC's, impresoras, etc.) a nuestra red. Este equipo resulta que solo dispone de un una interfaz libre que es la Gi0/7. Adquirimos un switch gestionable de nivel 2 con 12 puertos. La idea es conectar el puerto Gi0/1 del nuevo switch (S1) al puerto Gi0/7 del RS1 y luego configurar los puertos del S1 del Gi0/2 al Gi0/12 en la vlan que necesitemos (ver la siguiente figura). El puerto Gi0/7 del RS1 y el Gi0/1 del S1 están configurados ambos en modo "trunk".

La siguiente figura muestra el detalle de este apartado:

Figura 4.- Detalle ampliación interfaces.



El comando "show running-config" ejecutado en el S1 muestra lo siguiente:

```
!
interface GigabitEthernet0/1
 description ConexionRS1
switchport mode trunk
switchport trunk encapsulation dot1q
!
interface GigabitEthernet0/2
switchport mode access
spanning-tree portfast
!
interface GigabitEthernet0/3
switchport mode access
spanning-tree portfast
!
interface GigabitEthernet0/4
switchport mode access
spanning-tree portfast
!
interface GigabitEthernet0/5
switchport access vlan 2
switchport mode access
spanning-tree portfast
!
interface GigabitEthernet0/6
switchport access vlan 2
switchport mode access
spanning-tree portfast
!
interface GigabitEthernet0/7
switchport access vlan 2
switchport mode access
spanning-tree portfast
!
interface GigabitEthernet0/8
switchport access vlan 2
switchport mode access
spanning-tree portfast
!
interface GigabitEthernet0/9
switchport access vlan 3
switchport mode access
spanning-tree portfast
!
interface GigabitEthernet0/10
switchport access vlan 3
switchport mode access
spanning-tree portfast
!
interface GigabitEthernet0/11
switchport access vlan 3
switchport mode access
spanning-tree portfast
!
interface GigabitEthernet0/12
switchport access vlan 3
switchport mode access
spanning-tree portfast
!
interface Vlan1
description Gestion
ip address 10.166.101.2 255.255.255.0
```

no ip route-cache
!
ip default-gateway 10.166.101.1
!

Teniendo en cuenta este escenario, marque la opción correcta (solo una) en las siguientes cuestiones.

J.8.- (1 punto) La finalidad de usar VLAN (*Virtual LAN*) en una infraestructura de red es:

1) ☐ Segmentar el dominio de *Broadcast* a nivel de la capa 3 del modelo TCP/IP
2) ☐ Separar el tráfico de red a nivel de la capa 2 del modelo TCP/IP
3) ☐ Aumentar el número de dispositivos físicos de red necesarios para implementar nuestra red, consiguiendo así mayor seguridad.
4) ☐ Todas las opciones anteriores son correctas.

J.9.- (1 punto) Con respecto a un trunk:

1) ☐ Es un enlace entre dos *switches* en el cual se canaliza todo el tráfico perteneciente a las *VLANs*.
2) ☐ El puerto en modo *Trunk* debe ser configurado en ambos extremos del enlace, es decir, en ambos *switches*.
3) ☐ El tráfico de la VLAN nativa en un enlace trunk pasa siempre "tageado" (tagged).
4) ☐ **Solamente las opciones 1 y 2 son correctas**

J.10.- (1 punto) Teniendo en cuenta el modelo TCP/IP, el tráfico generado entre los equipos PC1 y PC0 para compartir una carpeta a través de la red

1) ☐ Basta con tener conectividad a nivel 2
2) ☐ Necesita conectividad a nivel 2 y 3
3) ☐ Es necesario que pase a través del Gateway de nivel 3
4) ☐ Ninguna opción es correcta

J.11.- (1 punto) Teniendo en cuenta el modelo TCP/IP, el tráfico generado entre los equipos PC1 y PC2 para compartir una carpeta a través de la red

1) ☐ **Basta con tener conectividad a nivel 2**
2) ☐ Necesita conectividad a nivel 2 y 3
3) ☐ Es necesario que pase a través del Gateway de nivel 3
4) ☐ Ninguna opción es correcta

J.12.- (1 punto) Teniendo en cuenta el modelo TCP/IP, el tráfico generado entre los equipos PC0 y PC3 para compartir una carpeta a través de la red

1) ☐ Basta con tener conectividad a nivel 2
2) ☐ Necesita conectividad a nivel 2 y 3
3) ☐ Es necesario que pase a través del Gateway de nivel 3
4) ☐ Las opciones 2 y 3 son correctas

J.13.- (1 punto) Teniendo en cuenta el modelo TCP/IP, el tráfico generado entre los equipos PC1 y PC4 para compartir una carpeta a través de la red

1) ☐ Basta con tener conectividad a nivel 2
2) ☐ Necesita conectividad a nivel 2 y 3
3) ☐ No es necesario que pase a través del Gateway de nivel 3
4) ☐ Las opciones 2 y 3 son correctas