

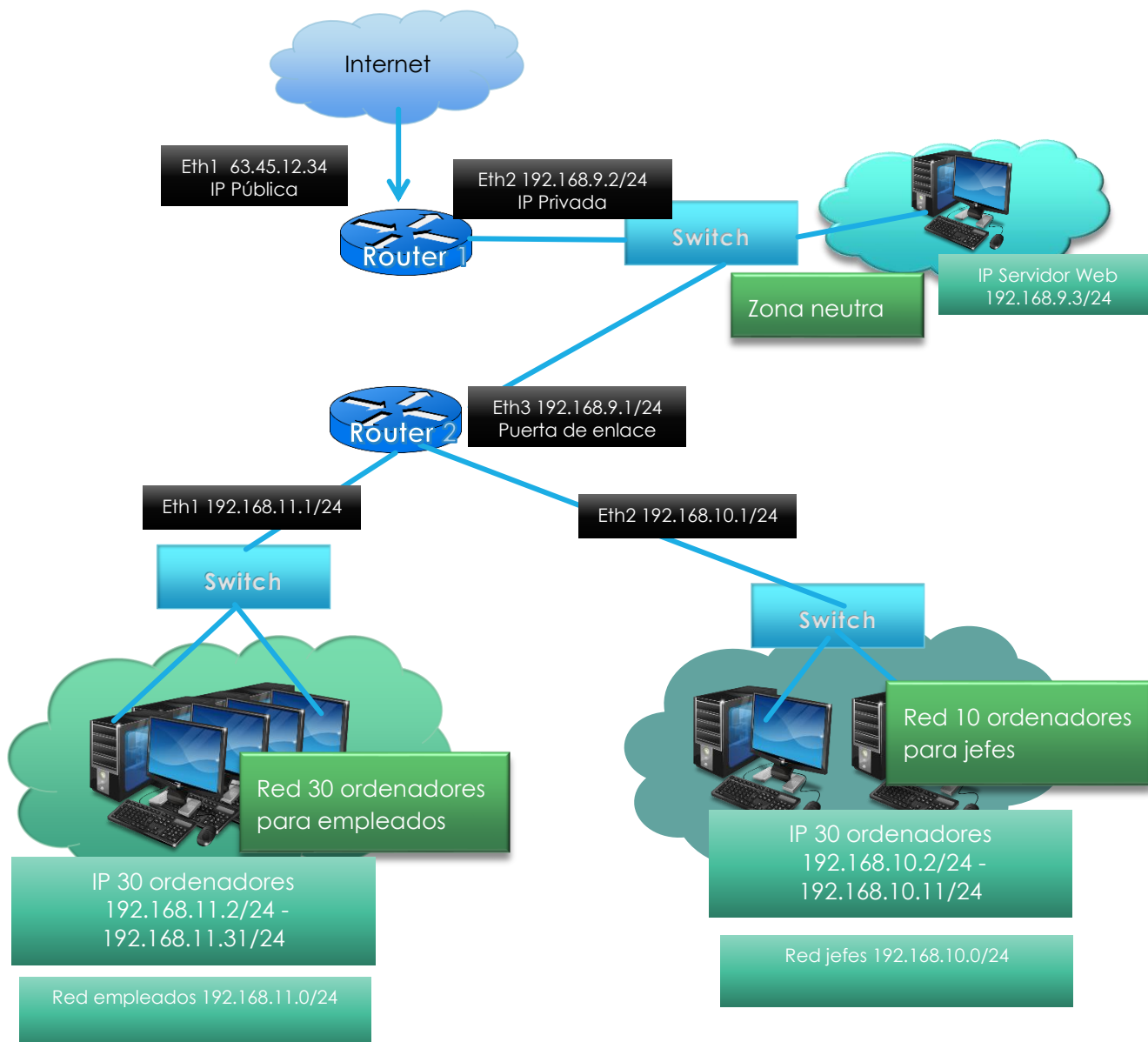
TAREA PARA SI04.

Detalles de la tarea de esta unidad.

Enunciado.

La tarea de la unidad está dividida en 3 actividades.

Actividad 4.1. Una empresa nos ha solicitado la configuración e implantación de su red de ordenadores. Dicha empresa consta de 3 plantas. La primera planta está compuesta por 30 ordenadores para los empleados, en la segunda planta hay un servidor web que ofrece sus servicios a Internet. Y por último, la tercera planta está reservada para que los jefes que tienen 10 equipos. Por motivos de seguridad se requiere que todas las redes estén aisladas y que se preste una especial atención al servidor web de la empresa. Para realizar la actividad hay que realizar el esquema físico, esquema lógico y la tabla de enrutado de los routers que componen la red.



He optado por utilizar **un esquema de red con una zona neutra y varias redes internas**. He separado la red de los empleados y los jefes para mejorar la seguridad ya que se requiere en el enunciado que estén aisladas, prestando especial atención al servidor.

Para proteger al servidor añado una **zona neutra** para proporcionar mayor protección. Aquí se suelen ubicar los servidores de la empresa. El principal objetivo de esta red es que ante un posible ataque en uno de los servidores se aislé la intrusión y no se permita el acceso a la red interna de la empresa.

En este esquema estoy trabajando con direcciones **IPv4**. El modificador **/24** al final de la dirección indica que se trata de una subred de clase C con una máscara de subred de 24 bits. Esto significa que la subred tiene una capacidad para 256 direcciones IP únicas, que van desde 192.168.10.0 hasta 192.168.10.255, de las cuáles podemos asignar 254. Estas direcciones IP se pueden utilizar para asignar direcciones a dispositivos que se conecten a una red privada, como una red LAN (Local Area Network) en la oficina propuesta en la actividad.

Tablas de enrutamiento Router 1:

Reglas	Interfaz	Origen	Destino	Puerto	Acción
1	Eth1	0.0.0.0	192.168.9.3/32	80	Permitir
2	Eth1	0.0.0.0	192.168.9.3/32		Denegar
3	Eth1	0.0.0.0	192.168.9.1/32		Denegar
4	Eth2	192.168.9.0/24	0.0.0.0		Permitir
5					Denegar

Regla 1. Esta regla permite el acceso entrante en el puerto 80, que normalmente se utiliza para el tráfico http. El host que está en 192.168.9.3/32 es el servidor web. La organización no puede predecir quién va a tener acceso a su sitio Web, por lo que no hay restricción en las direcciones IP de origen.

Regla 2. Esta regla elimina todos los paquetes que tienen como destino la red donde se encuentran los servidores. Como la regla 1 se ejecuta antes se permitirá el acceso al puerto 80.

Regla 3. No se permite el tráfico desde internet hacia las redes internas de los jefes y empleados.

Reglas 4. Permite la salida a internet desde el switch de la zona neutra.

Regla 5. Esta regla bloquea explícitamente todos los paquetes que no han coincidido con ningún criterio de las reglas anteriores. La mayoría de los dispositivos de análisis realizan este paso de forma predeterminada, pero es útil incluir esta última regla de limpieza. Incluirla aclara la aplicación de la directiva predeterminada y, en la mayoría

de los casos, permite registrar los paquetes que coinciden con ella. Esto es útil por motivos jurídicos y administrativos.

Tablas de enrutamiento Router 2:

Reglas	Interfaz	Origen	Destino	Puerto	Acción
1	Eth1	192.168.11.0/24	192.168.9.1		Permitir
2	Eth2	192.168.10.0/24	192.168.9.1		Permitir
3	Eth3	0.0.0.0	192.168.11.0/24		Denegar
4	Eth3	0.0.0.0	192.168.10.0/24		Permitir
5					Denegar

Regla 1. Permito la salida a internet y al servidor web desde la red de empleados.

Regla 2. Permito la salida a internet y al servidor web desde la red de jefes de la misma manera.

Regla 3. Esta regla elimina todos los paquetes que tienen como destino la red de empleados. Como la regla 1 y 2, se ejecutan antes, sí se permite el tráfico que va dirigido a la red de empleados proveniente de la red de jefes y empleados. Si se pone esta regla al principio de la tabla de enrutado, no se podrá acceder a la red empleados.

Reglas 4. Esta regla elimina todos los paquetes que tienen como destino la red de jefes. Como la regla 1 y 2, se ejecutan antes, sí se permite el tráfico que va dirigido a la red de jefes proveniente de la red de jefes y empleados. Si se pone esta regla al principio de la tabla de enrutado, no se podrá acceder a la red de jefes.

Regla 5. Esta regla bloquea explícitamente todos los paquetes que no han coincidido con ningún criterio de las reglas anteriores. La mayoría de los dispositivos de análisis realizan este paso de forma predeterminada, pero es útil incluir esta última regla de limpieza. Incluirla aclara la aplicación de la directiva predeterminada y, en la mayoría

Red	Dirección	Intervalo IP	Máscara	Gateway
Zona neutra	192.168.9.0/24	192.168.9.1 - 192.168.9.3	255.255.255.0	192.168.9.2
Empleados	192.168.11.0/24	192.168.11.1 - 192.168.11.31	255.255.255.0	192.168.11.1
Jefes	192.168.10.0/24	192.168.10.1 - 192.168.10.11	255.255.255.0	192.168.10.1

Actividad 4.2. Dividir la dirección de red 150.200.10.0/24 en las siguientes subredes:

- 3 redes de 50 ordenadores.
- 4 redes de 12 ordenadores.

Rango red	Rango IP	Broadcast
150.200.10.0/26	150.200.10.1 a 150.200.10.62	150.200.10.63
150.200.10.64/26	150.200.10.65 a 150.200.10.126	150.200.10.127
150.200.10.128/26	150.200.10.129 a 150.200.10.190	150.200.10.191
150.200.10.192/28	150.200.10.193 a 150.200.10.206	150.200.10.207
150.200.10.208/28	8 150.200.10.209 a 150.200.10.222	150.200.10.223
150.200.10.224/28	150.200.10.225 a 150.200.10.238	150.200.10.239
150.200.10.240/28	150.200.10.241 a 150.200.10.254	150.200.10.255

La dirección de **broadcast** es una dirección especial que se utiliza para enviar mensajes a todos los dispositivos en la red.

/26 es una dirección de red con un prefijo de **máscara de subred de 26**. Esto significa que la dirección de red es **150.200.10.0** y la máscara de subred es **255.255.255.192**. La máscara de subred se utiliza para determinar qué parte de la dirección IP pertenece a la red y cuál parte se utiliza para identificar dispositivos individuales en la red.

En este caso, la máscara de subred indica que los primeros 26 bits de la dirección IP son parte de la dirección de red y los últimos 6 bits son parte de la dirección del host. Esto significa que puede haber **hasta 64 dispositivos individuales** con direcciones IP de los cuales solo vamos a utilizar **52 (50 direcciones más la dirección de broadcast y dirección de red)** dejando 12 direcciones sin utilizar.

En la máscara **/28** la máscara de red es 255.255.255.240 pudiendo haber hasta 16 dispositivos individuales con direcciones IP válidas en esta red. Teniendo en cuenta la dirección de red, broadcast y los 12 equipos conectados, dejamos 2 direcciones sin utilizar.

- ¿Cuántas direcciones IP se pierden?

Perderíamos 44 direcciones IP.

Actividad 4.3. Enumera los servicios que has visto en la unidad.

- Servicio DNS
- Servicio DHCP
- Servicio Web
- Servicio Correo Electrónico.
- Servicio FTP
- Servicio Acceso remoto