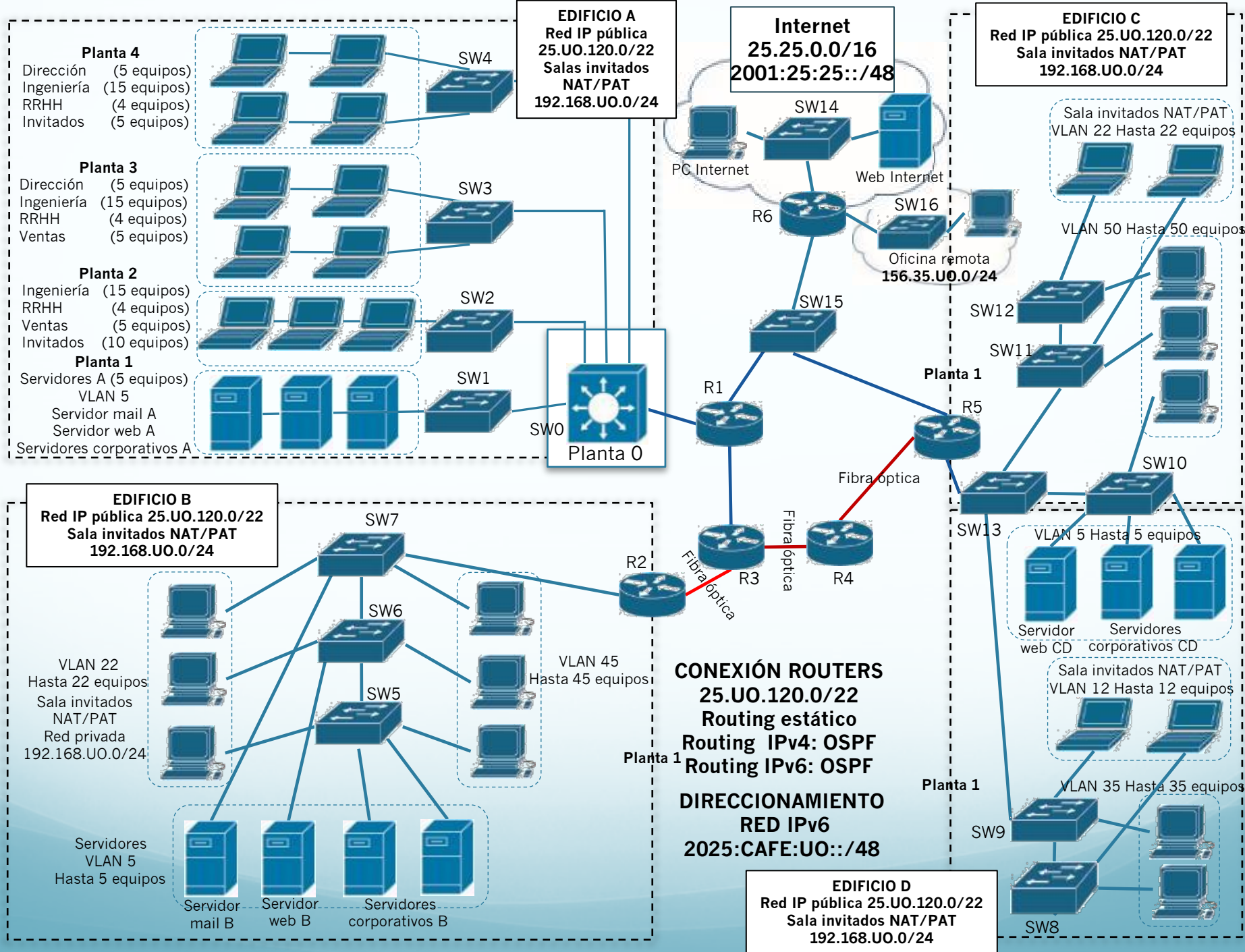


Ingeniería de Redes

Escenario examen laboratorio 2025

Grado en Ingeniería Informática en Tecnologías de la
Información



Enunciado

- Una compañía dispone de 4 edificios en un parque empresarial (Edificios A, B, C, D). La estructura de la compañía hace que la distribución y funcionalidad de la red sea distinta en cada edificio, como muestra la figura.
- Para el direccionamiento **IP público** de **todas las redes de todos los edificios**, UO son las dos últimas cifras de vuestro identificador UO (ej: UO123456, UO=56, red 25.56.120.0/22).
- En el **Edificio A** las plantas 2 a 4 del edificio están ocupadas por personal de dirección y los departamentos de ingeniería, RRHH y ventas con la distribución que se indica. Se han habilitado dos salas para invitados que utilizarán direcciones IPv4 privadas. La planta 1 alberga la sala de servidores A. La conectividad entre los equipos se realizará mediante redes VLAN. Aunque para el direccionamiento IP se debe tener en cuenta el número de equipos de cada departamento, en el escenario simulado solamente es necesario incluir un PC por departamento y planta. Se incluirán 4 servidores en la planta 1, según se indica en el escenario (mail A, web A y dos servidores corporativos A).
- La sala de invitados utiliza **NAT/PAT** con direcciones privadas 192.168.UO.0/24.
- Para el routing entre las VLAN de A se utilizará un switch layer 3 (SW0 según se indica en el escenario).
- En el **Edificio A** todas las direcciones IPv4 son públicas (25.UO.120.0/22) y para los invitados se utilizan direcciones IP privadas (192.168.UO.0/24). No es necesario hacer subnetting para las salas de invitados.
- A los servidores web A y mail A debe poder acceder cualquier equipo de la empresa e Internet a los puertos web y smtp. Al resto de puertos de esos equipos sólo accederá el personal de A, excepto los invitados.
- A los servidores corporativos A (todos los puertos) sólo puede acceder el personal del edificio A y los empleados de la VLAN 35 del edificio D. Los invitados no pueden acceder a estos servidores.

Enunciado

- En el **Edificio B**, de una planta, se ha dividido la red en tres segmentos: un segmento de equipos del personal de la empresa (VLAN 45), un segmento de equipos para una sala de invitados (VLAN 22) y un segmento de servidores (VLAN 6) con el servidor web B, el servidor mail B y el resto de servidores corporativos B. Los tres segmentos se configurarán en tres switches apilados (SW5-SW6-SW7), conectados por enlaces troncales y la conexión a R2 se realizará utilizando una sola interfaz del router (*router-on-a-stick*).
- Por motivos de seguridad, la compañía desea que los equipos de la sala de invitados del **edificio B** sólo puedan intercambiar información con los servicios web B, web A, mail B, mail A (tcp, puertos 80/25) y con Internet. No deben acceder a ningún otro equipo de la empresa. A los servidores corporativos B (todos los puertos) sólo puede acceder el personal de la empresa (25.UO.120.0/22).
- La sala de invitados utiliza **NAT/PAT** con direcciones privadas 192.168.UO.0/24. El **edificio B** comparte espacio de direccionamiento IP público con la red de routers y el resto de edificios (25.UO.120.0/22). Se debe utilizar **DHCP** para la autoconfiguración de todos los PCs del edificio (VLAN 22, VLAN 45). Los servidores (VLAN 6) se configuran manualmente para disponer de una IP fija.
- NOTA: si las ACL filtran el tráfico **DHCP** puede solucionarse con la regla aplicada en sentido *in* en la interfaz/subinterfaz del router:
 - `access-list NUM permit udp any eq bootpc any eq bootps`
- Los equipos de la **oficina remota** en Internet (156.35.UO.0/24) tienen acceso a todos los puertos de los servidores del **edificio B**.

Enunciado

- Los **Edificios C-D**, anexos, constan de una planta, con switches apilados para conectar varios equipos (SW8-SW9, SW11-SW12). En cada edificio hay una sala de invitados (VLAN 22-VLAN 12) y una sala de trabajo del personal de la empresa (VLAN 50-VLAN 35). La sala de servidores (VLAN 6) es compartida por los dos edificios.
- Para las salas de invitados, tanto de estos **edificios C-D** como de los **edificios A y B**, se utilizará NAT/PAT (red privada 192.168.UO.0/24). Se debe utilizar **DHCP** para la autoconfiguración de todos los PCs del edificio. Los servidores (VLAN 6) se configuran manualmente.
- Las salas de invitados solamente tendrán acceso a los servicios web A, web B, web C-D (tcp, puerto 80), mail A, mail B (tcp, puerto 25) y a Internet.
- Las salas de trabajo del personal de la empresa sólo pueden acceder al edificio A, a la sala de servidores C-D y a todos los servidores web y mail de la empresa (web A, web B, web C-D, mail A, mail B). Además, los empleados de VLAN 35 del edificio D podrán acceder a todos los puertos de los servidores corporativos B.
- A los servidores corporativos C-D (todos los puertos) pueden acceder el personal de esos edificios, la oficina remota (156.35.UO.0/24) y el personal de dirección e ingeniería del Edificio A.

Enunciado

- En la **red de routers** se utilizan las líneas marcadas en rojo (Fibra óptica) para disponer de más capacidad en el intercambio de datos entre los edificios B-CD. El resto de conexiones se han incluido para disponer de la posibilidad de redundancia en la red. Se deben configurar rutas estáticas (IPv4 e IPv6) para asegurar que las conexiones entre los edificios B-CD, en ambos sentidos, se realicen a través de los enlaces de fibra. El resto de rutas se obtendrán mediante OSPF para IPv4 e IPv6. Todos los routers y SW0 tendrán configurados OSPF.
- El **router R3** debe filtrar todas las direcciones IPv4 privadas en todas sus interfaces:
 - 10.0.0.0 - 10.255.255.255 (10.0.0.0/8)
 - 172.16.0.0 - 172.31.255.255 (172.16.0.0/12)
 - 192.168.0.0 - 192.168.255.255 (192.168.0.0/16)
- La **red Internet** puede simplificarse a un switch con un PC y un servidor web (duals IPv4/IPv6) conectados a R6, con el direccionamiento IP del rango indicado en el esquema de red. Desde Internet solo se puede acceder a los servidores web A, mail A, web B, mail B, web C-D y a los PCs de la empresa que dispongan de acceso a Internet. Los equipos de la **oficina remota** en Internet (156.35.UO.0/24) tienen acceso a todos los puertos de los servidores del **edificio B y C-D**.
- Todos los equipos de la red son **duals**, de forma que soportan **IPv4 e IPv6**. Las direcciones IPv6 se obtendrán mediante *subnetting* de la red **2025:CAFE:UO::/48** en subredes /64. Para obtener la misma funcionalidad que con IPv4 se configurará routing **IPv6 estático** para la conexión entre los edificios B-CD y routing **OSPF** en el resto de la red. No se emplea NAT/PAT en IPv6
- Las **listas de acceso** se configurarán solamente para **IPv4**. Se utilizarán listas de acceso **extendidas** en todos los casos.

Enunciado

- Puede utilizarse el **router 2911** añadiendo interfaces de fibra óptica con el módulo **HWIC-1GE-SFP** y un adaptador **SFP** (el adaptador es **GLC-LH-SMD** que va acoplado al "hueco" del módulo HWIC-1GE-SFP). Si se necesita (no obligatorio) configurar enlaces a 100Mbps se puede emplear el comando **speed** en la configuración de las interfaces de cobre.
- Para asegurar la comunicación Gigabit Ethernet con el módulo SFP de fibra óptica del router, en el **switch PT-SWITCH** se debe añadir una interface de fibra de Gigabit Ethernet con el módulo **PT-SWITCH-NM-1FGE**
- También se puede emplear el módulo **HWIC-2T** con dos interfaces serie para disponer de más interfaces para los enlaces entre routers. El comando **clock rate** permite configurar la velocidad de envío de datos (en bits por segundo) por el enlace serie.
- Como **Switch Layer 3** debe utilizarse el equipo **3650-24 PS** ya que tiene soporte para IPv6 (**#ipv6 unicast-routing**).