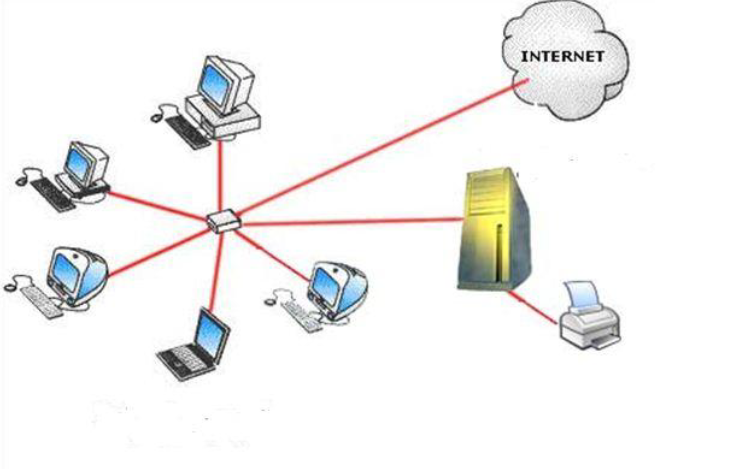
|  |  |  |
| --- | --- | --- |
| sistemas informaticos | | CASO PRACTICO 1 UD5 |
|  | | |
|  | | |
|  |  | |
| alumno cesur 24/25  Alejandro Muñoz de la Sierra | PROFESOR  Efren Zurita Alonso | |

introduccion

Miremos el caso práctico: una compañía que se dedica al suministro de material de oficina necesita que todos sus aparatos se comuniquen sin andar de rodeos. Se dispone de cuatro PC de sobremesa, un portátil, un servidor (al que se conecta, a su vez, una impresora) y la idea es simple, que cada dispositivo tenga acceso a internet y pueda "hablar" con los otros sin mayores complicaciones. La red se arma, en esencia, con una topología en estrella –esto significa que un aparato central (normalmente un switch gestionado) dirige todo el tráfico–, y para esto se asignan direcciones IP, se elige el dispositivo interconector, se evalúan los sistemas operativos y se mira el impacto de cada configuración en el rendimiento general (en la mayoría de los casos, esto resulta clave).

Esquema suministrado para el caso práctico



# 01

Asignación de direcciones IP y máscara de red

Distribuir direcciones IP y definir la máscara de red es, en esencia, darle a cada dispositivo un “DNI” digital para que pueda charlar con los demás. Una dirección IP se comporta casi como una huella única asignada a cada aparato dentro de una red; en nuestro caso, usamos IPv4, que llega en cuatro pedazos numéricos separados por puntos, por ejemplo, 192.168.1.1. Lo básico es que esta cifra se reparte en dos partes: una que señala a qué “barrio”—o red—pertenece el dispositivo, y otra que lo diferencia del resto, como cuando en 192.168.1.20, “192.168.1” designa la comunidad y “20” es el número de casa, por decirlo de alguna manera.

Ahora bien, la máscara de red funciona casi como un cartón que delimita cuál parte del número le corresponde al barrio y cuál a la casa. Se expresa igual que la IP (por ejemplo, 255.255.255.0) y, en la mayoría de los casos, actúa como un límite: si dos aparatos comparten el mismo barrio y barrera, se comunican sin que haya intermediarios (sin embargo, de vez en cuando, si no están en sintonía, es necesario pasar por un router). Así, una máscara de 255.255.255.0 quiere decir que los tres primeros bloques (ej. 192.168.1) ya están fijos como la zona y el último bloque abre la posibilidad de tener hasta 254 dispositivos, casi como tener 254 casitas en el mismo vecindario.

Cuando nos metemos a elegir el rango de direcciones, se prefiere, para redes internas, valerse de direcciones privadas definidas en la norma RFC 1918. Esto asegura que esos números, que no se pueden ver desde Internet, aumenten la seguridad. Curiosamente, hay tres “vecindarios” en IPv4:

• Clase A: Desde 10.0.0.0 hasta 10.255.255.255 (16.777.216 opciones, imagina la cantidad)

• Clase B: Entre 172.16.0.0 y 172.31.255.255 (aproximadamente 1.048.576 hosts)

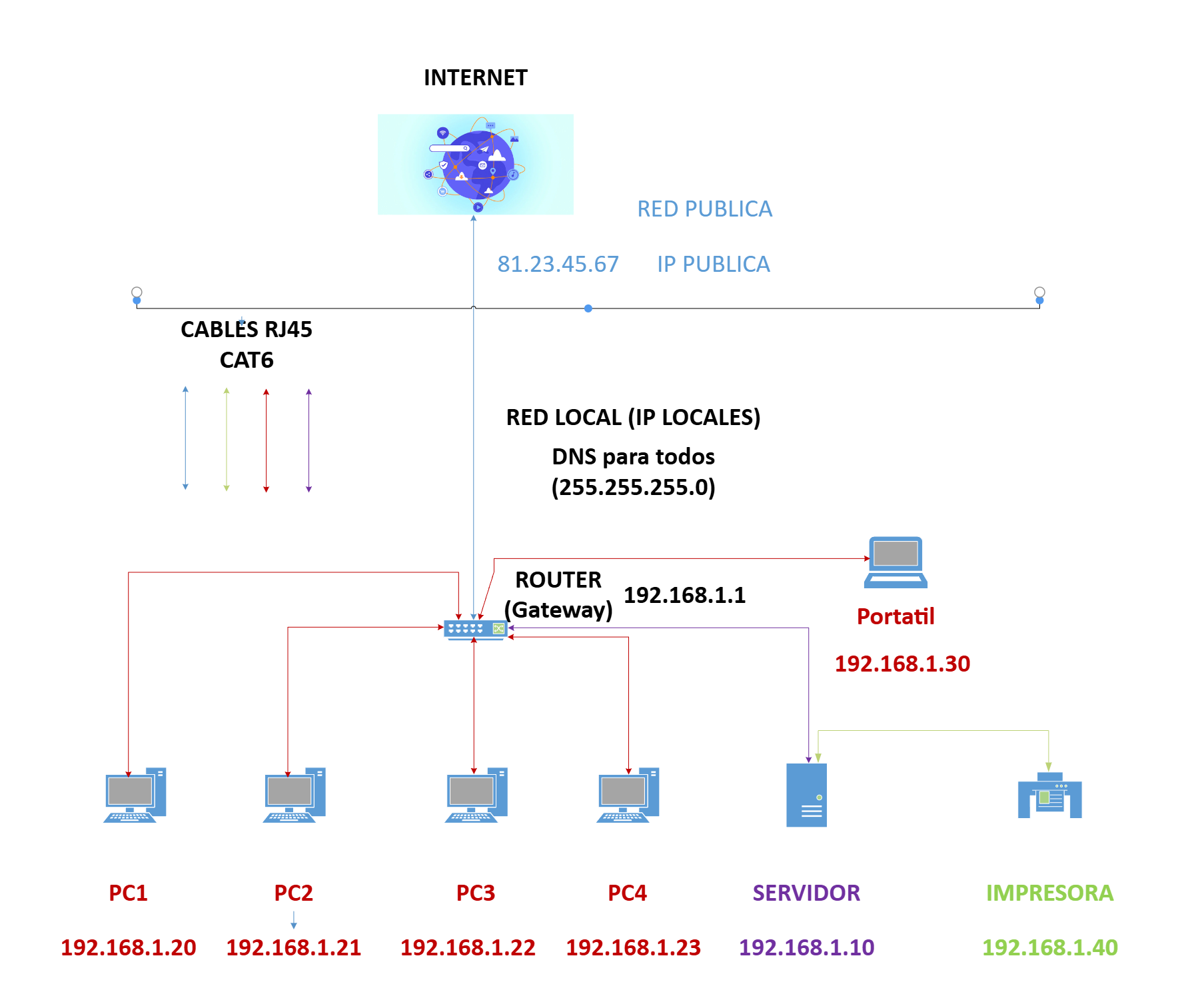
• Clase C: Del 192.168.0.0 al 192.168.255.255 (alrededor de 65.536 direcciones)

En nuestro caso, se opta por una red de Clase C, concretamente 192.168.1.0/24, porque solo necesitamos un grupo acotado (máximo 254 dispositivos) lo que simplifica, a la vez, la administración y reduce la complejidad.

Pasando ya a la parte práctica, la red se diseñó de modo que cada equipo tenga su espacio numérico bien definido. Por ejemplo, el router (o puerta de enlace principal) se asienta en 192.168.1.1, siendo el encargado de conectar con el exterior, mientras que el servidor se ubica en 192.168.1.10 para destacarlo entre los clientes. Los PCs se acomodan en la secuencia 192.168.1.20, 192.168.1.21, 192.168.1.22 y 192.168.1.23, lo que ayuda a identificarlos de inmediato; el portátil se fija en 192.168.1.30, dándole su propio pedacito alejado, y la impresora se reserva el 192.168.1.40, lo que facilita su manejo por separar su función de la de usuario.



Diagrama de red



¿Por qué organizarlo así? Pues, en la mayoría de los casos esta estructura ayuda a mantener el orden y la escalabilidad:

El router en 192.168.1.1 actúa como la entrada natural para redes pequeñas.

Ubicar el servidor en 192.168.1.10 lo separa de los clientes, siendo más fácil su gestión.

Los PCs, al acumularse en el intervalo 192.168.1.20–192.168.1.23, se pueden identificar rápidamente.

Asignando direcciones diferentes para el portátil y la impresora se evitan confusiones y se mejora el control general.

Este modo de repartir los números no solo ayuda a evitar choques de direcciones (esas colisiones indeseables que pueden causar problemas) sino que también abre la puerta a futuras expansiones sin que se arme un lío. Aunque, claro, si la empresa llega a crecer y se requieren más subredes, siempre se podrá recurrir al subnetting para adaptar la red a nuevos requerimientos—algo así como dividir el vecindario en manzanas más pequeñas.

En definitiva, contar con una asignación precisa de direcciones IP y una máscara que actúe como un límite bien definido permite:

– Una comunicación directa entre dispositivos que comparten el mismo “barrio”.

– Un sistema escalable que, en la mayoría de los casos, mantiene el orden sin que se complique demasiado la administración.

– La evitación de conflictos gracias a una distribución lógica y un tanto flexible de las direcciones.

Así, al final del día, la red se vuelve fácil de gestionar y cualquier comunicación interna se lleva a cabo sin mayores inconvenientes, aportando a la seguridad y eficiencia del sistema en general. Divide la red en partes más pequeñas.

🔹 Emplea VLANs para segregar el tráfico – por ejemplo, separa los datos de empelados, visitantes y dispositivos IoT en compartimentos distintos.

🔹 Ajusta las reglas del firewall y utiliza parámetros de QoS para que, en la mayoría de los casos, se refuerce la seguridad y se administre el flujo de tráfico de forma más eficaz.

En definitiva, este plan nos brinda, generalmente, una base robusta que facilita el desarrollo y la expansión de la red, adaptándose a las futuras necesidades empresariales.

# 02

Elección del dispositivo de interconexión

Dado que la red se basa en una estructura en estrella, se hizo necesario escoger un dispositivo central robusto. En vez de un hub simple, se prefirió un switch gestionado, ya que estos permiten manejar el tráfico de datos de manera más inteligente (reduciendo colisiones y ofreciendo segmentación mediante VLANs) y mejoran la seguridad interna. Además, la escalabilidad para incorporar futuros equipos es mucho mejor. Aclaramos que el router se encarga de conectar a internet y distribuye IPs de forma dinámica mediante DHCP, algo especialmente útil para dispositivos móviles o IoT.

# 03

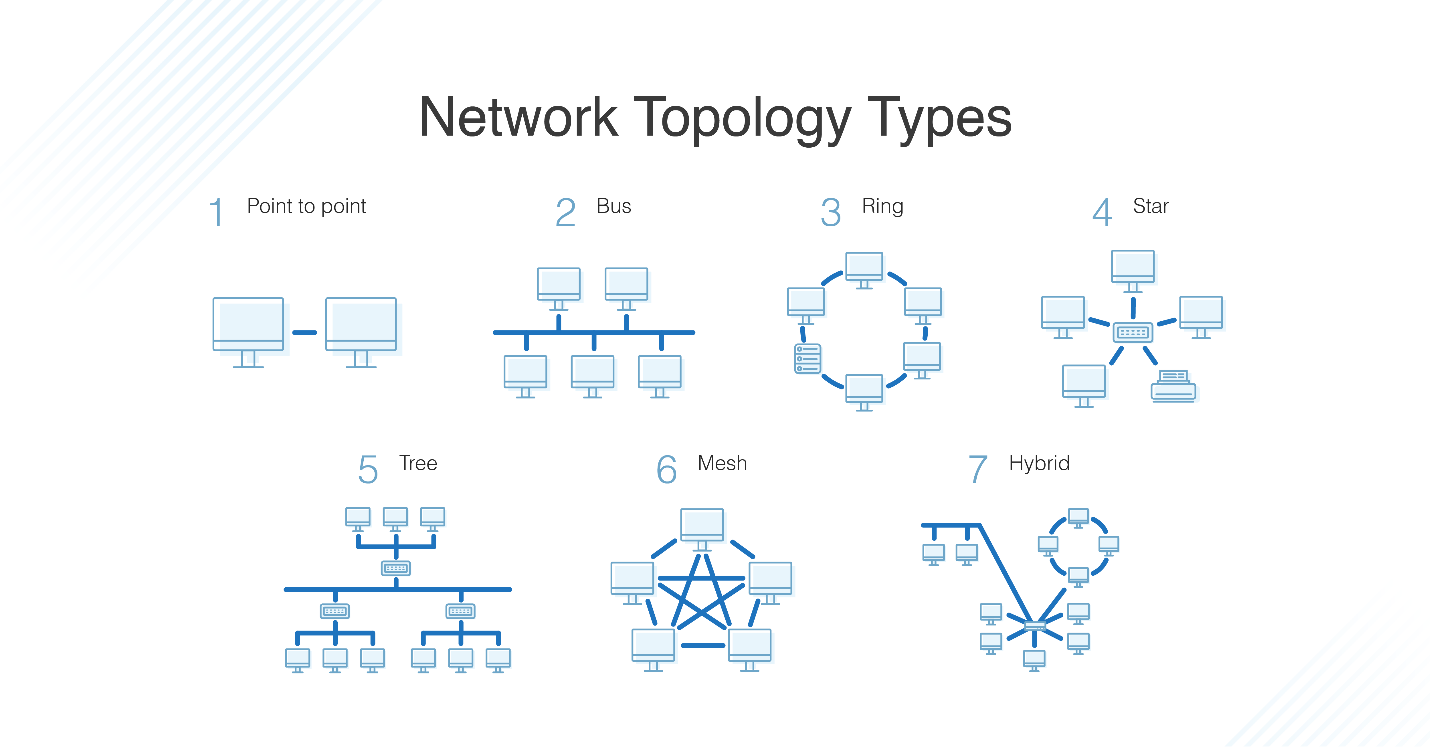
Sistemas operativos de los equipos

Para las PC de sobremesa y el portátil, se recurrió a Windows, pues es el sistema habitual en oficinas y soporta una amplia variedad de software empresarial. En cambio, para el servidor se escogió una distribución Linux, por ejemplo Ubuntu Server o Debian, dadas sus bondades en cuanto a estabilidad, seguridad y rendimiento en tareas críticas como la gestión de archivos, impresión, control de accesos y hasta en el hosting de aplicaciones empresariales. Con respecto a la impresora, si es un modelo en red, generalmente trae su propio sistema operativo embebido, que se administra a través de una interfaz web –lo cual, aunque parezca obvio, agilizaba el trabajo.

# 04

Identificación del modelo de red

La topología que se implementó es, en pocas palabras, de estrella. Cada dispositivo se conecta a un nodo central (aunque a veces se alterna entre un switch o el mismo router). Entre sus ventajas destacan la facilidad para gestionar y mantener la red, el hecho de que la falla en un aparato no derrumba toda la red y su buen rendimiento en redes pequeñas o medianas. Eso sí, hay que ser consciente de que si el dispositivo central se avería, toda la red se ve afectada, y puede resultar algo más costoso frente a alternativas como la topología de bus.



# 05

Impacto de conectar la impresora a un equipo en lugar del servidor

Se barajó la opción de conectar la impresora directamente a uno de los PCs, pero surgieron varios inconvenientes. Por un lado, se genera una dependencia directa del equipo host: si dicho PC falla, la impresora se ve comprometida. Además, esto complica la administración de la impresora y su accesibilidad para otros usuarios de la red. En resumen, es preferible mantener la impresora vinculada al servidor para garantizar una gestión centralizada y un funcionamiento más estable.

En definitiva, esta configuración –con sus diversas consideraciones y pequeñas imperfecciones en el proceso de asignación (¡nada perfecto en la primera pasada, claro!)– se ajusta bastante bien a las necesidades de una empresa de suministros de oficina, combinando lo técnico con una solución práctica y escalable. Si la impresora se conecta directamente a un equipo, cualquier apagón o fallo hace que nadie pueda imprimir; además, la máquina encargada de gestionar esas tareas se sobrecarga, lo que baja notablemente su rendimiento. Compartirla entre Windows y Linux también complica todo, ya que la administración se vuelve un lío inesperado.

💡 Alternativa recomendada:

Mejor dejar la impresora fija en el servidor; así se centraliza la gestión y se garantiza un acceso casi ininterrumpido.

Y si la impresora solo admite conexión USB, se puede optar por un servidor de impresión dedicado o emplear un adaptador de red para transformarla en una impresora de red.

# 05

conclusiones

Con este caso práctico, pusimos en marcha conceptos básicos de administración de redes y armamos una infraestructura que, en la mayoría de los casos, resulta tanto eficiente como segura para la empresa.

🔹 Algunos aspectos clave en nuestra configuración fueron:

Una asignación de direcciones IP bien organizada,

El uso de un switch gestionado que mejora el flujo de datos,

La implementación de un servidor Linux que facilita la administración de la red, y

La elección de una topología en estrella, que simplifica la gestión y permite escalabilidad.

También consideramos el impacto de conectar la impresora al servidor en vez de a una PC individual y llegamos a la conclusión de que centralizar su gestión es, generalmente hablando, la opción que asegura la disponibilidad del recurso compartido.

Posibles mejoras futuras:

🔹 Quizá implementar VLANs para conseguir una segmentación de red más fina,

🔹 Configurar QoS para darle prioridad al tráfico crítico, y

🔹 Usar firewalls para robustecer la seguridad de toda la infraestructura.

Este ejercicio, en definitiva, nos ayudó a reforzar conocimientos sobre protocolos TCP/IP, distintas topologías de red y el manejo de dispositivos de interconexión, sentando una base sólida para futuras configuraciones y ampliaciones de la red.

# 06

referencias

https://ccnadesdecero.es/router-direccion-192-168-0-1-o-192-168-1-1/

https://www.redeszone.net/tutoriales/configuracion-routers/activar-configurar-firewall-cortafuegos-router-pc/

<https://community.fs.com/es/article/network-switch-vs-network-router-vs-network-firewall.html>

<https://www.fortinet.com/lat/resources/cyberglossary/firewall-configuration>

<https://miro.com/es/diagrama/que-es-diagrama-red/>

<https://www.youtube.com/watch?v=Y2L_7ewQteI>

<https://www.pccomponentes.com/search/?query=redes&fm-390>

<https://mundowin.com/configuracion-de-redes-informacion-basica-y-conexiones/>

<https://www.youtube.com/watch?v=awLJkNHBoms>

<https://www.youtube.com/watch?v=hP459L3FIZ0>

<https://www.youtube.com/watch?v=1pB2kan_AFk>

<https://www.dte.us.es/personal/sivianes/TC/P1Enunciado.pdf>