Sistemas Informáticos

UD6. Actividad 4

Entendiendo las redes

Pavel Miron

Contenido

Actividad: Entendiendo conceptos

Objetivo

El objetivo de esta actividad es comprobar que el alumnado ha comprendido los conceptos fundamentales sobre conexiones de red: direccionamiento IP, subredes, configuración IP, resolución de nombres y puertos de comunicación.

Instrucciones

Responde de forma individual y razonada a los siguientes apartados. Se valorará tanto la exactitud como la claridad en la explicación.

Bloque 1: Direccionamiento IP

1. Contesta a la siguiente pregunta y justifica tu respuesta

La IP 172.16.0.12 pertenece a:

a) Clase A
b) Clase B

c) Clase C
d) Ninguna de las anteriores

2. Conversión binaria. Escribe en binario la dirección IP 192.168.1.1.

¿A qué clase pertenece?
Pertenece a la clase C

Binario completo es: 11000000.10101000.00000001.00000001

3. Tipo de dirección IP. Indica si las siguientes direcciones son **válidas para un host**, **dirección de red**, **broadcast** o **especiales** (loopback, no asignable, etc.). Justifica cada caso.

127.0.0.1 Loopback (uso interno en el equipo).
192.168.1.0 Dirección de red (no asignable a hosts).
192.168.1.255 Broadcast (envía datos a todos los hosts en la red).
0.0.0.0 No asignable (usada como marcador de posición).
10.0.0.15 Válida para host (parte de la red privada clase A).

4. **Identificación de red y broadcast.** Dada la IP 192.168.2.101 y la máscara 255.255.255.192, indica:

Dirección de red: 192.168.2.64
Dirección de difusión: (broadcast) 192.168.2.127
Número máximo de equipos conectables (hosts): 62 (64 para red y broadcast)

5. **Direcciones disponibles en una subred.** Si una red utiliza el rango 192.168.10.0/26, responde:

¿Cuántas direcciones totales hay en la subred?

64

¿Cuántas se pueden asignar a hosts?
62

¿Cuál es la primera y la última dirección asignable?
Primera dirección: 192.168.10.1
Ultima dirección: 192.168.10.62

6. **IPv4 vs IPv6.** ¿Qué limitación principal tiene IPv4 que pretende resolver IPv6? Escribe un ejemplo de dirección IPv6.

IPv4: Agotamiento de direcciones (~4.3 mil millones).

IPv6: 2001:0db8:85a3::8a2e:0370:7334.

7. **Razonamiento aplicado.** ¿Por qué crees que muchas redes locales utilizan direcciones de clase C como 192.168.x.x en lugar de otras?

Son ideales para redes pequeñas (hasta 254 hosts), fáciles de administrar y privadas (no enrutables en Internet).

Bloque 2: Configuración IP

8. **Configuración estática y dinámica.** Explica la diferencia entre configuración IP estática y dinámica. Da **dos ventajas y dos inconvenientes** de cada una.

Estática:
Ventajas: Estabilidad, control total.
Inconvenientes: Administración manual, riesgo de conflictos.

Dinámica (DHCP):
Ventajas: Automatización, escalabilidad.
Inconvenientes: Dependencia del servidor DHCP, posible latencia.

9. **Aplicación práctica.** Imagina que vas a montar un servidor web en tu casa. ¿Usarías una IP estática o dinámica? ¿Por qué?

Usaría IP estática.
Evita cambios de dirección que romperían el acceso externo.

10. **Windows vs Linux.** ¿Cómo configurarías manualmente una IP estática en:
Windows 10 (entorno gráfico)
Linux Ubuntu (terminal)?

Windows 10:
Ajustes > Red > Propiedades TCP/IPv4 > Ingresar IP manualmente.

Linux Ubuntu Terminal:
sudo nano /etc/netplan/01-netcfg.yaml
sudo netplan apply

11. Comandos útiles:
    ¿Qué comando te permite ver la configuración IP en Windows?
    ¿Y en Linux?

Windows: ipconfig
Linux: ifconfig

12. **Identificación.** Dada esta configuración en un equipo:

```
Dirección IP: 192.168.0.10
Máscara: 255.255.255.0
Puerta de enlace: 192.168.0.1
DNS: 8.8.8.8
```

¿Qué ocurre si otro equipo se configura con la misma IP? ¿Qué problemas puede haber?

Conflicto de IP, pérdida de conectividad en ambos equipos.

Bloque 3: Máscaras de subred

13. Cálculo de red. Dada la IP 192.168.1.34 y la máscara 255.255.255.224, calcula:

- Dirección de red 192.168.1.32
- Dirección de broadcast 192.168.1.63
- Número de hosts disponibles 30
- Primer y último host asignable

Primer :
192.168.1.33

Ultimo:
192.168.1.62

14. **Notación CIDR. ¿Qué es la notación CIDR?** Convierte a formato CIDR las siguientes máscaras:

- 255.255.255.0 /24
- 255.255.254.0 /23
- 255.255.255.248 /29

15. **Diseño de red.** Si quieres diseñar una red para 50 dispositivos, ¿qué máscara usarías? ¿Por qué?

/26 son 62 hosts, el tamaño mas pequeño que cubre 50 hosts

16. **Aplicación web.** Usa la web https://www.calculadora-redes.com para comprobar tus resultados del ejercicio 13. ¿Coinciden?

Si coinfiden

Bloque 4: DNS y resolución de nombres

17. **Funcionamiento del DNS** Describe paso a paso cómo se resuelve un nombre de dominio cuando escribimos www.google.com en el navegador.

- Al principio hace una consulta para mirar en el chache local, si ya esta no hace falta preguntar a DNS.
- Si no esta, pregunta al servidor DNS, que le manda la respuesta.
- El servidor DNS busca recursivamente (root - .com – google.com).
- Devuelve la IP

18. **Caché DNS.** ¿Qué es la caché de resolución de nombres? ¿Qué ventajas y qué riesgos tiene?

Es mecanismo que nos ayuda almacenar temporalmente todos los registros DNS de nombres de dominio previamente vistas.

19. Ficheros locales.

• ¿Qué información contiene el fichero /etc/hosts en Linux?

Contiene las líneas de texto, que son asociados a un nombre de dominio son una solo dirección web IP

• ¿Y el archivo hosts en Windows?

Lo mismo que en el Linux los nombres de dominio y los IPs

20. **DNS públicos.** ¿Qué son los DNS públicos? Da el nombre y dirección IP de **dos servicios DNS gratuitos conocidos**.

Son opciones recomendadas, gratuitas por su rapidez y su preocupación de la privacidad de los usuarios. Ejemplo: GOOGLE DNS (8.8.8.8) o CLOUDFARE DNS (1.1.1.1 y 1.0.0.1)

21. **DNS y seguridad.** ¿Qué tipo de ataques pueden dirigirse al sistema DNS? Nombra uno y explica brevemente en qué consiste.

Secuestro de DNS: Redirección fraudulenta de consultas DNS a sitios maliciosos para robo de datos o propagar malware.

Inundaciones TCP SYN: Ataque DoS que satura recursos del servidor con solicitudes SYN falsas, bloqueando tráfico legítimo.

Ataque de dominio fantasma: Creación masiva de dominios falsos para sobrecargar servidores DNS y provocar denegación de servicio.

Tunelización DNS: Uso de consultas DNS para evadir seguridad y filtrar datos o controlar sistemas remotos.

Ataques con Botnet: Redes de dispositivos infectados que lanzan ataques masivos (DDoS, spam, etc.) de forma coordinada.

Amplificación DDoS: Explotación de servidores para multiplicar el tráfico enviado a la víctima, saturando su ancho de banda.

Envenenamiento de caché DNS: Inyección de registros DNS falsos en un servidor para redirigir usuarios a sitios maliciosos.

Ataque de cobertura: Manipulación DNS como distracción para ocultar otro ataque más grave.

Malware DNS: Software malicioso que altera la resolución DNS o compromete servidores.

Inundación DNS: Envío masivo de peticiones DNS para colapsar servidores y denegar servicio.
Ataque DRDoS: Ataque DDoS que usa servidores DNS públicos para reflejar y amplificar tráfico hacia la víctima.

Bloque 5: Puertos y protocolos

22. **Protocolos TCP vs UDP.** Completa la tabla:

Característica	TCP	UDP
Orientado a conexión	Conexión	Sin conexión
Velocidad	Más lento	Mas rápido
Fiabilidad	Fiable	No fiable
Ejemplo de uso	HTTP, FTP	VoIP, DNS

23. Asociación de puertos

Asocia los siguientes servicios a sus puertos por defecto:

- HTTP **80**
- HTTPS **443**
- FTP **21**
- MySQL **3306**
- SMTP **25**
- DNS **43**
- SSH **22**

24. **Detección de puertos abiertos.** ¿Qué comando puedes usar en:

- Windows para ver puertos abiertos?

Netstat –a –n –o
-a: muestra todos los puertos y conexiones.
-n: muestra direcciones y números de puerto en formato numérico.
-o: muestra el ID del proceso (PID) asociado al puerto.

- Linux para lo mismo?

ss –tulnp o netstat –tulnp

25. **Puertos bien conocidos y registrados.** Explica qué diferencia hay entre puertos **bien conocidos**, **registrados** y **dinámicos**. ¿Por qué es importante conocer esta clasificación?

Los puertos bien conocidos (0–1023), son los mas importantes asignados a los servidores universales.
Ejemplo: 80 HTTP (web) o 443 HTTPS (web seguro).

Puertos registrados (1024–49151)para aplicaciones o servicios menos comunes como, pero oficiales: 3306 MySQL o alternativo para HTTP 8080.

Puertos dinámicos (49152–65535), temporales que los usan las programas para conectarse, por ejemplo Chrome usa una de estos para recibir datos.

26. **Cierre de puertos.** ¿Cómo cerrarías manualmente un puerto en Windows mediante el firewall?

Por comandos porque es mas rápido

```
New-NetFirewallRule -DisplayName "Bloquear Puerto 8080" -Direction Inbound -L
ocalPort 8080 -Protocol TCP -Action Block
```

-DisplayName: Nombre de la regla.
-Direction Inbound: Bloquea conexiones entrantes.
-LocalPort 8080: Puerto a bloquear (cambia al que necesites).
-Protocol TCP/UDP: Elige el protocolo.
-Action Block: Deniega el tráfico.

27. **Puertos y seguridad.** ¿Por qué es importante cerrar puertos no utilizados en un sistema operativo y/o en el router? Da un ejemplo de riesgo.

Los puertos proporciona o facilita diversos servicios y aplicaciones de internet, permitiendo que funcionan correctamente. Si los puertos no amenazan la seguridad de la red, pueden ser utilizadas por hackers, por esto es fundamental tenerlos adecuadamente.
Ejemplo:
Puerto 3389 (RDP - Escritorio Remoto)
Si está abierto en tu router o PC y no lo usas, un atacante podría intentar con fuerza bruta para robar tu contraseña y tomar el control de tu ordenador.