**PREGUNTA1: ¿Cómo dividirías la red 172.16.0.0/24 en subredes para satisfacer las necesidades anteriores, asignando direcciones IP a cada segmento de la base? Indica las subredes obtenidas (con su notación de máscara /xx), la cantidad de hosts útiles en cada una, y especifica qué subred se destinaría al enlace troncal interplanetario.**

Subredes Asignadas

1. Comando Central

* Subred: 172.16.0.0/26
* Rango de hosts: 172.16.0.1 – 172.16.0.62
* Broadcast: 172.16.0.63
* Hosts útiles: 62

2. Defensa Perimetral

* Subred: 172.16.0.64/27
* Rango de hosts: 172.16.0.65 – 172.16.0.94
* Broadcast: 172.16.0.95
* Hosts útiles: 30

3. Centro Médico

* Subred: 172.16.0.96/27
* Rango de hosts: 172.16.0.97 – 172.16.0.126
* Broadcast: 172.16.0.127
* Hosts útiles: 30

4. Hangar y Taller

* Subred: 172.16.0.128/28
* Rango de hosts: 172.16.0.129 – 172.16.0.142
* Broadcast: 172.16.0.143
* Hosts útiles: 14

5. Enlace Troncal con la Antena

* Subred: 172.16.0.144/30
* Rango de hosts: 172.16.0.145 – 172.16.0.146
* Broadcast: 172.16.0.147
* Hosts útiles: 2

RESUMEN DEL PLAN DE REDES:

| **Subred** | **Dirección de red** | **Máscara** | **Rango de Hosts** | **Broadcast** | **Hosts útiles** |
| --- | --- | --- | --- | --- | --- |
| Comando Central | 172.16.0.0 | /26 | 172.16.0.1 – 172.16.0.62 | 172.16.0.63 | 62 |
| Defensa Perimetral | 172.16.0.64 | /27 | 172.16.0.65 – 172.16.0.94 | 172.16.0.95 | 30 |
| Centro Médico | 172.16.0.96 | /27 | 172.16.0.97 – 172.16.0.126 | 172.16.0.127 | 30 |
| Hangar y Taller | 172.16.0.128 | /28 | 172.16.0.129 – 172.16.0.142 | 172.16.0.143 | 14 |
| **Enlace Troncal** | 172.16.0.144 | /30 | 172.16.0.145 – 172.16.0.146 | 172.16.0.147 | 2 |

**Direcciones Disponibles Restantes**

Después de la subred /30, quedan sin asignar:

* Desde 172.16.0.148 hasta 172.16.0.255  
  Esto permite futuras expansiones, sensores remotos, o nodos de defensa adicionales.

**PREGUNTA 2: Compara el enrutamiento estático con el enrutamiento dinámico. ¿Cuáles son las ventajas e inconvenientes de cada enfoque en la administración de rutas? En tu respuesta, menciona al menos un protocolo de enrutamiento dinámico (por ejemplo, RIP u OSPF) y comenta por qué los protocolos de vector de distancia difieren de los de estado de enlace en términos de rendimiento y complejidad.**

| **Característica** | **Enrutamiento Estático** | **Enrutamiento Dinámico** |
| --- | --- | --- |
| **Configuración** | Manual por el administrador | Automática entre routers |
| **Adaptabilidad** | No se adapta a cambios en la red | Se ajusta automáticamente ante caídas o nuevas rutas |
| **Uso de CPU/RAM** | Bajo consumo de recursos | Mayor consumo de recursos (procesamiento, memoria) |
| **Escalabilidad** | Limitada (difícil de gestionar en redes grandes) | Muy buena para redes grandes o complejas |
| **Seguridad** | Más segura (rutas predefinidas, sin intercambio de info) | Puede ser más vulnerable si no se configura adecuadamente |
| **Mantenimiento** | Alto (cada cambio requiere reconfiguración manual) | Bajo (se autoconfigura con los protocolos) |

**Ventajas e Inconvenientes**

**Ventajas del Enrutamiento Estático**

* Control total del tráfico.
* Más seguro (no se intercambia información con otros routers).
* Consumo mínimo de recursos.

**Desventajas del Enrutamiento Estático**

* No se adapta a fallos de red automáticamente.
* Escalar requiere mucho trabajo manual.
* Difícil de mantener en redes con muchos enlaces o cambios frecuentes.

**Ventajas del Enrutamiento Dinámico**

* Se adapta automáticamente ante caídas o cambios.
* Escalabilidad en redes grandes.
* Ahorra tiempo en configuración en redes complejas.

**Desventajas del Enrutamiento Dinámico**

* Uso de CPU, RAM y ancho de banda mayor.
* Más complejo de configurar y depurar.
* Potencial riesgo si se propagan rutas incorrectas.

**Ejemplo de protocolo dinámico: OSPF**

* **OSPF (Open Shortest Path First)** es un protocolo de enrutamiento dinámico basado en **estado de enlace**.
* Es ideal para redes empresariales grandes y críticas.
* Calcula la mejor ruta usando el algoritmo de **Dijkstra**, tomando en cuenta el "costo" (ancho de banda, retraso, etc.).

| **Comparativa** | **Vector de Distancia (Ej. RIP)** | **Estado de Enlace (Ej. OSPF)** |
| --- | --- | --- |
| **Método** | Informa a sus vecinos de rutas conocidas | Conoce toda la topología de la red |
| **Frecuencia de Actualización** | Periódica (cada 30 seg en RIP) | Solo cuando hay cambios |
| **Velocidad de convergencia** | Lenta | Rápida |
| **Uso de recursos** | Bajo | Alto |
| **Complejidad** | Baja (fácil de configurar) | Alta (requiere planificación) |
| **Escalabilidad** | Limitada (máx 15 saltos en RIP) | Alta (ideal para grandes redes) |

**PREGUNTA 3: Explica el funcionamiento básico del sistema DNS y su importancia en la comunicación en redes. ¿Cómo realiza la red rebelde (o cualquier red TCP/IP) la resolución de nombres de dominio a direcciones IP? Incluye en tu explicación qué es un servidor DNS y un registro (por ejemplo, un registro A), ilustrando con un ejemplo simple (por ejemplo: traducir holonet.rebelion.org a una dirección IP)​.   
Además, menciona brevemente qué sucede si el servidor DNS no está disponible y cómo eso afectaría a las comunicaciones de la Alianza  
¿Qué es el DNS y por qué es tan importante?**

El Sistema de Nombres de Dominio (DNS) es como la agenda telefónica de la galaxia: traduce nombres fáciles de recordar (como holonet.rebelion.org) en direcciones IP (como 192.168.50.7) que los dispositivos realmente utilizan para comunicarse.

Sin DNS, los usuarios tendrían que memorizar direcciones IP, lo que haría la comunicación tan difícil como navegar un campo de asteroides a ciegas.

Funcionamiento básico del DNS (paso a paso)

Cuando en la Red Rebelde alguien intenta conectarse a echo.base, la red realiza estos pasos:

1. Consulta Local: El dispositivo revisa primero su caché DNS local. Si no tiene la IP asociada al nombre, consulta a su servidor DNS configurado (generalmente el del router o proveedor de red).
2. Servidor Recursivo DNS: Este servidor actúa como mensajero Jedi, y si no tiene la información, pregunta a otros servidores:
   * Servidor raíz (.): Le indica dónde están los servidores del dominio de nivel superior (TLD) como .org.
   * Servidor TLD (.org): Le dice cuál es el servidor DNS autoritativo para rebelion.org.
   * Servidor autoritativo (rebelion.org): Este finalmente responde con la IP real de holonet.rebelion.org, por ejemplo: 192.168.50.7.
3. Respuesta al Cliente: La IP se devuelve al dispositivo, que ahora puede contactar directamente al servidor de holonet.rebelion.org.
4. Caché: Para no repetir esta misión cada vez, el resultado se guarda temporalmente en la memoria local (caché DNS).

¿Qué es un Servidor DNS?

Un Servidor DNS es un equipo en la red cuya misión es resolver nombres de dominio y devolver sus respectivas direcciones IP.

Existen distintos tipos de servidores DNS:

* Recursivos: hacen la búsqueda completa por el usuario.
* Autoritativos: tienen las respuestas finales (como registros de dominios específicos).

¿Qué es un Registro DNS?

Los registros DNS son entradas que definen qué IP u otra información se asocia a un nombre.

Ejemplo común:

* Registro A (Address): Asocia un nombre de dominio con una dirección IPv4.

Ejemplo:

makefile

CopiarEditar

Nombre: holonet.rebelion.org

Tipo: A

Dirección: 192.168.50.7

Esto significa que si alguien quiere acceder a holonet.rebelion.org, la red sabrá que debe contactarse con la IP 192.168.50.7.

Fallo en la Resolución de Nombres

* Las estaciones de trabajo, naves o sistemas de la Alianza no podrán traducir los nombres de dominio (como echo.base, holonet.rebelion.org, etc.) a sus respectivas direcciones IP.
* En consecuencia, los equipos no podrán iniciar conexiones, aunque la red física funcione perfectamente.

Impacto en la Comunicación Rebelde

* Correo electrónico, acceso web, transmisiones seguras y módulos de coordinación de flotas que dependen de nombres de dominio dejarán de funcionar.
* Solo funcionarán las conexiones directas por IP (si se conocen), lo que limita enormemente la operación y ralentiza las respuestas estratégicas.

Medidas de contingencia galácticas

* Configurar múltiples servidores DNS (principal y secundario).
* Usar caché DNS local para resolver temporalmente nombres ya consultados.
* Implementar DNS interno redundante en las bases

**PREGUNTA 4: Pregunta: Compara los protocolos TCP y UDP y sus características en contexto de la transmisión de datos. ¿Por qué TCP se considera un protocolo confiable y orientado a conexión, y qué implica eso en cuanto a rendimiento? ¿Por qué UDP es no confiable y sin conexión, y en qué casos su rapidez resulta ventajosa?​**

[**es.linkedin.com**](https://es.linkedin.com/advice/0/youre-trying-establish-network-connection-rwzie?lang=es#:~:text=1%20Caracter%C3%ADsticas%20de%20TCP)

**​**

[**es.linkedin.com**](https://es.linkedin.com/advice/0/youre-trying-establish-network-connection-rwzie?lang=es#:~:text=2%20Caracter%C3%ADsticas%20de%20UDP)

**En tu respuesta, menciona ejemplos de aplicaciones o situaciones galácticas para cada protocolo: por ejemplo, qué tipo de datos enviarías mediante UDP durante una misión crítica, y cuál vía TCP en comunicaciones rutinarias. *(Pista: TCP garantiza la entrega de datos completa y ordenada – ideal para transmitir planes estratégicos; UDP minimiza retrasos – útil para enviar coordenadas de combate en tiempo real, aunque alguna pueda perderse.)*.**

TCP (Transmission Control Protocol)

* Orientado a conexión: Antes de transmitir datos, TCP establece una conexión entre emisor y receptor mediante el "three-way handshake".
* Garantiza que los datos lleguen completos, en orden, y sin duplicados.
* Control de flujo y congestión: Ajusta la velocidad de transmisión para no saturar la red.
* Retransmisión automática si hay pérdida de paquetes.
* Más lento, debido a los mecanismos de control, pero ideal para datos críticos.

Ejemplo:

* Enviar los planos detallados de la Estrella de la Muerte desde Scarif a la base rebelde.
* Transmitir informes estratégicos entre comandantes de la flota.

UDP (User Datagram Protocol)

* No orientado a conexión: No hay verificación previa ni aseguramiento de recepción.
* No confiable: Los paquetes pueden perderse, duplicarse o llegar desordenados.
* Sin control de flujo o congestión: Transmisión más directa y rápida.
* Ideal cuando la velocidad es más importante que la precisión.

Ejemplo :

* Coordenadas de combate enviadas en tiempo real a cazas X-Wing.
* Transmisión en vivo desde una cámara de un droide espía en Mustafar.
* Voz sobre IP entre líderes rebeldes durante una batalla.

**PREGUNTA 5: Explica brevemente la diferencia entre cifrado simétrico y cifrado asimétrico en el contexto de las comunicaciones de la Alianza. ¿Cómo funciona cada esquema y qué ventajas ofrece?​**

[**blog.mailfence.com**](https://blog.mailfence.com/es/cifrado-simetrico-vs-asimetrico/#:~:text=El%20cifrado%20sim%C3%A9trico%20utiliza%20una,el%20mensaje%20se%20descifra%20correctamente)

**Por ejemplo, si Leia y Luke comparten una frase clave secreta para cifrar sus holomensajes, ¿qué tipo de cifrado es ese? En cambio, si la Alianza quiere enviar un mensaje a un nuevo aliado sin haber intercambiado una clave secreta previamente, ¿cómo podría ayudar el cifrado asimétrico (claves pública/privada) en ese caso? Comenta también sobre la importancia de autenticación y no repudio en los mensajes (cómo podemos estar seguros de que el mensaje no ha sido alterado y proviene realmente de quien dice ser). Finalmente, menciona por qué utilizar un protocolo seguro (como SSH en lugar de Telnet) es crucial al administrar remotamente los equipos de la red rebelde​**

[**hackernoon.com**](https://hackernoon.com/lang/es/cual-es-la-diferencia-entre-telnet-y-ssh#:~:text=SSH%20usa%20encriptaci%C3%B3n%2C%20espec%C3%ADficamente%20encriptaci%C3%B3n,una%20clave%20privada%20y%20viceversa)

Cifrado Simétrico – “Una sola clave para gobernarlos”

* ¿Cómo funciona?  
  Usa la misma clave secreta para cifrar y descifrar un mensaje.  
  Ambos extremos deben compartir previamente esa clave y mantenerla segura.
* Ejemplo :  
  Si Leia y Luke comparten una frase clave secreta para intercambiar holomensajes cifrados, están usando cifrado simétrico.  
  Ejemplo de algoritmo: AES (Advanced Encryption Standard).
* Ventajas:
  + Rápido y eficiente para grandes volúmenes de datos.
  + Ideal cuando las partes ya tienen una clave compartida.
* Desventajas:
  + Necesita un canal seguro previo para compartir la clave.
  + Si la clave se filtra, todo queda comprometido.

Cifrado Asimétrico – “Dos claves, una pública y otra privada”

* ¿Cómo funciona?  
  Usa un par de claves:
  + Una clave pública (que cualquiera puede conocer)
  + Una clave privada (que solo el destinatario guarda con celo)  
    Lo que se cifra con una, solo puede descifrarse con la otra.
* Ejemplo :  
  Si la Alianza Rebelde quiere enviar un mensaje seguro a un nuevo aliado, sin haber compartido claves antes, puede usar la clave pública del aliado para cifrar el mensaje. Solo el aliado podrá descifrarlo con su clave privada.  
  Ejemplo de algoritmo: RSA (Rivest-Shamir-Adleman).
* Ventajas:
  + No requiere compartir claves secretas previamente.
  + Escalable y útil para entornos abiertos o desconocidos.
* Desventajas:
  + Más lento que el cifrado simétrico.
  + Menos eficiente para grandes volúmenes de datos.

Autenticación y No Repudio – “Confianza en la verdad del mensaje”

* Autenticación: Permite verificar la identidad del remitente. Por ejemplo, si Luke firma digitalmente su mensaje con su clave privada, Leia puede usar su clave pública para verificar la firma.
* No repudio: El remitente no puede negar que envió el mensaje, porque solo él tiene su clave privada para firmarlo.

Esto es crucial para que la Alianza esté segura de que los mensajes no han sido interceptados ni alterados por espías imperiales.

¿Por qué usar protocolos seguros como SSH en lugar de Telnet?

* Telnet transmite datos (¡incluidas contraseñas!) en texto claro, lo cual es peligrosísimo en ambientes hostiles como la galaxia.
* SSH (Secure Shell) cifra toda la comunicación entre terminales, protegiendo la gestión remota de routers, servidores y sensores de la red rebelde.