Parte I – Misiones de Conocimiento Teórico

## Misión 1: Reconexión en la Base Eco (Hoth) – *Direccionamiento IP y Subredes*

**¿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.**

| **Departamento** | **Hosts requeridos** | **Hosts necesarios con margen** | **Tamaño de subred óptima** |
| --- | --- | --- | --- |
| Comando Central | 50 | 62 (por margen) | /26 (64 direcciones, 62 útiles) |
| Defensa Perimetral | 30 | 30 | /27 (32 direcciones, 30 útiles) |
| Centro Médico | 20 | 30 | /27 |
| Hangar y Taller | 14 | 14 | /28 (16 direcciones, 14 útiles) |
| Enlace Troncal | 2-4 | 2+ | /30 (4 direcciones, 2 útiles) |

**Asignación de Subredes y Rango de Hosts:**

1. **Comando Central – /26**
   * Subred: 172.16.0.0/26
   * Rango de hosts útiles: 172.16.0.1 – 172.16.0.62
   * Broadcast: 172.16.0.63
   * 62 hosts útiles
2. **Defensa Perimetral – /27**
   * Subred: 172.16.0.64/27
   * Rango de hosts útiles: 172.16.0.65 – 172.16.0.94
   * Broadcast: 172.16.0.95
   * 30 hosts útiles
3. **Centro Médico – /27**
   * Subred: 172.16.0.96/27
   * Rango de hosts útiles: 172.16.0.97 – 172.16.0.126
   * Broadcast: 172.16.0.127
   * 30 hosts útiles
4. **Hangar y Taller – /28**
   * Subred: 172.16.0.128/28
   * Rango de hosts útiles: 172.16.0.129 – 172.16.0.142
   * Broadcast: 172.16.0.143
   * 14 hosts útiles
5. **Enlace Troncal a la Antena – /30**
   * Subred: 172.16.0.144/30
   * Rango de hosts útiles: 172.16.0.145 – 172.16.0.146
   * Broadcast: 172.16.0.147
   * 2 hosts útiles

## **Misión 2: Sabiduría de Yoda – *Algoritmos de Enrutamiento y Rutas***

**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​**

En redes, existen dos enfoques principales para establecer rutas: enrutamiento estático y enrutamiento dinámico. Ambos tienen ventajas e inconvenientes según el tamaño, la estabilidad y la complejidad de la red.

**Enrutamiento Estático**

Este tipo de enrutamiento se configura manualmente por el administrador de red. Se definen rutas fijas hacia cada destino. Es útil en redes pequeñas o muy estables, donde los caminos no cambian con frecuencia.

Ventajas:

* Mayor control sobre el flujo de datos.
* Bajo consumo de recursos (no hay procesamiento constante ni tráfico de actualización).
* Más seguro, ya que no acepta rutas externas automáticamente.

Inconvenientes:

* No se adapta automáticamente a cambios o fallos en la red (como la caída de un nodo).
* Poco escalable; mantener rutas manuales en redes grandes es complejo y propenso a errores.

**Enrutamiento Dinámico**

En este caso, los routers usan protocolos de enrutamiento para intercambiar información y calcular automáticamente las mejores rutas hacia cada destino. Se adapta de forma constante a los cambios en la topología de red.

Ventajas:

* Adaptable: reacciona ante fallos o cambios sin intervención humana.
* Escalable: ideal para redes grandes o con muchos routers.
* Reducción de errores humanos en la configuración de rutas.

Inconvenientes:

* Requiere más recursos (CPU, RAM, ancho de banda).
* Puede ser más vulnerable si no se configura bien (por ejemplo, aceptar rutas no deseadas).
* Más complejo de implementar y mantener.

Ejemplo de protocolo dinámico: **OSPF**

OSPF (Open Shortest Path First) es un protocolo de estado de enlace, donde cada router conoce toda la topología de la red y calcula las rutas usando el algoritmo de Dijkstra. Es rápido, preciso y adecuado para redes grandes.

En cambio, protocolos como **RIP** (Routing Information Protocol) son de vector de distancia: cada router solo conoce la distancia (en número de saltos) a una red y aprende de sus vecinos.

Diferencias entre Vector de Distancia y Estado de Enlace:

* Vector de distancia (RIP):
  + Más simple y fácil de implementar.
  + Convergencia lenta (puede tardar en detectar cambios).
  + Limitado a 15 saltos.
  + Propenso a bucles si no se usa prevención (como split horizon o hold-down).
* Estado de enlace (OSPF):
  + Más rápido y preciso.
  + Convergencia rápida.
  + Mejor rendimiento y escalabilidad.
  + Mayor uso de recursos y configuración más compleja.

Respuesta ante fallos

* Estático: no detecta automáticamente una caída; se requiere reconfiguración manual.
* Dinámico (como OSPF): detecta la caída del nodo y recalcula las rutas automáticamente, manteniendo la conectividad.

En resumen, el enrutamiento estático es útil en redes simples y controladas. El dinámico, aunque más complejo, es indispensable en entornos grandes y variables como una red interplanetaria.

## Misión 3: Los Nombres del Holonet – *DNS y Resolución de Nombres*

**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.**

El DNS (Domain Name System) es un sistema esencial en cualquier red basada en TCP/IP. Su función principal es traducir nombres de dominio legibles para humanos (como holonet.rebelion.org) en direcciones IP que las computadoras necesitan para comunicarse entre sí (como 192.0.2.42).

Sin DNS, los usuarios tendrían que memorizar direcciones IP numéricas para acceder a servicios, lo cual sería poco práctico, especialmente a escala galáctica.

Consulta local: El sistema operativo primero revisa si el nombre ya fue resuelto recientemente (en caché).

Servidor DNS configurado: Si no está en caché, el dispositivo pregunta al servidor DNS configurado (a menudo proporcionado por la red local).

Resolución jerárquica: Si ese servidor no conoce la respuesta, comienza una búsqueda jerárquica:

* Contacta a un servidor raíz.
* Este le refiere al servidor de dominio de nivel superior (por ejemplo, .org).
* Luego, ese servidor refiere al servidor autoritativo del dominio rebelion.org.

Respuesta final: El servidor autoritativo devuelve la dirección IP asociada a holonet.rebelion.org (por ejemplo, 192.0.2.42).

Conexión: Con esa IP, el dispositivo puede ahora conectarse al servicio deseado.

Un servidor DNS es un equipo que almacena y proporciona información sobre nombres de dominio. Puede ser:

* Recursivo: hace todo el trabajo de buscar en la jerarquía por ti.
* Autoritativo: contiene respuestas oficiales sobre los dominios que administra.

Un registro A (Address Record) es un tipo de entrada en un servidor DNS que asocia un nombre de dominio con una dirección IPv4.

Si el servidor DNS falla o no está accesible, ningún nombre de dominio podrá resolverse. Aunque las redes físicas estén funcionando, los dispositivos no sabrán cómo llegar a los servicios. En el caso de la Alianza Rebelde:

* No podrían acceder a bases de datos, estaciones o comandos usando nombres.
* Comunicaciones críticas se interrumpirían, aunque la red esté activa.
* Se necesitaría usar direcciones IP directamente (si se conocen), lo que reduce eficiencia y aumenta el riesgo de errores.

## Misión 4: *“Es una trampa… de protocolos!”* – TCP vs UDP en las transmisiones

**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?​**

TCP (Transmission Control Protocol) es un protocolo orientado a conexión. Antes de transmitir datos, establece una conexión entre emisor y receptor mediante un proceso de handshake (intercambio inicial de paquetes). Además:

* Asegura que los datos lleguen completos, sin errores y en el orden correcto.
* Implementa control de flujo, retransmisiones en caso de pérdida, y verificación de entrega.
* Es más lento, pero muy confiable.

Por eso TCP es ideal para:

* Transferencia de archivos importantes (como los planos de la Estrella de la Muerte).
* Correo electrónico (para que no se pierda ni una palabra de la estrategia rebelde).
* Navegación web (consultas a bases de datos, reportes de inteligencia).

Ventaja: Alta confiabilidad.  
Desventaja: Más latencia (retraso), más sobrecarga en la red.

Luke siente diferencias en sus transmisiones porque está experimentando dos estrategias distintas de envío de datos:

* Cuando los datos deben llegar completos y confiables, como instrucciones estratégicas o información crítica: se usa TCP.
* Cuando es más importante la rapidez y el tiempo real, como imágenes en vivo o coordenadas de combate, incluso si se pierde alguna trama: se usa UDP.

## Misión 5: Comunicación Segura o lado oscuro – *Criptografía y Seguridad de la Red*

**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?​**

Existen dos enfoques principales para cifrar mensajes:

Cifrado Simétrico

* Definición: Se utiliza una sola clave secreta para cifrar y descifrar la información.
* Ejemplo galáctico: Leia y Luke comparten una frase clave (“Alderaan vive”) y la usan para codificar sus mensajes privados. Ambos necesitan conocerla de antemano y mantenerla en secreto.
* Ventajas:
  + Rápido y eficiente para cifrar grandes volúmenes de datos.
* Desventajas:
  + Requiere un canal seguro previo para intercambiar la clave, lo que puede ser peligroso si es interceptado.

Cifrado Asimétrico (Criptografía de clave pública)

* Definición: Utiliza un par de claves:
  + Una clave pública (que se puede compartir abiertamente).
  + Una clave privada (que se mantiene en secreto).
* Funcionamiento:
  + Si la Alianza quiere enviar un mensaje a un nuevo aliado, simplemente usa la clave pública del receptor para cifrarlo.
  + Solo el receptor podrá descifrarlo con su clave privada.
* Ventajas:
  + No requiere compartir una clave secreta previamente.
  + Permite autenticación y firma digital.

Autenticación y No Repudio

* Autenticación: Verifica que el mensaje proviene realmente del remitente.
  + Esto se puede lograr usando firmas digitales: el remitente cifra un resumen del mensaje con su clave privada, y el receptor lo verifica con la clave pública.
* No repudio: Garantiza que el remitente no pueda negar haber enviado el mensaje.
  + En otras palabras, si Leia firma un mensaje, no puede luego decir que fue falsificado.

Seguridad en la Administración Remota: SSH vs Telnet

* Telnet transmite la información sin cifrar, incluyendo contraseñas. Un espía imperial podría leerla fácilmente.
* SSH (Secure Shell) cifra toda la comunicación, evitando que el Imperio pueda ver las órdenes enviadas a los sistemas remotos.
* Por eso, al administrar servidores o routers de la red rebelde, usar SSH es crucial para proteger las credenciales y comandos.