**Examen Parcial 2**

**Rodrigo Yepes Rubio**

**Parte I – Misiones de Conocimiento Teórico**

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

Para dividir eficientemente la red 172.16.0.0/24 en subredes que cubran los requerimientos de la Base Eco, se aplicó subneteo considerando la cantidad de hosts que necesita cada departamento. A continuación se detallan las subredes asignadas, con su notación CIDR, cantidad de hosts útiles y el rango de direcciones para cada una:

**1. Comando Central (~50 hosts)**

Se necesita una subred con al menos 50 hosts útiles.  
Una subred /26 ofrece 64 direcciones, con 62 hosts útiles.

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

**2. Defensa Perimetral (~30 hosts)**

Se requiere al menos 30 hosts útiles.  
Una subred /27 ofrece 32 direcciones, con 30 hosts útiles.

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

**3. Centro Médico (~20 hosts**)

Se necesita al menos 20 hosts útiles.  
Una subred /27 también es suficiente aquí.

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

**4. Hangar y Taller (~14 hosts)**

Se requieren al menos 14 hosts útiles.  
Una subred /28 ofrece 16 direcciones, con 14 hosts útiles.

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

**5. Enlace Troncal (antena interplanetaria)**

Este enlace generalmente necesita pocas IPs, pero se asignará una subred /30, que permite solo 2 hosts útiles (punto a punto, ideal para enlaces troncales).

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

**Tabla de subredes asignadas:**

| **Departamento** | **Subred** | **Hosts útiles** | **Rango de Hosts** |
| --- | --- | --- | --- |
| Comando Central | 172.16.0.0/26 | 62 | 172.16.0.1 – 172.16.0.62 |
| Defensa Perimetral | 172.16.0.64/27 | 30 | 172.16.0.65 – 172.16.0.94 |
| Centro Médico | 172.16.0.96/27 | 30 | 172.16.0.97 – 172.16.0.126 |
| Hangar y Taller | 172.16.0.128/28 | 14 | 172.16.0.129 – 172.16.0.142 |
| Enlace Troncal Antena | 172.16.0.144/30 | 2 | 172.16.0.145 – 172.16.0.146 |

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

El enrutamiento es el proceso por el cual los datos encuentran su camino desde el origen hasta el destino a través de una red. Existen dos grandes enfoques: **enrutamiento estático** y **enrutamiento dinámico**. Ambos tienen ventajas y desventajas, y la elección de uno u otro depende del tamaño, estabilidad y necesidades de la red.

**Enrutamiento Estático**

Definición:  
Las rutas se configuran manualmente por un administrador de red. Los dispositivos no cambian ni descubren nuevas rutas automáticamente.

Ventajas:

* Simplicidad: Fácil de implementar en redes pequeñas o estables.
* Control total: El administrador sabe exactamente por dónde pasan los datos.
* Menor carga de CPU y ancho de banda: No hay necesidad de intercambiar información de rutas.

Desventajas:

* No se adapta a fallos: Si un enlace o nodo cae, la ruta sigue existiendo aunque esté inactiva, a menos que se corrija manualmente.
* Difícil de escalar: En redes grandes o cambiantes, mantener rutas estáticas es complejo y propenso a errores.

Ejemplo de uso: Una red entre dos estaciones rebeldes fijas que nunca cambian.

**Enrutamiento Dinámico**

Definición:  
Los dispositivos intercambian información sobre la red para aprender y actualizar automáticamente sus tablas de enrutamiento.

Ventajas:

* Adaptación automática: Si un nodo cae o cambia el estado de un enlace, los routers ajustan sus rutas sin intervención humana.
* Escalabilidad: Ideal para redes grandes como la HoloRed galáctica.
* Redundancia y resiliencia: Permite múltiples caminos alternativos.

Desventajas:

* Mayor consumo de recursos: Necesita más CPU, memoria y ancho de banda para intercambiar información.
* Complejidad: Configurar y entender los protocolos puede requerir experiencia avanzada.

Ejemplo de protocolo dinámico:

* OSPF (Open Shortest Path First) – Protocolo de estado de enlace, muy eficiente y escalable, ideal para grandes organizaciones.

**Diferencias entre Protocolos de Vector de Distancia y Estado de Enlace**

1. Protocolos de Vector de Distancia (como RIP)

* Cada router informa a sus vecinos sobre la distancia (en saltos) a cada red conocida.
* Simples, pero lentos en adaptarse a cambios (pueden tardar hasta 180 segundos en RIP).
* Sufren del problema de *cuentas envenenadas* o *bucles de enrutamiento*.
* Requieren menos procesamiento.

2. Protocolos de Estado de Enlace (como OSPF)

* Cada router conoce el estado de todos los enlaces de la red y calcula la ruta más corta usando algoritmos como Dijkstra.
* Se propagan rápidamente los cambios, lo que mejora la convergencia.
* Más complejos y requieren más recursos, pero ofrecen mejor rendimiento y estabilidad.

**Comparación general**

| **Característica** | **Estático** | **Dinámico** |
| --- | --- | --- |
| Configuración inicial | Manual | Automática con protocolos |
| Adaptación a fallos | No | Sí |
| Escalabilidad | Baja | Alta |
| Requiere experiencia | Moderada | Alta |
| Consumo de recursos | Bajo | Medio-Alto |
| Ejemplo de protocolo | N/A | RIP (vector de distancia), OSPF (estado de enlace) |

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

El Sistema de Nombres de Dominio (DNS, por sus siglas en inglés) es uno de los pilares de la comunicación en redes TCP/IP, tanto en la galaxia como en la Tierra. Su función es traducir los nombres simbólicos (fáciles de recordar para los seres vivos, como *holonet.rebelion.org*) en direcciones IP (comprensibles para las máquinas, como *192.0.2.15*).

**¿Cómo funciona el DNS?**

Cuando un equipo rebelde quiere conectarse a un nombre como echo.base, necesita saber a qué dirección IP corresponde. La resolución de nombres se realiza en los siguientes pasos:

1. El equipo cliente (por ejemplo, un droide o terminal) consulta su caché local para ver si ya conoce la IP del dominio.
2. Si no la tiene, envía una solicitud a su servidor DNS configurado (generalmente asignado por DHCP).
3. El servidor DNS recursivo busca la IP correspondiente, consultando otros servidores DNS en caso necesario. Por ejemplo:
   * Si se pide holonet.rebelion.org, el DNS consultará primero a los servidores raíz, luego a los servidores del dominio “org”, y finalmente a los de “rebelion.org”, hasta obtener la IP asociada al nombre.
4. El servidor DNS devuelve al cliente un registro que contiene la dirección IP, como por ejemplo:
   * Registro A: vincula un nombre de dominio con una dirección IPv4.  
     Ejemplo: holonet.rebelion.org → 192.0.2.15
5. Con esta dirección IP, el dispositivo puede establecer la conexión deseada con la base, servidor o nave remota.

**Registros DNS (solo uno):**

* **Registro A**: Traduce un dominio a una dirección IPv4.  
  Ejemplo:  
  Nombre: holonet.rebelion.org  
  Tipo: A  
  Dirección IP: 192.0.2.15

**¿Qué es un servidor DNS?**

Un servidor DNS es un equipo o servicio encargado de procesar solicitudes de resolución de nombres. Puede:

* Ser recursivo, buscando la información por sí mismo.
* Ser autoritativo, si posee la información exacta de un dominio específico.

**¿Qué pasa si el servidor DNS no está disponible?**

Si el servidor DNS no responde:

* Los nombres de dominio no pueden resolverse a direcciones IP.
* Aunque la red esté físicamente conectada, no será posible acceder a sitios, servidores o servicios por nombre.
* Esto interrumpe las comunicaciones en la HoloRed, como si intentaras llamar a alguien sin saber su número.

En el contexto rebelde, eso significa que las naves no podrían conectarse entre sí usando nombres simbólicos, lo que complicaría enormemente las operaciones tácticas, coordinación entre bases, y acceso a sistemas de datos remotos.

**Ejemplo de resolución completa:**

* El técnico ingresa: ping holonet.rebelion.org
* El sistema busca en el DNS y recibe: 192.0.2.15
* Se establece la conexión con el servidor ubicado en esa dirección IP.

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

En la capa de transporte del modelo TCP/IP existen dos protocolos principales: TCP (Transmission Control Protocol) y UDP (User Datagram Protocol). Ambos se encargan de transportar datos entre dispositivos, pero lo hacen de forma muy diferente según las necesidades de la comunicación.

**TCP – Protocolo confiable y orientado a conexión**

Características principales:

* Confiable: Garantiza que los datos lleguen completos, sin errores y en el orden correcto.
* Orientado a conexión: Antes de enviar datos, se establece una conexión entre emisor y receptor (proceso de *three-way handshake*).
* Control de errores y retransmisión: Si un paquete se pierde, TCP lo detecta y lo reenvía.
* Control de flujo y congestión: Evita sobrecargar la red o al receptor.

Ventajas:

* Ideal para transmisiones que requieren integridad total de los datos.
* Asegura una comunicación estable y estructurada.

Desventajas:

* Más lento debido al establecimiento de conexión, verificaciones, y retransmisiones.
* Consume más recursos.

Ejemplos galácticos de uso de TCP:

* Enviar los planos de la Estrella de la Muerte al Alto Mando Rebelde: es vital que toda la información llegue íntegra.
* Comunicaciones de mando seguras, archivos logísticos, mensajes estratégicos o administrativos entre bases.

**UDP – Protocolo rápido pero no confiable**

Características principales:

* No confiable: No asegura que los datos lleguen, ni controla si se entregan en orden.
* Sin conexión: No hay necesidad de establecer una conexión antes de enviar.
* Sin retransmisión ni control de flujo.

Ventajas:

* Muy rápido: Ideal para situaciones en tiempo real donde la velocidad es más importante que la precisión total.
* Menor sobrecarga de red.

Desventajas:

* Algunos paquetes pueden perderse sin notificación.
* El orden de llegada puede no coincidir con el orden de envío.

Ejemplos galácticos de uso de UDP:

* Stream de vídeo en vivo desde una X-Wing durante combate: perder un fotograma no es tan grave como retrasarse.
* Coordenadas de combate o telemetría en tiempo real: es preferible recibir datos nuevos rápidamente aunque se pierda alguno.
* Comunicaciones por voz o hologramas en tiempo real (tipo VoIP o streaming).

**Tabla de comparación**

| **Característica** | **TCP** | **UDP** |
| --- | --- | --- |
| Confiabilidad | Alta (control de errores, orden) | Baja (sin garantías) |
| Establece conexión | Sí (orientado a conexión) | No (sin conexión) |
| Velocidad | Más lento | Muy rápido |
| Uso de recursos | Alto | Bajo |
| Casos ideales | Archivos, datos importantes | Video, voz, juegos, sensores |

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

Para proteger las comunicaciones de la Alianza Rebelde y evitar que caigan en manos del Imperio, es esencial usar técnicas de cifrado. El cifrado transforma un mensaje legible en uno incomprensible, a menos que se posea la clave correcta para descifrarlo. Existen dos formas principales de cifrado: simétrico y asimétrico.

**Cifrado simétrico**

* Utiliza una sola clave secreta, que se usa tanto para cifrar como para descifrar el mensaje.
* Todos los participantes deben conocer y mantener segura la misma clave.
* Es rápido y eficiente, ideal para comunicaciones frecuentes y de alto volumen.

Ejemplo galáctico:  
Si Leia y Luke comparten una frase clave secreta para cifrar y descifrar sus holomensajes, están usando cifrado simétrico.  
💬 Frase clave: "QueLaFuerzaTeAcompañe" → ambos deben conocerla de antemano.

Ventaja: Velocidad y eficiencia.  
Desventaja: Requiere que ambas partes se pongan de acuerdo y protejan la clave. Si la clave se filtra, toda la comunicación está comprometida.

**Cifrado asimétrico (clave pública/privada)**

* Usa dos claves diferentes pero relacionadas: una clave pública (puede compartirse libremente) y una clave privada (que solo conoce el propietario).
* Si alguien cifra un mensaje con la clave pública de un destinatario, solo ese destinatario podrá descifrarlo usando su clave privada.
* También se puede firmar un mensaje con la clave privada para garantizar la identidad del emisor.

**Ejemplo**:  
Si la Alianza quiere enviar un mensaje a un nuevo aliado en Naboo sin haber intercambiado claves previamente, puede usar la clave pública del aliado para cifrar el mensaje. Así, solo ese aliado podrá leerlo con su clave privada.

Ventaja: No es necesario compartir previamente una clave secreta.  
Desventaja: Es más lento y computacionalmente exigente.

**Autenticación y no repudio**

Para que una comunicación rebelde sea completamente segura, debe garantizar:

* Autenticación: Saber con certeza quién envió el mensaje.  
  → Se puede lograr con firmas digitales basadas en la clave privada del emisor.
* No repudio: Evitar que el remitente niegue haber enviado el mensaje.  
  → Una firma digital vinculada a la clave privada del emisor sirve como prueba irrefutable.

Esto es clave para asegurar que, por ejemplo, un mensaje enviado por Mon Mothma realmente proviene de ella y no ha sido alterado por espías del Imperio.

**🛰️ Seguridad en protocolos: ¿por qué usar SSH en vez de Telnet?**

Protocolos como Telnet transmiten datos en texto claro, por lo que un espía imperial podría fácilmente interceptar credenciales y comandos. En cambio, SSH (Secure Shell) cifra toda la comunicación, asegurando que incluso si es interceptada, no pueda leerse.