Examen final redes

Parte teórica

Misión 1:

Red asignada: 172.16.0.0/24

Subred Comando central:

- Host útiles: 62
- **Dirección de Red:** 172.16.0.0/26
- **Máscara de Subred:** 255.255.255.192
- **Rango de Hosts:** 172.16.0.1 - 172.16.0.62
- **Dirección de Broadcast:** 172.16.0.63

Subred de Defensa Perimetral:

- **Host útiles:** 30
- **Dirección de red**: 172.16.0.64/27
- **Máscara de subred**: **255.255.255.224** (/27)
- **Rango de hosts**: 172.16.0.65 - 172.16.0.94
- **Dirección de broadcast**: 172.16.0.95

Subred para centro médico:

- **Host útiles**: 30
- **Dirección de red**: 172.16.0.96/27
- **Máscara de subred**: **255.255.255.224** (/27)
- **Rango de hosts**: 172.16.0.97 - 172.16.0.126
- **Dirección de broadcast**: 172.16.0.127

Subred para Hangar y Taller:

- **Host útiles:** 14
- **Dirección de red**: 172.16.0.128/28
- **Máscara de subred**: **255.255.255.240** (/28)
- **Rango de hosts**: 172.16.0.129 - 172.16.0.142

- **Dirección de broadcast**: 172.16.0.143

Subred para enlace troncal:

- **Host útiles:** 2
- **Dirección de red**: 172.16.0.144/30
- **Máscara de subred**: **255.255.255.252** (/30)
- **Rango de hosts**: 172.16.0.145 - 172.16.0.146
- **Dirección de broadcast**: 172.16.0.147

Misión 2:

El enrutamiento estático se hace manualmente, por lo que es mas sencillo de configurar en redes pequeñas. No requiere la ejecución de protocolos de enrutamiento adicionales, lo que significa menos consumo de recursos en los dispositivos de red.

El enrutamiento dinámico es mucho mejor en cuanto a adaptabilidad los enrutadores ajustan sus tablas de enrutamiento automáticamente ante cambios en la red, como enlaces caídos o nuevos dispositivos. En escalabilidad es mucho más adecuado para redes grandes o complejas, ya que la administración de rutas se realiza automáticamente. Si un enlace falla, los enrutadores pueden encontrar rutas alternativas sin intervención manual, lo que mejora la confiabilidad de la red.

El enrutamiento dinámico es mucho más complejo de configurar que el estático y consume muchos más recursos.

Protocolos de Vector de Distancia (Ej. RIP):

- **Funcionamiento**: Cada enrutador conoce solo las rutas hacia sus vecinos y las actualiza periódicamente.
- **Ventajas**: Simples de configurar, adecuados para redes pequeñas.
- **Inconvenientes**: Convergencia lenta, propensos a bucles de enrutamiento, no escalables para redes grandes.
- **Rendimiento**: Lento y menos eficiente en redes grandes.

Protocolos de Estado de Enlace (Ej. OSPF):

- **Funcionamiento**: Cada enrutador tiene una visión completa de la topología de la red y calcula la ruta más corta usando algoritmos como Dijkstra.
- **Ventajas**: Convergencia rápida, evita bucles, adecuado para redes grandes.
- **Inconvenientes**: Más complejo de configurar y mantener, requiere más recursos.
- **Rendimiento**: Rápido y eficiente, especialmente en redes grandes.

Comparación clave:

- **Rendimiento**: Los protocolos de estado de enlace son más rápidos y robustos, especialmente en redes grandes.
- **Complejidad**: Los protocolos de vector de distancia son más simples pero menos eficientes en redes grandes.

Misión 3:

El DNS (Sistema de Nombres de Dominio) es un sistema de base de datos distribuida que permite resolver nombres de dominio en direcciones IP.

El proceso básico de **resolución de nombres** sigue estos pasos:

1. **Solicitud de Resolución**: El dispositivo (por ejemplo, un navegador) realiza una consulta DNS para obtener la dirección IP asociada con el nombre de dominio **holonet.rebelion.org**.
2. **Consulta al Servidor DNS**: La solicitud se envía a un servidor DNS. Si el servidor DNS no tiene la dirección IP en su caché, la consulta se redirige hacia otros servidores DNS hasta encontrar la respuesta.
3. **Respuesta del Servidor DNS**: El servidor DNS responde con la dirección IP correspondiente al nombre de dominio solicitado. Por ejemplo, podría devolver **192.168.1.10** para **holonet.rebelion.org**.

4. **Conexión**: Una vez que el dispositivo recibe la dirección IP, puede usarla para establecer una conexión directa con el servidor de destino, como un servidor web, y acceder a los recursos solicitados.

Misión 4

El uso de TCP garantiza la llegada de los datos, ya que establece una conexión previa al envio de los datos y mantiene un control de flujo según la capacidad de quien recibirá el paquete ajustando así la velocidad de envio.

En el caso de que se pierda algún byte este se retransmitirá. A diferencia de TCP el protocolo UDP no necesita hacer establecer una conexión previa, lo que disminuye la latencia del envío, tampoco tiene control de flujo y si un paquete se pierde no se reenviara.

Por esto TCP es mejor para servicios de alta fiabilidad, ya que te garantiza que ty paquete llegue.

En cambio UDP es muy útil para transmisiones en tiempo real como por ejemplo un stream, ya que en estos caso la menor latencia es mucho mas importante que la perdida de un paquete.

Mision 5

Cifrado Simétrico

- Funciona: Usa una sola clave secreta que ambas partes deben conocer.
- Ejemplo: Si Leia y Luke comparten una frase clave para cifrar y descifrar sus holomensajes, están usando cifrado simétrico.
- Ventajas:
    - Rápido y eficiente, ideal para transmisiones en tiempo real.
- Desventajas:
    - La clave debe ser compartida de forma segura. Si el Imperio la intercepta, puede leer todos los mensajes.
    - Cifrado Asimétrico
- Funciona: Usa dos claves: una pública (que cualquiera puede usar para cifrar) y una privada (que solo el destinatario tiene para descifrar).

- Ejemplo: Si la Alianza quiere contactar a un nuevo aliado infiltrado en Coruscant sin intercambiar claves previamente, puede usar su clave pública para cifrar el mensaje. Solo él podrá descifrarlo con su clave privada.
- Ventajas:
    - No se necesita compartir claves secretas con anticipación.
    - Permite autenticación y no repudio usando firmas digitales.
- Desventajas:
    - Más lento que el simétrico. A menudo se usa combinado: el asimétrico para intercambiar una clave simétrica, y luego usar ésta para la comunicación continua.