Examen Final de Redes II: Jose Jurado Cortes

# Parte I – Misiones de Conocimiento Teórico (60%)

## Misión 1: Reconexión – Direccionamiento IP y Subredes

Para diseñar un esquema de direccionamiento eficiente usando la red 172.16.0.0/24, aplicamos subnetting para los siguientes requerimientos:  
  
- Comando Central: 50 hosts → Subred de al menos 64 direcciones → /26  
- Defensa Perimetral: 30 hosts → Subred de al menos 32 direcciones → /27  
- Centro Médico: 20 hosts → Subred de al menos 32 direcciones → /27  
- Hangar y Taller: 14 hosts → Subred de al menos 16 direcciones → /28  
- Enlace troncal: ~2 hosts → Subred de 4 direcciones → /30  
  
Subredes asignadas:  
1. Comando Central: 172.16.0.0/26 → Rango: 172.16.0.1 - 172.16.0.62  
2. Defensa Perimetral: 172.16.0.64/27 → Rango: 172.16.0.65 - 172.16.0.94  
3. Centro Médico: 172.16.0.96/27 → Rango: 172.16.0.97 - 172.16.0.126  
4. Hangar y Taller: 172.16.0.128/28 → Rango: 172.16.0.129 - 172.16.0.142  
5. Enlace troncal: 172.16.0.144/30 → Rango: 172.16.0.145 - 172.16.0.146

## Misión 2: Algoritmos de Enrutamiento y Rutas

El enrutamiento estático implica configurar manualmente las rutas. Es confiable y predecible, pero no escala bien ni responde automáticamente a fallos.  
  
Ventajas:  
- Control total del administrador  
- Menor uso de CPU y ancho de banda  
  
Desventajas:  
- No se adapta a fallos automáticamente  
- No escalable para redes grandes  
  
El enrutamiento dinámico, como RIP o OSPF, ajusta rutas automáticamente.  
  
Ventajas:  
- Adaptable a cambios en la red  
- Escalable  
  
Desventajas:  
- Mayor consumo de recursos  
  
Protocolos como RIP (vector de distancia) son simples, intercambian tablas completas periódicamente. OSPF (estado de enlace) es más eficiente: construye un mapa topológico completo, calcula rutas con Dijkstra y converge más rápido.

## Misión 3: DNS y Resolución de Nombres

El DNS (Domain Name System) traduce nombres de dominio a direcciones IP.  
  
Ejemplo: holonet.rebelion.org → 192.0.2.10  
  
Funcionamiento:  
1. Cliente consulta su servidor DNS local.  
2. Si no tiene la respuesta, consulta servidores raíz, luego TLD, y finalmente autoritativos.  
3. Obtiene el registro A (IPv4) y responde.  
  
Si el servidor DNS falla, no se puede resolver nombres a IP, y servicios web, correo o VoIP fallan.  
  
Importancia: Sin DNS, los usuarios necesitarían recordar direcciones IP, lo que dificulta la gestión y el uso de redes.

## Misión 4: Comparación TCP vs UDP

TCP: Confiable, orientado a conexión, asegura entrega ordenada.  
- Ejemplo: transferencia de archivos, correo electrónico, HTTP.  
- Garantiza integridad y orden, pero con más latencia.  
  
UDP: No confiable, sin conexión, más rápido y ligero.  
- Ejemplo: videollamadas, streaming en tiempo real.  
- Permite pérdidas para ganar velocidad.  
  
Uso:  
- TCP para transmisiones críticas que no toleran pérdida.  
- UDP para datos en tiempo real donde velocidad es clave.

## Misión 5: Criptografía y Seguridad de la Red

Cifrado simétrico: misma clave para cifrar y descifrar (ej. AES).  
- Ejemplo: Leia y Luke comparten una frase clave.  
- Rápido, pero requiere intercambio seguro de claves.  
  
Cifrado asimétrico: par de claves pública/privada (ej. RSA).  
- Ejemplo: un nuevo aliado recibe clave pública de la Alianza para mensajes.  
- Más seguro para entornos distribuidos.  
  
Autenticación: asegura identidad del emisor.  
No repudio: evita que el emisor niegue haber enviado el mensaje.  
Protocolos como SSH en vez de Telnet cifran comunicaciones, previniendo espionaje en conexiones remotas.