

Examen redes

Parte 1

1. El Mural de las Siete Capas

El mural representa el modelo OSI que esta formado por:

- Capa física: define las Interfaces mecánicas y eléctricas/ópticas mediante los que se transmite la información.
- Capa de enlace de datos: convierte el medio de transmisión físico en una línea de comunicación.
- Capa de red: Se encarga del enrutamiento de paquetes desde el origen hasta el destino
- Capa de transporte: Divide los datos para adaptarlos a la red y se asegura que los mensajes vayan en orden de llegada y que lleguen a todas las capas.
- Capa de sesión: Establece y administra sesiones entre dispositivos.
- Capa de presentación: sirve para traducir datos a distintos formatos.
- Capa de aplicación: Interactúa con el usuario y les permite usar protocolos (ej: correo electrónico)

Este antiguo protocolo se relaciona con el actual en su paso por las diferentes capas en la que cada una modifica el mensaje para adaptarlo según va llegando a su destino.

2. Los Dos Pergaminos del Mensajero

El Mensajero Confiable equivale a TCP El Mensajero representa UDP.

TCP es más fiable ya que garantiza que las entregas lleguen sin errores y en el orden en el que fueron enviados, mientras que UDP no lo garantiza.

TCP está protegido de la sobrecarga de la red gracias al control de flujo, no como UDP

En cuanto a velocidad UDP es más rápido que TCP porque no necesita verificar la recepción de los paquetes.

TCP tiene también un mayor uso de recursos por el control de los datos, UDP no tiene este problema por lo que consume mucho menos.

Cada protocolo se utiliza en diferentes situaciones ya que en uno te aseguras de que los mensajes lleguen como se enviaron, sin errores y en orden, mientras que en el otro usas menos recursos y transmites de forma más veloz los datos pero con menos seguridad.

3. El Enigma de las Subredes

Su máscara de red por defecto era 255.255.255.0 por lo que necesitarían cambiarla a **255.255.255.192** para conseguir 4 subredes del mismo tamaño, cada subred tendría **62 hosts utilizables**.

Dividir la red en 4 subredes corresponde a quitarle a una máscara de /24 2 bits de los 8 que tienen para hosts, estos se usaran para subredes. Para calcular los host por subred utilizamos los 6 bits de hosts $2^6 = 64$, a estos 64 hosts se les quita por subred uno que estará reservado para red y otro que estará reservado para broadcast por lo que no serán hosts utilizables.

4. La Encrucijada de las Rutas

El tótem representa una tabla de enrutamiento, estas son utilizadas por los routers consultando las redes accesibles y los caminos que tienen que seguir para enviar los paquetes hasta su destino.

Las tablas de enrutamiento indican en cada entrada:

- El destino: la dirección de red o host al que se quiere acceder.
- La puerta de enlace: el siguiente salto que se tiene que hacer.
- Interfaz de salida: el puerto del router por donde saldrá el paquete.
- Métrica: da preferencias a distintas rutas según diferentes requisitos.

Actualmente el router se guía por estas tablas de enrutamiento para determinar por donde enviar cada paquete que recibe.

Las flechas fijas y las flechas móviles representan las **rutas estáticas** y las **rutas dinámicas**.

Rutas estáticas: Son rutas establecidas manualmente, que como las flechas son fijas e inmutables ya que estas solo pueden ser modificadas por un administrador, debido a esto son vulnerables sin su ruta deja de estar disponible.

Rutas dinámicas: Son rutas que se adaptan a las condiciones de la red configurándose automáticamente gracias a protocolos de los routers esto las hace muy flexibles ya que cada la ruta cambiará para ser la mejor para las distintas topologías que pueda tener una red a lo largo del tiempo.

5. El Guardián de la Máscara Única

La técnica que se refleja es NAT.

NAT permite que una dirección ip pública sea compartida por varios dispositivos que se encuentren en la misma red privada. Esto funciona mediante el router que en las solicitudes a internet de los dispositivos que están conectados a la red les cambia sus Ips privadas por la ip pública del router. Cuando la información viene del exterior al router este recuerda que dispositivo originó la petición y le reenvía el mensaje.

Beneficios

- Seguridad: el ocultar la ip privada del exterior dificulta a las amenazas digitales a llegar a los dispositivos ya que no pueden acceder directamente a estos.
- Conservación de direcciones IPv4: Al compartir múltiples dispositivos la misma ip pública eliminamos la necesidad de que cada dispositivo tenga su propia Dirección pública lo que deja libres otras ips y no las agota.

Parte 2

La Ruta Perdida entre Dos Reinos

Para reconstruir la conexión entre las dos ciudades sin nombre conocido utilicé una Cloud-PT que mediante seriales conectaba 2 routers uno en cada ciudad, restaurando así la Ruta sagrada. La nube representará un lugar de autorización de paso para los viajeros, con la intención de hacer más seguro este camino. Cada ciudad está compuesta de un router un switch y 2 pcs. En la Ciudad A los habitantes utilizan la Ip 192.168.10.0/24 siendo 192.168.10.1 la ip del router para g0/0, esta Ip también será la puerta de enlace con los ordenadores de la ciudad. En la ciudad B de igual manera se utiliza la Ip 192.168.20.0/24 utilizándose la 192.168.20.1/24 también para el router y como puerta de enlace. Los

ordenadores de cada ciudad están configurados de forma manual con las ips mencionadas. Por ultimo también se usa la ip 192.168.30.0/30 para conectar los routers mediante los seriales, esta tiene de máscara de red 255.255.255.252 lo que la hace perfecta para conecta únicamente dos dispositivos que vayan a relacionarse entre ellos.

La Ciudad de las Redes Aisladas

Para restaurar esta antigua metrópolis y sus gremios configuré varios dispositivos que representan las redes de esta gran ciudad. El dispositivo mas importante de la ciudad, su torre de comunicación el router que junto a un switch conectado a mas switches para otros gremios permitieron la creación de diferentes vlans representando a cada gremio.

En esta ciudad antigua había 3 gremios los recolectores, los arquitectos y los escribas.

- **Vlan 10** los recolectores: estos utilizan 2 PC y 1 laptop sus conexiones se encuentran en la ip 192.168.10.0
- **Vlan 20** los arquitectos tienen varios ordenadores conectados con ethernet y un Access point con otro par de ordenadores conectados a él. Los arquitectos utilizan la ip 192.168.20.0.
- **Vlan 30** los escribas tiene dos ordenadores un laptop y una impresora. Los escribas utilizan la ip 192.168.30.0.
- **Vlan 100 (GuardiaDHCP)** Este vlan es exclusivamente para automatizar la conexión de dispositivos en los diferentes gremios. Al conectar un dispositivo al puerto del switch que proporcione una vlan específica al dispositivo se le asignara una ip y una puerta de enlace automáticamente, esta ip será diferente según la vlan al que este conectado el dispositivo. La GuardiaDHCP tiene una ip 192.169.100.0.

