1. El Mural de las Siete Capas

Te adentras en la sala principal del templo y descubres un gran mural compuesto por siete franjas horizontales superpuestas, decoradas con símbolos y jeroglíficos. Cada franja representa un nivel diferente en un ritual de comunicación. Los sabios de esta civilización entendían que un mensaje debía pasar por varias etapas desde su origen hasta su destino, refinándose o traduciendo su forma en cada nivel de la pirámide comunicativa.

Pregunta: ¿Qué representa el mural de las siete capas en términos de las redes de comunicación modernas? Identifica brevemente cada capa y explica cómo se relaciona este antiguo "modelo" con el proceso de comunicación de datos actual.

El mural milenario representa el modelo OSI, modelo estructura en las siguientes siete capas:

1. **Capa Física**

• Transmite bits crudos (1s y 0s) a través de un medio físico (cables, fibra, ondas).

• Define aspectos eléctricos, mecánicos, ópticos y funcionales.

• Ejemplo: voltajes, conectores, tipos de cable.

2. **Capa de Enlace de Datos**

• Asegura la transmisión libre de errores entre dos nodos conectados directamente.

• Divide en tramas, controla el flujo y gestiona errores.

• Subcapas: MAC (acceso al medio) y LLC (lógica de enlace).

3. **Capa de Red**

• Determina la ruta que seguirán los paquetes desde el origen hasta el destino.

• Encargada del direccionamiento lógico (como IP) y enrutamiento.

4. **Capa de Transporte**

• Asegura la entrega completa y ordenada de los datos.

• Protocolos: **TCP** (confiable, orientado a conexión), **UDP** (rápido, sin conexión).

• Divide los datos en segmentos/datagramas.

5. **Capa de Sesión**

• Administra sesiones (conexiones) entre aplicaciones.

• Soporta control de diálogo, sincronización y recuperación.

6. **Capa de Presentación**

• Traduce los datos entre el formato de red y el que entiende la aplicación.

• Maneja cifrado, compresión y conversión de formatos.

7. **Capa de Aplicación**

• Es la más cercana al usuario. Proporciona servicios de red a las aplicaciones.

• Protocolos como HTTP, FTP, SMTP, DNS.

La relación con las comunicaciones modernas es que aunque hoy en día se utiliza más el modelo TCP/IP, el modelo OSI sigue siendo fundamental para entender y diseñar redes. Sirve como referencia para identificar fallos, desarrollar protocolos y garantizar la interoperabilidad entre distintos fabricantes y tecnologías.

2. Los Dos Pergaminos del Mensajero

En una cámara oculta encuentras dos pergaminos polvorientos. El primero describe el Ritual del Mensajero Confiable: antes de entregar un mensaje, el mensajero realiza un saludo de tres pasos con el receptor para asegurarse de que ambos estén listos, luego entrega el mensaje y espera una confirmación de recibido. Si la confirmación no llega, reintenta el envío. El segundo pergamino narra el Ritual del Mensajero Veloz: un mensajero que sale disparado a entregar mensajes sucesivos sin aviso previo ni asegurarse de la recepción, cubriendo la mayor distancia en el menor tiempo, aunque a veces los mensajes se pierdan en el camino.

Pregunta: Interpreta los dos rituales descritos. ¿A qué protocolos de comunicación actuales equivalen el mensajero confiable y el mensajero veloz? Compara sus características, explicando las ventajas y desventajas de cada enfoque en redes modernas.

Los mensajeros equivalen a los siguientes protocolos de comunicación actuales:

El Mensajero Confiable → Protocolo TCP (Transmission Control Protocol)

El Mensajero Veloz → Protocolo UDP (User Datagram Protocol)

Ambos son protocolos de la capa de transporte (modelo OSI y TCP/IP) y se encargan de permitir la comunicación entre aplicaciones que se ejecutan en diferentes dispositivos de red.

Característica	TCP (Mensajero Confiable)	UDP (Mensajero Veloz)
Tipo de conexión	Orientado a conexión (handshake previo)	No orientado a conexión
Fiabilidad	Alta: garantiza entrega y orden de los datos	Baja: no garantiza entrega ni orden
Control de errores	Sí: detección y corrección con confirmaciones	No: los errores no son gestionados
Reenvío de datos perdidos	Sí: si no se recibe ACK, se reenvía	No se realiza retransmisión
Control de flujo y congestión	Sí: adapta la velocidad al receptor	No lo implementa
Velocidad	Menor, debido a la sobrecarga de control	Mayor, al eliminar control adicional
Tamaño de cabecera	20 bytes (mínimo)	8 bytes
Uso típico	Web (HTTP/HTTPS), correo (SMTP), archivos (FTP)	Video/audio en tiempo real (VoIP, streaming), DNS, juegos online

VENTAJAS (V) /DESVENTAJAS (DV)

TCP

• (V)Muy fiable: garantiza que todos los datos lleguen y en orden.

• (V)Ideal para aplicaciones donde la precisión y completitud es esencial.

• (DV)Mayor latencia y uso de recursos.

• (DV)No apto para tiempo real o multimedia.

UDP

•(V)Muy rápido: bajo retardo, ideal para aplicaciones en tiempo real.

•(V)Menor consumo de red y procesamiento.

•(DV)No garantiza entrega ni orden de mensajes.

•(DV)Requiere que la aplicación gestione los errores, si es necesario.

PREGUNTA 3

3. El Enigma de las Subredes

Avanzando por un pasillo, encuentras una losa de piedra con inscripciones que parecen ser direcciones numéricas. Una inscripción cuenta: "Nuestro reino digital tenía la dirección sagrada 192.168.50.0. Los cuatro grandes gremios de la ciudad exigían su propio distrito en la red, todos de igual tamaño". Junto a esto, ves un diagrama borroso de algo que parecen ser subredes

emanando de la dirección principal, cada una con su propio identificador.

Pregunta: Descifra el enigma de la losa. Si la antigua red usaba la dirección 192.168.50.0 como base y necesitaba dividirse en 4 subredes de igual tamaño (una para cada gremio), ¿qué máscara de subred habrían utilizado los antiguos para lograrlo?

¿Cuántas direcciones de host (utilizables) tendría cada subred resultante? Explica brevemente tu razonamiento al calcular la máscara.

1. Clase de IP original:

La dirección 192.168.50.0 pertenece a la clase C, cuya máscara por defecto es:

255.255.255.0 → /24

2. Cálculo de bits necesarios para subredes:

Se desea dividir en 4 subredes:

2n≥4⇒n=2 bits necesarios para subred2^n \geq 4 \Rightarrow n = 2 \text{ bits necesarios para subred}2n≥4⇒n=2 bits necesarios para subred

Sumando estos 2 bits a la máscara original /24:

/24+2=/26/24 + 2 = /26/24+2=/26

Por lo tanto, la nueva máscara de subred es: 255.255.255.192 → /26

3. Cálculo de direcciones por subred:

Con una máscara /26:

2^6=64 direcciones por subred

Restamos 2 direcciones (una para la red y otra para el broadcast):

64-2=62 hosts utilizables por subred

PREGUNTA 4

Llegas a una encrucijada dentro de las ruinas: cuatro caminos diferentes se extienden hacia distintas aldeas en los alrededores de la ciudad antigua. En el centro, un totem tallado muestra flechas apuntando hacia cada camino, con inscripciones de destinos y distancias. Notas que algunas flechas parecen fijas e inmutables (talladas en la piedra), mientras que otras son piezas móviles que pudieron reorientarse si se abría o cerraba algún camino en el pasado. Este tótem se asemeja a un antiguo dispositivo de enrutamiento que dirigía el tráfico de datos por el camino adecuado.

Pregunta: ¿Qué concepto moderno de redes representa el tótem con flechas de la encrucijada? Explica qué es una tabla de enrutamiento y cómo funciona en un router actual. Además, interpreta la diferencia entre las flechas talladas en piedra y las flechas móviles en términos de enrutamiento estático vs. enrutamiento dinámico en redes.

El tótem con flechas representa a un router (encaminador) moderno, encargado de dirigir el tráfico de datos entre diferentes redes.

Tabla de enrutamiento:

La tabla de enrutamiento es una base de datos interna de los routers que indica por dónde deben enviarse los paquetes de datos para llegar a su destino. Cada entrada en la tabla indica:

- Dirección de destino (red o IP)
- Máscara de subred
- Puerta de enlace (siguiente salto)
- Interfaz de salida
- Métrica (coste o prioridad)

Los routers consultan esta tabla cada vez que reciben un paquete, seleccionando el camino más adecuado según la información almacenada.

Flechas talladas en piedra vs. flechas móviles:

- Flechas talladas en piedra simbolizan enrutamiento estático:
    - Las rutas se configuran de forma manual por el administrador.
    - No cambian automáticamente ante fallos o cambios en la red.
    - Son rígidas, estables, pero menos flexibles.
    - Útiles en redes pequeñas o simples.

- Flechas móviles simbolizan enrutamiento dinámico:
    - El router utiliza protocolos dinámicos (como RIP, OSPF o BGP) para aprender y actualizar rutas automáticamente.
    - Se adaptan ante caídas de enlaces, nuevos routers o cambios topológicos.
    - Son flexibles y eficientes en redes grandes y cambiantes.

PREGUNTA 5

5. El Guardián de la Máscara Única

En la última sala del templo, frente a la salida, te encuentras con la estatua de un guardián con dos caras. Según una leyenda grabada en la base, este guardián protegía la ciudad oculta de los forasteros. Cuando un mensajero salía de la ciudad, el guardián reemplazaba su máscara por la suya propia, de modo que, para el mundo exterior, todos los mensajes parecían venir únicamente del guardián. Al regresar la respuesta, el guardián recordaba qué máscara original correspondía a cada mensaje y reenviaba la respuesta al habitante correcto dentro de la ciudad. Gracias a este ardid, la ciudad pudo ocultar la identidad de sus miembros y usar un único rostro para todas sus comunicaciones externas.

Pregunta: ¿Qué técnica de redes moderna se refleja en la leyenda del Guardián de la Máscara? Nombra y describe brevemente este mecanismo, explicando cómo permite que múltiples dispositivos internos de una red compartan una única identidad (dirección) al comunicarse con el exterior, y menciona dos beneficios que brinda esta estrategia a las redes actuales.

La leyenda del Guardian de la máscara representa el funcionamiento de la técnica de redes conocida como NAT.

NAT es un mecanismo que permite que múltiples dispositivos dentro de una red privada utilicen una única dirección IP pública para comunicarse con el exterior. Al salir un paquete desde la red interna hacia Internet:

- El router sustituye la dirección IP privada del dispositivo por su propia IP pública (como si fuera “la máscara del guardián”).
- Cuando llega una respuesta desde el exterior, el router recuerda qué dispositivo interno originó la solicitud y redirecciona la respuesta adecuadamente.

¿Cómo funciona internamente?

- El router mantiene una tabla de traducción donde guarda temporalmente qué IP y puerto interno se corresponden con qué puerto externo.
- Esto le permite hacer coincidir cada respuesta con el dispositivo correcto, aunque externamente solo se vea una única IP.

Beneficios de NAT:

1. Ahorro de direcciones IPv4 públicas: Al usar una sola IP pública para muchos dispositivos privados, se reduce el consumo del limitado espacio de direcciones IPv4.
2. Mayor seguridad: Oculta la estructura interna de la red, dificultando accesos no autorizados desde el exterior.

Ejercicio 1: *La Ruta Perdida entre Dos Reinos*

Tras cruzar las puertas de las antiguas metrópolis digitales, me encontré con dos ciudades desconectadas entre sí, aisladas en su propio silencio tecnológico. Cada urbe, Ciudad A y Ciudad B, alguna vez fue un centro próspero de intercambio de información, pero con el paso del tiempo sus caminos de red se deterioraron y su comunicación cesó por completo.

Mi misión fue restaurar la conectividad entre ambas ciudades usando los recursos disponibles.

CIUDAD A

Mi viaje comenzó en las ruinas de Ciudad A, donde los ecos de una red silenciosa aún vibraban entre routers apagados y switches oxidados. Esta fue la primera ciudad en la que reconstruí el tejido de comunicación perdido, pieza a pieza, interfaz a interfaz.

Subred: 192.168.10.0/24
Elementos:

Router3

- Modelo: Cisco 1941

- Función**:** actúa como la puerta de enlace principal de la Ciudad A.
- Interconexión**:**
    - Conectado al switch de la ciudad por la interfaz GigabitEthernet0/0.
    - Enruta tráfico hacia otras redes (como la Ciudad B, a través de su interfaz serial).
    - Sirve de gateway predeterminado para todos los dispositivos locales.

Switch (2960)

- Función: distribuye la conectividad local entre los dispositivos cableados y el punto de acceso inalámbrico.
- Interconexión**:**
    - Recibe conexión desde Router3.
    - Está conectado a los PCs (PC0 y PC1).
    - También conecta el Access Point, que a su vez da servicio al smartphone.
    - Es un switch plano, sin VLANs ni segmentación especial.

PC0 y PC1

- Función**:** PCs con los que las dos ciudades se comunican
- Configuración IP:
    - PC0: IP 192.168.10.2 – Gateway 192.168.10.1
    - PC1: IP 192.168.10.3 – Gateway 192.168.10.1
- Interconexión**:** conectados al switch por FastEthernet.

Access Point0

- Instalado para permitir conectividad Wi-Fi dentro de la ciudad.
- Conectado al Switch0 con cable.
- SSID configurado como CiudadA y cuenta con contraseña para que solamente se pueda conectar el dispositivo que introduzca la contraseña y así se evita que dispositivos de la CiudadB se conecten a Access Point de la CiudadA

- Permite a los dispositivos inalámbricos operar dentro de la misma subred que los PCs cableados.

Smartphone2

- **Función:** dispositivo móvil de la ciudad, con el que las dos ciudades también se pueden comunicar.
- **Configuración IP estática:**
    - IP: 192.168.10.5
    - Gateway: 192.168.10.1
- **Conectividad:**
    - Se conecta al Access Point0.
    - Opera en la misma subred que el resto de los dispositivos cableados.

CIUDAD B

Tras cruzar la Zona Desierta, alcancé la legendaria Ciudad B, una urbe brillante, conectada internamente por estructuras sólidas y bien organizadas. Para restaurar su red, repliqué la lógica de la Ciudad A, pero con algunas particularidades que hicieron del desafío una experiencia única.

Router6

- Modelo: Cisco 1941
- Función: actúa como puerta de enlace principal en Ciudad B y entre Ciudad B y Ciudad A.
- Configuración:
    - Se asignó la IP 192.168.20.1/24 a la interfaz GigabitEthernet0/0.
    - Este router no tenía interfaces seriales por defecto, así que tuve que acceder a la vista física del dispositivo y añadir manualmente un módulo serial (WIC-2T), para poder crear la interconexión con Router3 en Ciudad A.
    - Se conectó a Router3 mediante el puerto Serial0/1/0.

Switch1 (2960)

- Función: conecta todos los dispositivos cableados de la ciudad.
- Conexiones:
    - Hacia Router6 (GigaEthernet)
    - Hacia los PCs PC2 y PC3 (FastEthernet)
    - Hacia el punto de acceso inalámbrico (Access Point) (Fa0/4)
- Modo de operación: sin VLANs, trabajando como un switch plano en la red 192.168.20.0/24.

Terminales cableados – PC2 y PC3

- PC2: IP 192.168.20.2 – Gateway 192.168.20.1
- PC3: IP 192.168.20.3 – Gateway 192.168.20.1
- Conectados al switch y plenamente funcionales con el resto de la ciudad.

Access Point1 – El Faro Inalámbrico

- Conectado al Switch1 por cable.
- SSID configurado (CiudadB) con contraseña para que así solamente pueda conectarse de forma inalámbrica el dispositivo que introduzca la contraseña.
- Permite que cualquier dispositivo móvil se conecte fácilmente.

Smartphone3

- Lo conecté al Access Point1 de forma inalámbrica.
- IP asignada estáticamente: 192.168.20.5
- Gateway: 192.168.20.1
- Puede comunicarse con los PCs de su ciudad y, tras configurar el enrutamiento, también con Ciudad A.

Interconexión entre ciudades

Para unir Ciudad A con la Ciudad B he tenido que hacer lo siguiente en la Zona Desierta:

- En Router6, se añadió el puerto Serial0/1/0 y se configuró con IP 192.168.30.2/30.
- Para conectarlos usé un cable serial a Router3 en Ciudad A (Serial0/1/0 también), usando un cable DCE/DTE para habilitar la comunicación punto a punto.

Una vez que configuré todos los elementos de cada una de las ciudades pude asegurar la conectividad de cada uno de los dispositivos, permitiendo la comunicación exitosa entre las dos ciudades.

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	Smart...	Smartphone2	ICMP		0.000	N	3	(edit)	
	Successful	PC1	Smartphone3	ICMP		0.000	N	4	(edit)	
	Successful	PC3	Smartphone3	ICMP		0.000	N	5	(edit)	
	Successful	PC0	Smartphone2	ICMP		0.000	N	6	(edit)	

Ejercicio 2: *La Ciudad de las Redes Aisladas*

Al llegar a la antigua metrópolis, descubrí que no era una ciudad común, sino una red dividida en gremios, cada uno operando en su propio canal sagrado de comunicación. Aunque todos compartían la misma infraestructura física, sus mensajes viajaban por caminos invisibles: VLANs.

Gremio	**VLAN**	**Subred**
Arquitectos	10	192.168.10.0/24
Escribas	20	192.168.20.0/24
Alquimistas	30	192.168.30.0/24
Servidor	99	192.168.99.0/24

1.Gremio de los Arquitectos (VLAN 10 – 192.168.10.0/24)

Tras restaurar los caminos troncales de la metrópolis, me dirigí al primer gremio ancestral: el de los Arquitectos. Conocidos por su disciplina y precisión, sus terminales estaban cableados con orden, y su infraestructura era un ejemplo de claridad digital.

Switch0 (2960)

- Función: distribuye el tráfico entre los dispositivos del gremio y permite su conexión hacia la Torre Central (router).
- Conexiones del gremio:
    - Fa0/1, Fa0/2, Fa0/3 → PCs principales
    - Fa0/11 y Fa0/12 → PCs secundarios y prueba de DHCP (PC11)
    - Fa0/19 → Access Point1 inalámbrico

Terminales cableados

- PC0: IP estática 192.168.10.11, Gateway 192.168.10.1
- PC1: IP estática 192.168.10.12, Gateway 192.168.10.1

- PC2: IP estática 192.168.10.13, Gateway 192.168.10.1
- PC11: Dirección IP obtenida por DHCP desde el servidor central(192.168.10.10)
- Todos conectados al switch y operando bajo la VLAN 10.

Access Point1

- Conectado a: Fa0/19 del Switch0
- SSID configurado: "Arquitectos" con contraseña para que se conecten solamente los dispositivos que introduzca dicha contraseña y eviten conectarse todos los dispositivos de distintos gremios al mismo AP.
- Función**:** canal inalámbrico exclusivo del gremio

Dispositivos inalámbricos

- Smartphone0: conectado al AP con IP por DHCP, gateway 192.168.10.1
- Laptop2 y Laptop3: conectados al SSID del gremio y funcionando con DHCP

2.Gremio de los Escribas (VLAN 20 – 192.168.20.0/24)

El segundo gremio al que devolví la voz fue el de los Escribas, guardianes del conocimiento y la organización. Su red se estructuraba con lógica impecable y reverencia por el orden.

Switch0

- Conexiones del gremio:
    - Fa0/4, Fa0/5, Fa0/6 → PCs principales
    - Fa0/13 → PC12 (cliente DHCP)
    - Fa0/22 → Access Point2

Terminales cableados

- PC3: IP estática 192.168.20.11, Gateway 192.168.20.1
- PC4: IP estática 192.168.20.12, Gateway 192.168.20.1
- PC5: IP estática 192.168.20.13, Gateway 192.168.20.1
- PC12**:** IP asignada automáticamente por el servidor DHCP (192.168.20.10)

- Todos conectados a la VLAN 20

Access Point2

- Conectado a: Fa0/20 del Switch0
- SSID configurado: “Escribas” con contraseña para que se conecten solamente los dispositivos que introduzca dicha contraseña y eviten conectarse todos los dispositivos de distintos gremios al mismo AP.
- Función: acceso inalámbrico al gremio

Dispositivos inalámbricos

- Smartphone2: IP dinámica vía DHCP, gateway 192.168.20.1
- Laptop0 y Laptop1: conectados al AP y operando con DHCP correctamente

3.Gremio de los Alquimistas (VLAN 30 – 192.168.30.0/24)

El último gremio que reactivé fue el de los Alquimistas (lo he añadido, para que el ejercicio fuese más completo), maestros de la transformación digital.

Switch0

- Conexiones del gremio:
    - Fa0/7, Fa0/8, Fa0/9 → PCs principales
    - Fa0/14 → PC13 (cliente DHCP)
    - Fa0/23 → Access Point0

Terminales cableados

- PC6: IP estática 192.168.30.11, Gateway 192.168.30.1
- PC7: IP estática 192.168.30.12, Gateway 192.168.30.1
- PC8: IP estática 192.168.30.13, Gateway 192.168.30.1
- PC13: configurado para obtener IP por DHCP (192.168.30.16)
- Todos conectados a la VLAN 30

Access Point0

- Conectado a: Fa0/22 del Switch0
- SSID configurado: "Alquimistas" con contraseña para que se conecten solamente los dispositivos que introduzca dicha contraseña y eviten conectarse todos los dispositivos de distintos gremios al mismo AP.

- Función: acceso inalámbrico exclusivo para el gremio

Dispositivos inalámbricos

- Smartphone1: IP por DHCP, Gateway 192.168.30.1
- Laptop4 y Laptop5: conectados al AP, reciben IP automáticamente usando DHCP

Configuración técnica

Switch Central – VLANs

Creo y nombro cada VLAN

```
vlan 10
 name Arquitectos
vlan 20
 name Escribas
vlan 30
 name Alquimistas
vlan 99
 name Servidor
```

Luego asigné los puertos correspondientes del switch a cada VLAN, así están vinculados al canal adecuado (en esta imagen se ve la línea de código que uso para la vlan10, así igual para las otras dos)

```
interface range fa0/1 - 3
 switchport mode access
 switchport access vlan 10

interface range fa0/11 - 12
 switchport mode access
 switchport access vlan 10

interface fa0/19
 switchport mode access
 switchport access vlan 10
```

VLAN	Puertos del switch
10	Fa0/1, Fa0/2, Fa0/3, Fa0/11, Fa0/12, Fa0/19 (AP)
20	Fa0/4, Fa0/5, Fa0/6, Fa0/13, Fa0/20 (AP)
30	Fa0/7, Fa0/8, Fa0/9, Fa0/10, Fa0/22, Fa0/23 (AP)
99	Fa0/21 (Servidor)

2.Puerto Trunk

Finalmente, configuré el puerto de enlace troncal (trunk), que conecta el switch al router central. Este enlace permite que el tráfico etiquetado de todas las VLANs viaje por una única interfaz física hacia las subinterfaces del router:

```
interface fa0/24
 switchport mode trunk
```

Para las subinterfaces en el Router central he hecho lo siguiente:

```
interface FastEthernet0/0.10
 encapsulation dot1Q 10
 ip address 192.168.10.1 255.255.255.0
 ip helper-address 192.168.99.2

interface FastEthernet0/0.20
 encapsulation dot1Q 20
 ip address 192.168.20.1 255.255.255.0
 ip helper-address 192.168.99.2

interface FastEthernet0/0.30
 encapsulation dot1Q 30
 ip address 192.168.30.1 255.255.255.0
 ip helper-address 192.168.99.2

interface FastEthernet0/0.99
 encapsulation dot1Q 99
 ip address 192.168.99.1 255.255.255.0
```

-Interface FastEthernet0/0.10→ lo que estoy haciendo es crear una subinterfaz lógica del router asociada a la VLAN 10, tratando únicamente el trafico etiquetado de esta.

-Encapsultaion dot1Q 10→ de esta forma activo el protocolo de encapsulación de VLAN, llamado 802.1Q.El numero 10 indica que solo trata tramas con etiqueta de VLAN 10

-Ip adress 192.168.10.1 255.255.255.0→ le estoy asignado a esta subinterfaz la IP que se va a usar como Gateway por los dispositivos de la VLAN10

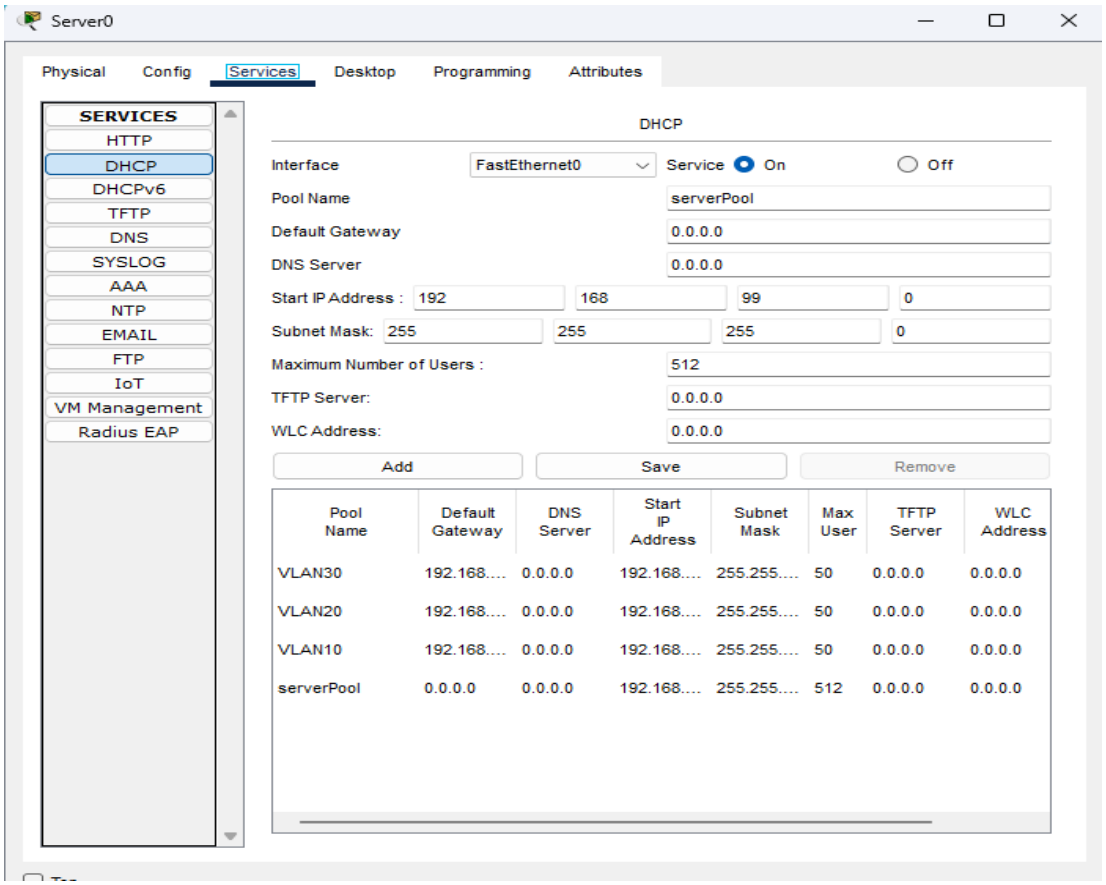
-Ip helper-adress 192.168.99.2→ este comando es obligatorio, porque lo he usado para indicarle al router que tiene que redirigir las solicitudes DHCP que lleguen desde la VLAN 10 hacia el servidor DHCP que esta en la Ip 192.168.99.2

De esta forma los dispositivos con los que he probado esta forma, se les asigna de forma dinámica direcciones IP mediante DHCP centralizado.

SERVIDOR

Para que funcione el DHCp he tenido que habilitar primer el servicio (Service→ON) para responder a las solicitudes de IP y he definido tres pools(un pool es como una caja llena de IPs que el servidor puede repartir) para cada VLAN.El servidor no puede recibir directamente los broadcasts DHCP de otras VLANs, por eso he usado subinterfaces en el router 'ip helper-address'

Cuando un PC o smartphone en VLAN10, 20 o 30 quiere una IP, envía un mensaje DHCP Discover. El router recibe ese broadcast, lo convierte en un mensaje unicast y lo reenvía a la IP del servidor (192.168.99.2). El servidor le responde con una IP del pool correspondiente según el gateway desde el que provino.



Después de haber terminado la configuración de cada uno de los gremios, del router, del servidor, y de todos los dispositivos, he conseguido unir los tres gremios que antes estaban aislados usando VLANs, manteniendo cada uno de ellos su independencia, pero ahora se pueden comunicar entre ellos, funcionando la red con eficiencia y seguridad.

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	Laptop1	PC3	ICMP		0.000	N	0	(edit)	
	Successful	Smart...	Smartphone0	ICMP		0.000	N	1	(edit)	
	Successful	Laptop1	Laptop5	ICMP		0.000	N	2	(edit)	
	Successful	Laptop2	Laptop5	ICMP		0.000	N	3	(edit)	