



Tecnicatura Desarrollo de software  
Programación sobre Redes  
Prof. Lucas Rusatti

# Trabajo Práctico Teórico

**Integrantes:**

Leonardo Bujan  
Martin Esperon  
Maryangelin Quintero

### ¿Qué es una VLAN (Virtual Local Area Network)?

Es una red lógica que agrupa un conjunto de dispositivos en diferentes redes físicas en una sola red lógica, lo que permite que estos dispositivos se comuniquen entre sí como si estuvieran en la misma red física, independientemente de su ubicación física.

### ¿Qué es una VPN (Virtual Private Network, o Red Privada Virtual)?

Es una tecnología que permite crear una conexión segura y privada entre dos o más dispositivos a través de una red pública, como Internet. La VPN cifra el tráfico de datos, lo que protege la información y garantiza la privacidad de las comunicaciones.

### ¿Qué es una SAN (Storage Area Network, o Red de Área de Almacenamiento) ?

Es una red especializada de alta velocidad que conecta servidores y dispositivos de almacenamiento, permitiendo que múltiples servidores accedan a un almacenamiento centralizado como si fuera un disco duro local.

### Diferencias entre un Hub, Repetidor, Router y SWITCH. Explicar las diferencias.

|                | <b>Hub</b>  | <b>Repetidor</b>  | <b>Router</b>   | <b>SWITCH</b>   |
|----------------|---|---|---|---|
| <b>Funcion</b> | Conecta múltiples dispositivos en una red local y retransmite el tráfico de red que recibe a todos los dispositivos conectados. | Amplifica o regenera la señal de red para extender la cobertura física de la red. | Conecta diferentes redes entre sí (por ejemplo, una red local a Internet) y dirige el tráfico de red entre ellas. | Conecta múltiples dispositivos en una red local (LAN) y envía los paquetes de datos solo al dispositivo específico al que están destinados. |

| capa OSI               | Capa 1 (Física)   | Capa 1 (Física)   | Capa 3 (Red)  | Capa 2 (Enlace de Datos)   |
|------------------------|---|---|---|--|
| <b>Características</b> | <ul style="list-style-type: none"> <li>- Retransmite los datos a todos los puertos.</li> <li>- No inteligente, no filtra tráfico.</li> <li>- Ancho de banda compartido, puede causar colisiones.</li> </ul> | <ul style="list-style-type: none"> <li>- Regenera señales para extender la cobertura.</li> <li>- No filtra ni dirige tráfico, simplemente amplifica.</li> </ul> | <ul style="list-style-type: none"> <li>- Determina la mejor ruta para los datos usando direcciones IP.</li> <li>- Conecta redes distintas, como una LAN con Internet.</li> <li>- Incluye funciones de seguridad como NAT y firewall.</li> </ul> | <ul style="list-style-type: none"> <li>- Envía datos solo al dispositivo destinatario.</li> <li>- Filtra tráfico utilizando direcciones MAC.</li> <li>- Mejora la eficiencia y reduce colisiones.</li> </ul> |

## ¿Qué es un protocolo de comunicaciones?

Es un conjunto de reglas y estándares que permiten que dos o más dispositivos intercambien información de manera efectiva y coherente en una red. Estos protocolos definen cómo se envían, reciben y procesan los datos, asegurando que los dispositivos, aunque sean de diferentes fabricantes o utilicen tecnologías distintas, puedan comunicarse entre sí.

## Explique TCP/IP y NetBios, resuma sus diferencias. (Acá sí explicar cada uno y sus diferencias)

- **TCP/IP (Transmission Control Protocol/Internet Protocol):** es el conjunto de protocolos de comunicación más ampliamente utilizado en redes, incluyendo Internet. Define cómo los dispositivos se comunican en una red y cómo se transmiten los datos de manera confiable.
  - alcance Global, usado en todas las redes modernas.
  - trabaja sobre las capas OSI: TCP en Capa 4 (Transporte), IP en Capa 3 (Red).
- **NetBIOS (Network Basic Input/Output System)** es un protocolo de red desarrollado por IBM que permite que las aplicaciones en diferentes computadoras

dentro de una red local (LAN) se comuniquen entre sí. Es más común en redes Windows y fue ampliamente utilizado en redes de área local antiguas.

- Alcance Local, principalmente en redes Windows antiguas.
- Trabaja sobre la capa OSI: Capa 5 (Sesión).

## ¿Cómo está formado un paquete de datos en TCP/IP? ¿Qué es un “flag” en un paquete de TCP/IP?

### Estructura de un Paquete TCP/IP

1. **Capa de Aplicación:** Contiene los datos de la aplicación (por ejemplo, datos HTTP, FTP, etc.).
2. **Capa de Transporte:**
  - **TCP:** Se encapsula en segmentos. Cada segmento incluye un encabezado TCP que contiene:
    - **Puerto de origen:** Identifica la aplicación que envía.
    - **Puerto de destino:** Identifica la aplicación que recibe.
    - **Número de secuencia:** Controla el orden de los segmentos.
    - **Número de acuse de recibo:** Indica el próximo número de secuencia esperado.
    - **Flags (banderas):** Controlan aspectos del manejo de la conexión, como el inicio y el cierre de conexiones.
    - **Tamaño de la ventana:** Controla el flujo de datos.
    - **Verificación de suma:** Controla la integridad de los datos.
  - **UDP:** Incluye un encabezado más simple que también contiene puertos de origen y destino, longitud y verificación de suma.
3. **Capa de Internet:**
  - **IP:** Cada paquete IP incluye un encabezado que contiene:
    - **Dirección IP de origen:** La dirección del remitente.

- **Dirección IP de destino:** La dirección del destinatario.
  - **Tiempo de vida (TTL):** Limita el tiempo que un paquete puede permanecer en la red.
  - **Protocolo:** Indica el protocolo de la capa superior (TCP o UDP).
4. **Capa de Acceso a la Red:** Se encarga de la transmisión física de los datos. Aquí se añaden encabezados y pies de página específicos de la tecnología de red (como Ethernet).

### “flag” en un paquete de TCP/IP

Un "flag" en un paquete TCP/IP, específicamente en el encabezado TCP, es un bit de control que indica el estado o el comportamiento del segmento TCP. Algunos de los flags más comunes son:

- **SYN:** Inicia una conexión (Synchronize).
- **ACK:** Confirma la recepción de datos (Acknowledgment).
- **FIN:** Indica que un extremo quiere terminar la conexión (Finish).
- **RST:** Reinicia la conexión (Reset).
- **PSH:** Indica que los datos deben ser entregados inmediatamente a la aplicación (Push).
- **URG:** Indica que hay datos urgentes en el segmento (Urgent).

Estos flags son esenciales para el control de la conexión y para garantizar la entrega ordenada y confiable de los datos en una red.

## Defina la red según su geografía. Explicar distintas variantes

Las redes pueden clasificarse según su alcance geográfico en varias categorías. Aquí están las principales variantes:

- LAN (Local Area Network):

Red que cubre un área geográfica limitada, como una oficina, un edificio o un campus tiene alta velocidad de transmisión, generalmente utiliza tecnología Ethernet o Wi-Fi, y permite la conexión de dispositivos dentro de un área pequeña.

*Ejemplo:* La red de una empresa que conecta las computadoras y dispositivos de oficina en un edificio.

- WAN (Wide Area Network):

Red que abarca un área geográfica extensa, que puede incluir ciudades, países o incluso continentes tiene Menor velocidad de transmisión comparada con LAN, utiliza tecnologías como líneas telefónicas, satélites o enlaces de fibra óptica para conectar redes LAN distantes.

*Ejemplo:* La red global de Internet o una red corporativa que conecta sucursales en diferentes ciudades.

- MAN (Metropolitan Area Network):

Red que cubre un área geográfica intermedia, como una ciudad o una gran área metropolitana es Más extensa que una LAN pero menos que una WAN, proporciona alta velocidad de transmisión y puede interconectar múltiples redes LAN en una región metropolitana.

*Ejemplo:* La red de una ciudad que conecta diferentes edificios gubernamentales y empresas.

- PAN (Personal Area Network):

Red que cubre un área muy pequeña, generalmente el alcance de una persona o un pequeño espacio, como una habitación. Utiliza tecnologías como Bluetooth o Wi-Fi para conectar dispositivos personales, como teléfonos, computadoras y periféricos.

*Ejemplo:* La red que conecta un teléfono móvil con una computadora y un auricular Bluetooth.

- CAN (Campus Area Network):

Red que cubre un área más amplia que una LAN pero más pequeña que una MAN, como un campus universitario o una gran empresa. Permite la interconexión de

varios edificios dentro de un campus, proporcionando alta velocidad y un control centralizado sobre la infraestructura de red.

*Ejemplo:* La red de una universidad que conecta varios edificios académicos y administrativos.

- WAN (Wireless Area Network):

Aunque menos común, se refiere a redes inalámbricas que pueden extenderse por áreas amplias, utilizando tecnologías como Wi-Fi, LTE o 5G. Permite la conectividad en áreas grandes sin la necesidad de cables físicos, con velocidades variables según la tecnología utilizada.

*Ejemplo:* Una red Wi-Fi pública en una ciudad o una red de sensores inalámbricos en una región agrícola.

Cada tipo de red tiene sus propias características y está diseñada para satisfacer diferentes necesidades según el alcance geográfico y los requisitos de conectividad.

## **Defina una red según su topología. Explicar distintas variantes**

La topología de red es un concepto que hace referencia a la forma en la que está dispuesta una red, incluyendo sus nodos –puntos de intersección, conexión o enlace de varios elementos– y las líneas utilizadas para asegurar la transmisión y recepción de datos de manera correcta y segura. Dependiendo de este arreglo, se pueden evitar cortes innecesarios o incrementar el flujo de la información transmitida.

Esencialmente, una topología de red se divide en dos niveles:

1. Topología de red física: Identifica cómo se conectan los terminales y dispositivos de forma física, utilizando cables y antenas. Los diversos conectores simbolizan los cables de red físicos, mientras que los nodos representan los dispositivos de red físicos, como los conmutadores (switches).

2. Topología de red lógica: Considera la manera en la que una red transfiere tramas de un nodo al siguiente. También toma en cuenta las subredes que existen y cómo estas se interconectan.

Tipos de topologías de red y sus características:

- Topología de Bus: en esta red informática todos los dispositivos se conectan directamente a un canal y no existe otro vínculo entre nodos. Entre sus ventajas están la fácil instalación, tener poco cableado y que es muy sencillo aumentar o disminuir el número de aparatos que se adjuntan a la red. Sin embargo, este sistema también trae aparejado ciertos inconvenientes, como problemas de congestión, colisión y bloqueo. Además, si existe un problema en el canal, todos los dispositivos quedarán desconectados.
- Topología de Anillo: se trata de una red cerrada formada por distintos componentes que forman una estructura anular. Cada nodo está vinculado solamente con los dos contiguos, por lo que para que la información pueda circular, cada estación debe transmitirla a la que tiene junto hasta que llegue a la receptora. Lo anterior significa que, cuando llega un mensaje a un dispositivo, este comprueba los datos de envío y si no es el receptor, lo pasa al siguiente, y así sucesivamente hasta que lo recibe el destinatario. Es decir, la información pasa por todos los nodos para poder llegar a su destino final.  
  
Lo destacable de esta topología es que es de fácil instalación, ofrece mejor rendimiento que la de bus y, cuando se presenta una falla, es fácil localizarla. La desventaja es que, al usar esta configuración, los nodos no pueden enviar mensajes al mismo tiempo y, si alguno de los dispositivos se desconecta, no servirá la conexión entre ninguno.
- Topología de Anillo Doble: funciona de igual manera que la red anterior pero existe una segunda estructura redundante que conecta a los nodos. Esto aporta más velocidad entre las terminales lejanas y una mayor confiabilidad ya que se pueden evitar fallos en la conexión.



- Topología de Estrella: todos los dispositivos se conectan a un punto central, ya sea, un concentrador, conmutador o servidor. Este punto funciona como un servidor, controlando y gestionando todas las funciones de la red. Lo bueno de este tipo de topología es que permite que todas las estaciones se comuniquen entre sí, pero las colisiones pueden representar un problema. Además, si el nodo central presenta alguna anomalía, toda la red queda expuesta a la misma e inclusive puede provocar una desconexión.
- Topología de Estrella Extendida: esencialmente, funciona igual que la configuración previa, pero cada elemento conectado al nodo central se convierte a su vez en el centro de otra estrella. Esto hace que el cableado sea más corto, pero también restringe la cantidad de dispositivos que se pueden asociar.
- Topología de Árbol: mezcla la topología de bus y de estrella y permite a los usuarios tener varios servidores. Esta red cuenta con un punto de enlace troncal desde el que se ramifican los demás nodos.

Existen además dos subclases:

- Árbol binario: cada nodo se fragmenta en dos enlaces.
- Árbol backbone: un tronco tiene un cable principal, denominado precisamente backbone, que lleva información a todos los nodos ramificados.

Uno de los principales atributos de esta configuración es que, si falla un dispositivo, no se presentan problemas entre los subsiguientes, reduce el tráfico de red y es compatible con muchos proveedores de hardware y de software. No obstante, es mejor aplicarla cuando se instala una red de gran tamaño. Si se hace con una pequeña, hay que utilizar muchos más cables que con otras topologías, por lo que se genera mucho desperdicio.

- Topología de Malla: en esta clase de red informática todos los componentes se enlazan directamente con todos mediante vías separadas. De esta forma, se ofrecen caminos repetitivos para que, si una conexión falla, la información fluya por varias rutas alternativas. Derivado de ello, proporciona una redundancia y una fiabilidad óptimas. Esta estrategia solamente funciona si hay una limitada cantidad de dispositivos que unir, ya que, con muchas terminales el número de conexiones se vuelve abrumador.
- Topología Híbrida: mezcla dos o más topologías de red diferentes para adaptar su estructura a las necesidades físicas del lugar en el que se realiza la instalación, así como a los requerimientos de seguridad, velocidad e interconexión.

## **Explicar el servicio de DHCP**

DHCP (Dynamic Host Configuration Protocol) es un protocolo de red que permite a los dispositivos obtener automáticamente una dirección IP y otros parámetros de configuración necesarios para conectarse a una red.

### **Funcionamiento:**

**Solicitud de IP:** Cuando un dispositivo (como una computadora o un teléfono) se conecta a una red, envía un mensaje de solicitud DHCP (DHCP Discover) a la red, buscando un servidor DHCP.

**Oferta de IP:** El servidor DHCP responde con un mensaje de oferta DHCP (DHCP Offer), que incluye una dirección IP disponible y otra información de configuración, como la máscara de subred, la puerta de enlace predeterminada y los servidores DNS.

**Petición de IP:** El dispositivo responde con una solicitud DHCP (DHCP Request), indicando que acepta la oferta del servidor DHCP y quiere usar la dirección IP ofrecida.

Confirmación: El servidor DHCP envía una confirmación DHCP (DHCP Acknowledgment), confirmando que la dirección IP y la configuración han sido asignadas al dispositivo.

Renovación: Las direcciones IP asignadas por DHCP tienen un tiempo de arrendamiento. Cuando el tiempo está por expirar, el dispositivo debe solicitar una renovación para seguir usando la misma dirección IP o puede obtener una nueva si es necesario.

## Explicar el servicio DNS

Miles de servidores, instalados en diversas ubicaciones, prestan los servicios que utilizamos a diario por Internet. A cada uno de estos servidores se le asigna una dirección IP única que lo identifica en la red local en la que está conectado.

Sería imposible recordar todas las direcciones IP de todos los servidores que prestan servicios de hospedaje por Internet. Por eso, existe una manera más sencilla de ubicar servidores mediante la asociación de un nombre con una dirección IP.

El sistema de nombres de dominios (**DNS, Domain Name System**) proporciona un método para que los hosts utilicen este nombre al solicitar una dirección IP de un servidor específico. Los nombres del DNS están registrados y organizados en Internet en grupos específicos de alto nivel, o dominios. Algunos de los dominios de alto nivel más comunes en Internet son: .com, .edu y .net.

Un servidor DNS contiene una tabla que asocia los nombres de hosts de un dominio con las direcciones IP correspondientes. Cuando un cliente tiene el nombre de un servidor, como un servidor Web, pero necesita encontrar la dirección IP, envía una solicitud al servidor DNS en el puerto 53. El cliente utiliza la dirección IP del servidor DNS configurada en los parámetros DNS de la configuración IP del host.

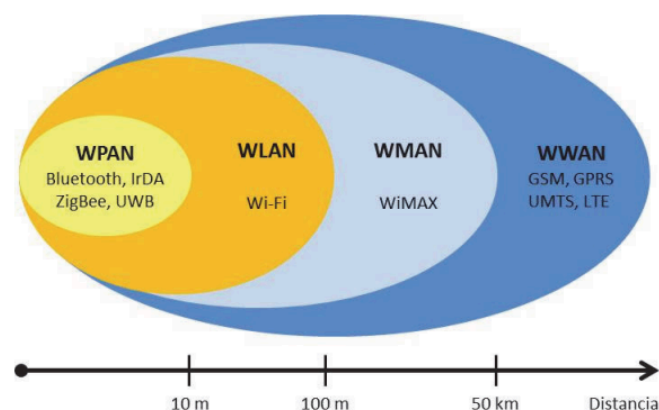
Cuando el servidor DNS recibe la solicitud, verifica la tabla para determinar la dirección IP asociada con ese servidor Web. Si el servidor DNS local no tiene una entrada para el nombre solicitado, realiza una consulta a otro servidor DNS dentro del dominio. Cuando el servidor DNS encuentra la dirección IP, esa información se envía nuevamente al cliente. Si el servidor DNS no puede determinar la dirección IP, se agotará el tiempo de espera de la respuesta y el cliente no podrá comunicarse con el servidor Web.

El software cliente trabaja con el protocolo DNS para obtener direcciones IP de un modo que resulte transparente para el usuario.

## Explicar las tecnologías Wireless y sus estándares

Las **redes inalámbricas** son redes que utilizan ondas de radio para conectar los dispositivos, sin la necesidad de utilizar cables de ningún tipo.

Las redes inalámbricas se pueden clasificar en cuatro grupos específicos según el área de aplicación y el alcance de la señal [1-3]: redes inalámbricas de área personal (Wireless Personal-Area Networks - WPAN), redes inalámbricas de área local (Wireless Local-Area Networks - WLAN), redes inalámbricas de área metropolitana (Wireless Metropolitan-Area Networks - WMAN), y redes inalámbricas de área amplia (Wireless Wide-Area Networks - WWAN).



## Redes inalámbricas de área personal (WPAN)

Las redes inalámbricas de área personal se basan en el estándar IEEE 802.15. Las redes inalámbricas permiten la comunicación en un rango de distancias muy corto, unos 10 metros.

Este tipo de redes se caracterizan por su bajo consumo de energía y también una baja velocidad de transmisión. Se basan en tecnologías como **Bluetooth**, **IrDA**, **ZigBee** o **UWB**. Desde un punto de vista de aplicación, **Bluetooth** está destinado a un ratón, un teclado, un manos libres; **IrDA** está pensado para enlaces punto a punto entre dos dispositivos para la transferencia de datos simples y sincronización de archivos; **ZigBee** está diseñado para redes inalámbricas fiables para el seguimiento y control de procesos, mientras que **UWB** está orientado a enlaces multimedia de gran ancho de banda.

### Bluetooth

Pertenece al estándar IEEE 802.15.1. Originalmente fue diseñado para comunicaciones omnidireccionales (punto a multipunto), de bajo consumo de energía, corto alcance y con dispositivos baratos, reemplazando el uso de cables y conectando los dispositivos a través de una conexión ad hoc por radio. Hoy en día los desarrolladores están diseñando componentes y sistemas habilitados para Bluetooth para una gama de aplicaciones adicionales. Los dispositivos que incorporan esta tecnología se clasifican en tres grupos diferentes según su alcance máximo: Clase 1, Clase 2 y Clase 3, donde el rango es de unos 100 metros, 10 metros y 1 metro, respectivamente. El uso de la banda de 2,4 GHz, permite que dos dispositivos dentro del rango de cobertura de cada uno puedan compartir hasta 720 Kbps de velocidad de transferencia. La clase 2 es la más utilizada.

### IrDA

La Asociación de Datos por Infrarrojos (Infrared Data Association - IrDA) especifica un conjunto completo de estándares para comunicaciones por infrarrojos. IrDA se refiere a ese conjunto de normas y se utiliza para proporcionar conectividad inalámbrica a los dispositivos que normalmente utilizan cables para la conectividad. IrDA es un estándar de transmisión de datos ad-hoc de bajo consumo de energía, bajo coste, unidireccional (punto a punto),

cono de ángulo estrecho ( $<30^\circ$ ), diseñado para operar con distancias de hasta 1 metro y a velocidades de 9600 bps a 4 Mbps (actualmente), 16 Mbps (en desarrollo). Algunos de los dispositivos que utilizan IrDA son portátiles, PDAs, impresoras y cámaras.

### **ZigBee**

Está basado en el estándar IEEE 802.15.4 que fue desarrollado como un estándar global abierto para abordar las necesidades de fácil aplicación, alta fiabilidad, bajo costo, bajo consumo y bajas velocidades de transmisión de datos en redes de dispositivos inalámbricos. ZigBee opera en las bandas sin licencia 2.4 GHz, 900 MHz y 868 MHz con una velocidad de transmisión máxima de 250 Kbps, lo suficiente para satisfacer las necesidades de un sensor y de automatización usando redes inalámbricas. ZigBee también sirve para la creación de redes inalámbricas más grandes que no exijan una gran cantidad de transmisión de datos. En una red ZigBee pueden participar dos tipos diferentes de dispositivos: dispositivos de funcionalidad completa (Full Function Device - FFD) y dispositivos de funcionalidad reducida (Reduced Function Device - RFD). Los FFDs pueden operar en tres modos distintos, como coordinador de la WPAN, coordinador o dispositivo. El RFD se diseñó sólo para aplicaciones muy simples, como la de un interruptor de luz. ZigBee soporta tres topologías de red diferentes: estrella, malla, y árbol.

### **UWB**

Basado en el estándar IEEE 802.15.3, la tecnología UWB ha atraído recientemente mucha atención como una red inalámbrica para comunicaciones de alta velocidad y corto alcance en interiores. UWB sirve a un propósito muy diferente que las otras tecnologías ya mencionadas en este apartado. UWB permite la transmisión de grandes archivos de datos a altas velocidades en distancias cortas. La tecnología 12 UWB ofrece una velocidad de transmisión de datos de más de 110 Mbps hasta 480 Mbps a distancias de hasta unos pocos metros capaz de satisfacer a la mayoría de las aplicaciones multimedia como pueda ser el audio y video en las redes del hogar, y también puede actuar como un sustituto inalámbrico del cable de buses serie de alta velocidad tales como el USB 2.0 y IEEE 1394. Las comunicaciones UWB transmiten información mediante la emisión de pulsos de muy corta duración y de gran ancho de banda, lo que permite utilizar modulación por posición o tiempo de pulso.

## **Redes inalámbricas de área local (WLAN)**

Las redes inalámbricas de área local (WLAN) están diseñadas para proporcionar acceso inalámbrico en zonas con un rango típico de hasta 100 metros y se utilizan sobre todo en el hogar, la escuela, una sala de ordenadores, o entornos de oficina. Esto proporciona a los usuarios la capacidad de moverse dentro de un área de cobertura local y permanecer conectado a la red. Las WLAN se basan en el estándar 802.11 del IEEE y son comercializadas bajo la marca Wi-Fi. Debido a la competencia, otros estándares como HIPERLAN nunca recibieron tanta aplicación comercial. El estándar IEEE 802.11 fue más sencillo de implementar y se hizo más rápido con el mercado; comprende toda una familia de diferentes estándares para redes inalámbricas de área local. El IEEE 802.11b fue el primer estándar aceptado, admitiendo hasta 11 Mbps en la banda frecuencial sin licencia de 2,4 GHz. Posteriormente, el estándar IEEE 802.11g fue diseñado como el sucesor del IEEE 802.11b con un mayor ancho de banda. Un punto de acceso IEEE 802.11g soportará clientes 802.11b y 802.11g. Del mismo modo, un ordenador portátil con una tarjeta IEEE 802.11g será capaz de acceder a los puntos de acceso 802.11b existentes, así como a los nuevos puntos de acceso 802.11g. Esto se debe a que las redes LAN inalámbricas basadas en 802.11g utilizan la misma banda de 2,4 GHz que utiliza el 802.11b. La velocidad de transferencia máxima para el enlace inalámbrico IEEE 802.11g es de 54 Mbps, pero se ve reducida automáticamente cuando la señal de radio es débil o cuando se detecta una interferencia.

## **Redes inalámbricas de área metropolitana (WMAN)**

Las redes inalámbricas de área metropolitana (WMAN) forman el tercer grupo de redes inalámbricas. Las WMAN se basan en el estándar IEEE 802.16, a menudo denominado WiMAX (Worldwide Interoperability for Microwave Access). WiMAX es una tecnología de comunicaciones con **arquitectura punto a multipunto** orientada a proporcionar una alta velocidad de transmisión de datos a través de redes inalámbricas de área metropolitana. Esto permite que las redes inalámbricas LAN más pequeñas puedan ser interconectadas

por WiMAX creando una gran WMAN. Consecuentemente, la creación de redes entre ciudades puede lograrse sin la necesidad de cableado costoso. WiMAX es similar a Wi-Fi, pero proporciona cobertura a distancias mayores. Mientras que Wi-Fi está destinado a proporcionar cobertura en áreas relativamente pequeñas, como en oficinas o hot spots, WiMAX opera en dos bandas de frecuencia, una mezcla de banda con licencia y banda sin licencia, de 2 GHz a 11 GHz y de 10 GHz a 66 GHz, pudiendo alcanzar velocidades de transmisión próximas a 70 Mbps en una distancia de 50 km a miles de usuarios desde una única estación base. Al poder operar en dos bandas de frecuencia, WiMAX puede trabajar con y sin línea de visión directa. En el rango de frecuencias de 2 a 11GHz se trabaja sin línea de visión directa, donde un equipo dentro de un edificio se comunica con una torre/antena exterior del edificio. Las transmisiones a baja frecuencia no son fácilmente perturbadas por obstáculos físicos. Por el contrario, las transmisiones a mayor frecuencia se utilizan en aplicaciones con línea de visión directa. Esto permite a las torres/antenas poder comunicarse entre sí en distancias mayores.

### ***Redes inalámbricas de área amplia (WWAN)***

Las redes inalámbricas de área amplia se extienden más allá de los 50 kilómetros y suelen utilizar frecuencias con licencia. Este tipo de redes se pueden mantener en grandes áreas, tales como ciudades o países, a través de los múltiples sistemas de satélites o ubicaciones con antena atendidos por un proveedor de servicios de Internet. Existen principalmente dos tecnologías disponibles: **la telefonía móvil y los satélites**.

#### **Red de telefonía móvil**

En la red de telefonía móvil, el área de cobertura se divide en celdas. Un transmisor de celda o estación base, en el centro de la celda, está diseñado para servir a una celda individual. Los dispositivos móviles están conectados a una estación base y estas últimas a una central de conmutación de telefonía móvil que une el teléfono móvil y la red cableada de telefonía. El sistema pretende hacer un uso eficiente de los canales disponibles mediante el uso de transmisores de baja potencia para permitir la reutilización de frecuencias a distancias mucho más pequeñas. Las diferentes generaciones de telefonía móvil se han



desarrollado desde principios de 1980. La primera generación, 1G, era analógica y fue concebida y diseñada exclusivamente para las llamadas de voz casi sin consideración de servicios de datos, con una velocidad de hasta 2,4 kbps. La segunda generación, 2G, está basada en tecnología digital y la infraestructura de red (GSM), permitiendo mensajes de texto con una velocidad de datos de hasta 64 Kbps. La generación 2.5G se sitúa entre la 2G y la 3G. También se la conoce como 2G + GPRS. Se trata de una versión mejorada de 2G, con una velocidad de hasta 144 Kbps. La generación 3G fue introducida en el año 2000, con una velocidad de datos de hasta 2 Mbps. La 3.5G es una versión mejorada de la 3G que utiliza HSDPA para acelerar las transferencias de datos hasta 14 Mbps. Por último, la cuarta generación, 4G, es capaz de proporcionar velocidades de hasta 1 Gbps y cualquier tipo de servicio en cualquier momento de acuerdo con las necesidades del usuario, en cualquier lugar. La generación 5G se espera para el año 2020.

### **Satélite**

Las comunicaciones inalámbricas también pueden llevarse a cabo a través de satélites. Debido a su gran altura, las transmisiones por satélite pueden cubrir una amplia área sobre la superficie de la tierra. Esto puede ser muy útil para los usuarios que se encuentran en zonas remotas o islas donde no hay cables submarinos en servicio. En estos casos, se necesitan teléfonos vía satélite. Cada satélite está equipado con varios transpondedores los cuales constan de un transceptor y una antena. La señal entrante se amplifica y luego es retransmitida en una frecuencia diferente.

### **¿Qué es un Proxy?**

Un servidor proxy proporciona una puerta de enlace entre los usuarios e Internet. Es un servidor denominado “intermediario”, porque está entre los usuarios finales y las páginas web que visitan en línea.

Los servidores proxy proporcionan una valiosa capa de seguridad para su computadora. Pueden configurarse como filtros web o firewalls, y protegen a su computadora contra amenazas de Internet como el malware.

## **Explicar el protocolo Spanning tree**

El spanning tree protocol o el protocolo de árbol de expansión se implementa en las redes de datos para controlar los bucles de red que ocurren en la capa 2 de OSI (modelo de interconexión de sistemas abiertos).

El protocolo spanning tree está diseñado para controlar enlaces redundantes que pueden afectar la red y su rendimiento. El protocolo se desarrolló a partir de la idea original de que los switch no pueden filtrar transmisiones. Por lo tanto, se envían a través de diferentes interfaces (excepto la interfaz de recepción) y eventualmente provocan una saturación debido a la difusión excesiva, lo que degrada significativamente el rendimiento de la red.

No debemos olvidar que una red informática de alta disponibilidad requiere equipos y conexiones redundantes, pero esto en última instancia crea problemas de rendimiento. La razón principal de esto es que se producen bucles en la red.

Los switch intercambian información BPDU (son paquetes que contienen información del protocolo) cada dos segundos y, si se detecta una anomalía en cualquier puerto, STP cambiará automáticamente el estado de cualquier puerto utilizando rutas redundantes sin perder la conectividad de la red.

Como podemos darnos cuenta, el spanning tree protocol tiene una aplicación respectivamente simple. Sin embargo, su utilidad y aplicación es enorme de cara a la usabilidad de las redes.

### **¿Cómo funciona?**

STP escanea continuamente la red para detectar inmediatamente cualquier falla o conexión de un enlace, switch o puente. Cuando cambia la topología de la red, el algoritmo de spanning tree reconfigura los puertos del switch o del puente para evitar la pérdida total de conectividad.

STP crea un proceso lógico para eliminar estas rutas de comunicación. El método consiste en generar un árbol de switch en la red y seleccionar uno de ellos como referencia. El switch que el sistema de protocolo elige como base para el resto del proceso se denomina puente raíz o root bridge y es el único switch que puede existir en la red. Se utilizarán

criterios de prioridad para seleccionarlos, pero también se tendrán en cuenta las direcciones MAC.

### **Tipos de Spanning Tree Protocol**

1. MSTP: Múltiple Spanning Tree
2. RSTP: Rapid Spanning Tree
3. VSTP: VLAN Spanning Tree

## **Explicar el protocolo de comunicaciones OSPF**

El protocolo OSPF (Open Shortest Path First) es un protocolo de enrutamiento que se usa en redes IP para determinar cuál es el mejor camino para el envío de los datos. Se trata de un tipo de protocolo que fue desarrollado para intentar sustituir al RIP (Routing Information Protocol) o como complemento para tener más opciones de elección en la configuración de redes informáticas.

### **Funcionamiento básico del protocolo OSPF**

El protocolo OSPF funciona recopilando y distribuyendo información de estado de los enlaces de red. Para ello, calcula las rutas más cortas empleando un algoritmo denominado SPF y crea tablas de enrutamiento. Estas tablas son las que guían la información y los paquetes a través de la red.

Además, este protocolo también cuenta con una serie de paquetes que hay que tener en cuenta ya que se usan para el intercambio de información en la red y para el cálculo de las rutas.

### **Tipos de paquetes en OSPF**

Los principales tipos de paquetes con los que trabaja el protocolo OSPF son:

- Link state request
- Hello packets
- Link state update

- Database description
- Link state acknowledgment

## **Explicar el protocolo ARP**

El protocolo de resolución de direcciones (Address Resolution Protocol, ARP) es un protocolo o procedimiento que conecta una dirección de protocolo de Internet (IP) en constante cambio a una dirección de máquina física fija, también conocida como dirección de control de acceso a medios (media access control, MAC), en una red de área local (local-area network, LAN).

Este procedimiento de mapeo es importante porque las longitudes de las direcciones IP y MAC difieren, y se necesita una traducción para que los sistemas puedan reconocerse entre sí. La IP más utilizada en la actualidad es la IP versión 4 (IPv4). Una dirección IP tiene 32 bits de longitud, pero las direcciones MAC tienen una longitud de 48 bits. El ARP traduce la dirección de 32 bits a 48 y viceversa.

### **¿Cómo funciona el ARP?**

Cuando una computadora nueva se une a una LAN, se le asigna una dirección IP única para su identificación y comunicación.

Los paquetes de datos llegan a una puerta de enlace, destinada a una máquina host en particular. La puerta de enlace, o la parte del hardware de una red que permite que los datos fluyan de una red a otra, le pide al programa ARP que encuentre una dirección MAC que coincida con la dirección IP. La caché del ARP mantiene un registro de cada dirección IP y su dirección MAC coincidente. La caché del ARP es dinámica, pero los usuarios de una red también pueden configurar una tabla ARP estática que contenga direcciones IP y direcciones MAC.

Las cachés del ARP se mantienen en todos los sistemas operativos en una red Ethernet IPv4. Cada vez que un dispositivo solicita una dirección MAC para enviar datos a otro

dispositivo conectado a la LAN, el dispositivo verifica su caché de ARP para ver si la conexión de dirección IP a MAC ya quedó completa. Si existe, no hará falta una nueva solicitud. Sin embargo, si la traducción aún no se realizó, se envía la solicitud de direcciones de red y se realiza el ARP.

El tamaño de caché del ARP está limitado por el diseño, y las direcciones tienden a permanecer en la caché solo unos minutos. Se purga regularmente para liberar espacio. Este diseño también está diseñado en función de la privacidad y la seguridad, para evitar que las direcciones IP sean robadas o suplantadas por ciberatacantes. Aunque las direcciones MAC son fijas, las direcciones IP cambian constantemente.

En el proceso de purga, se eliminan las direcciones no utilizadas; ocurre lo mismo con cualquier dato relacionado con los intentos fallidos de comunicación con computadoras no conectadas a la red o que ni siquiera están encendidas.

### **¿Cuál es la diferencia funcional entre ARP, DHCP y DNS?**

El ARP es el proceso de conectar una dirección IP dinámica a la dirección MAC de una máquina física. Como tal, es importante analizar algunas tecnologías relacionadas con la IP.

Como se mencionó anteriormente, las direcciones IP, por diseño, están pensadas para que cambien constantemente por el simple motivo de que hacerlo les da a los usuarios seguridad y privacidad. Sin embargo, las direcciones IP no deben ser completamente aleatorias. Debe haber reglas que asignen una dirección IP de un rango definido de números disponibles en una red específica. Esto ayuda a evitar problemas, como que dos computadoras reciban la misma dirección IP. Estas reglas se conocen como DHCP o protocolo de configuración dinámica de host.

Las direcciones IP como identidades de computadoras son importantes porque son necesarias para realizar una búsqueda en Internet. Cuando los usuarios buscan un nombre de dominio o un localizador uniforme de recursos (Uniform Resource Locator, URL), utilizan un nombre alfabético. Por otra parte, las computadoras utilizan la dirección IP numérica

para asociar el nombre de dominio con un servidor. Para conectar los dos, se utiliza un servidor de sistema de nombres de dominio (Domain Name System, DNS) para traducir una dirección IP de una cadena confusa de números a un nombre de dominio más legible y fácil de entender, y viceversa.

### **¿Qué es un Firewall?**

Es un sistema de seguridad de red de las computadoras que restringe el tráfico de Internet entrante, saliente o dentro de una red privada. Este software o esta unidad de hardware y software dedicados funciona bloqueando o permitiendo los paquetes de datos de forma selectiva.

### **¿Qué es un Gateway?**

Gateway es un término inglés que significa puerta o portal. Es un tipo de enrutador que funciona como un punto de parada para los datos en su camino hacia otras redes. Gracias a los Gateway es posible la comunicación y envío de datos de un lado a otro.

### **Según Microsoft, ¿qué significa NLB?**

El equilibrio de carga de red (NLB, por sus siglas en inglés) de Windows Server® 2008 proporciona distribución de tráfico mediante TCP o IP y se puede usar con la característica de configuración compartida de IIS para crear una granja de servidores web que proporcione redundancia y tolerancia a errores. NLB funciona mediante el equilibrio del tráfico entre los nodos de una granja de servidores web o un clúster. Los servidores emiten una señal intermitente a otros hosts del clúster y escuchan la señal de otros hosts. Si se produce un error en un host, los hosts restantes ajustan y redistribuyen la carga de trabajo.

NLB no supervisa el estado de la aplicación. En su lugar, permite al desarrollador de aplicaciones determinar el estado de una aplicación con carga equilibrada. Dado que cada aplicación tiene su propia definición de carga y estado, la mejor manera de medir y supervisar estas cantidades es por medio de la propia aplicación. Mediante el uso de

medidas recopiladas de la aplicación y el proveedor de WMI público de NLB, agregar seguimiento de carga y estado a la aplicación con equilibrio de carga es una tarea relativamente sencilla.

### **Tipos de enlace: MPLS, LAN to LAN, microonda, VSAT.**

- a. Explique cada uno de estos tipos de enlace.**
- b. Agregue dos tipos de enlaces, no mencionados anteriormente.**
- c. Ranking de enlaces según lo pedido (de uno a seis, siendo uno el mejor): Por económico, performance, mayor capacidad, mayor o mejor configuración de restricciones, soporte a mayor distancia, menor esfuerzo de configuración.**
- d. Elija un tipo de enlace para los siguientes escenarios:**
  - i. Conectividad de varios de call centers con un data center central.**
  - ii. Conectar los datos de los pozos petroleros durante 15 minutos por día.**
  - iii. Comunicar dos edificios enfrentados en la misma calle.**

MPLS (Multiprotocol Label Switching): Es una técnica de conmutación de datos que utiliza etiquetas para dirigir los paquetes a través de una red. MPLS puede operar sobre diferentes tecnologías de red y proporciona una forma eficiente de gestionar el tráfico y mejorar la calidad del servicio (QoS).

LAN to LAN: Se refiere a la interconexión de dos redes de área local (LAN) a través de una conexión de red, como una VPN o enlaces dedicados.

Microonda: Utiliza ondas electromagnéticas para transmitir datos entre dos puntos. Requiere una línea de vista directa entre los equipos transmisores y receptores.

VSAT (Very Small Aperture Terminal): Utiliza satélites para transmitir y recibir datos. Se emplea comúnmente en áreas remotas o para comunicaciones globales.

### **Dos tipos adicionales de enlaces**

Fibra Óptica: Utiliza cables de fibra óptica para transmitir datos a través de pulsos de luz. Es conocida por su alta capacidad y velocidad.

Redes Móviles (4G/5G): Usa redes celulares para transmitir datos. Es una opción flexible y móvil.

### Ranking de enlaces según criterios

| Criterio                             | 1º           | 2º   | 3º         | 4º         | 5º         | 6º           |
|--------------------------------------|--------------|------|------------|------------|------------|--------------|
| Económico                            | LAN to LAN   | VSAT | 4G/5G      | Microonda  | MPLS       | Fibra Óptica |
| Performance                          | Fibra Óptica | MPLS | Microonda  | 4G/5G      | LAN to LAN | VSAT         |
| Mayor Capacidad                      | Fibra Óptica | MPLS | Microonda  | VSAT       | 4G/5G      | LAN to LAN   |
| Mejor Configuración de Restricciones | Fibra Óptica | MPLS | Microonda  | LAN to LAN | 4G/5G      | VSAT         |
| Soporte a Mayor Distancia            | Fibra Óptica | VSAT | Microonda  | MPLS       | 4G/5G      | LAN to LAN   |
| Menor Esfuerzo de Configuración      | 4G/5G        | VSAT | LAN to LAN | Microonda  | MPLS       | Fibra Óptica |

### Elección del tipo de enlace para los escenarios

- Conectividad de varios call centers con un data center central:

MPLS. ya que ofrece una red segura y eficiente, con buena calidad de servicio y soporte para múltiples ubicaciones.

- Conectar los datos de los pozos petroleros durante 15 minutos por día:

VSAT. Permite la conexión en ubicaciones remotas con baja frecuencia de uso, aunque la latencia puede ser una consideración.

- Comunicar dos edificios enfrentados en la misma calle:



Microonda. Proporciona una solución rápida y efectiva para distancias cortas, siempre que haya una línea de vista directa.

## Describir la tecnología LTE

LTE (Long-Term Evolution) es una tecnología de comunicaciones inalámbricas diseñada para mejorar la velocidad y eficiencia de las redes móviles. Desarrollada como parte de la evolución hacia 4G, LTE proporciona una mayor capacidad de datos y menor latencia en comparación con sus predecesores (como 3G).

### Características clave:

- Velocidad: Ofrece tasas de descarga de hasta 300 Mbps y subida de hasta 75 Mbps.
- Latencia: Reduce el tiempo de respuesta entre la solicitud y la entrega de datos, mejorando la experiencia en aplicaciones en tiempo real.
- Espectro: Soporta una variedad de bandas de frecuencia, lo que permite mayor flexibilidad en el despliegue de redes.
- Eficiencia: Optimiza el uso del ancho de banda mediante la técnica OFDMA (Acceso Múltiple por División de Frecuencia Ortogonal) en enlace descendente y SC-FDMA (Acceso Múltiple por División de Frecuencia de Portadora Única) en el enlace ascendente.
- VoLTE: Permite la transmisión de llamadas de voz sobre la red LTE en lugar de utilizar redes 2G o 3G.

**Explique la solución de Microsoft Teams. Si quieren describir otra solución de otra empresa es también válido.**

### Reuniones y Conferencias

- Reuniones online
- Videoconferencia
- Pantalla compartida

- Fondos Personalizados
- Seminarios web
- Accesibilidad
- Puesto temporal
- Asamblea informativa

### **Teléfonos Teams**

- Teléfono Teams
- VOIP
- PBX
- Videollamadas
- Teléfonos Empresariales
- Centro de Contacto

### **Chat y Colaboración**

- Mensajería Instantánea
- Uso compartido de archivos
- Colaboración
- Chat

### **Dispositivos**

- Dispositivos de Teams
- Salas de Teams

### **Aplicaciones**

- Aplicaciones y flujos de trabajo
- Aplicaciones de reuniones
- Microsoft Mesh

### **Personal de Primera Línea**

- Soluciones de primera línea

- Administración de recursos
- Personal y programación

## ¿Qué significa aplicar calidad en un enlace MPLS?

MPLS ofrece la posibilidad de predefinir rutas que establecen el camino que debe seguir un paquete desde el punto de origen al de destino. De esta forma, MPLS logra descongestionar la gran carga que soportaban antes los sistemas de enrutamiento.

Esta técnica es usada principalmente por operadores que quieren garantizar la calidad del servicio en el marco de la ingeniería o gestión de tráfico (Traffic engineering, TE), así como en las redes virtuales privadas (VPN).

Una de sus grandes ventajas es la seguridad, ya que permite a los dispositivos conectarse a una red sin que estén físicamente conectados entre sí, es decir, consigue una conexión fuera del Internet público, de manera que los datos transmitidos quedan más protegidos frente a diversos tipos de ataques a la red del cliente, como por ejemplo los de denegación de servicio (DDoS).

La interconexión MPLS se realiza incorporando a cada paquete de datos que va a ser transmitido (ya sea voz, texto, video o imagen) un **encabezado**. Este contiene una o varias etiquetas apiladas según la operación que llevan a cabo en los enrutadores por los que el paquete va pasando hasta alcanzar su destino.

Además de la etiqueta, que permite establecer los circuitos virtuales, MPLS tiene la capacidad de aplicar **QoS**, acrónimo de **Quality of Service (calidad de servicio)**, que establece varios mecanismos para asegurar la fluidez en el tráfico de la red. Para ello, prioriza el tráfico en función del tipo de datos.

Para administrar el tráfico de forma eficiente, la tecnología MPLS tiene distintos mecanismos:

- **La etiqueta:** permite determinar a dónde reenviar los datos para crear circuitos virtuales a través de la infraestructura, mejorando la velocidad de transmisión.
- **Bits experimentales:** su función es dar prioridad a unos paquetes de información sobre otros, en función de la actividad que realicen en la red los usuarios.
- **Parte inferior de la pila:** mensaje que comunica a los enrutadores que los paquetes han sido enviados con éxito y que ya no quedan más para compartir.
- **Tiempo de vida:** número de veces que un paquete concreto de información puede ser enviado antes de descartarse.
- **QoS (Calidad de servicio):** permite soporte de calidad de servicio en redes IP.

## ¿Qué diferencias puede encontrar entre una conexión Coaxial, UTP o Fibra?

Las principales características de los medios guiados son:

- El tipo de conductor utilizado.
- La velocidad máxima de transmisión.
- Las distancias máximas que puede ofrecer entre repetidores.
- La inmunidad frente a interferencias electromagnéticas.
- La facilidad de instalación.
- La capacidad de soportar diferentes tecnologías de nivel de enlace.
- La velocidad de transmisión depende directamente de la distancia entre los terminales, y de si el medio se utiliza para realizar un enlace punto a punto o un enlace multipunto.

| Cable Coaxial  | Cables UTP y FTP   | Fibra Óptica   |
|--|--|--|
| Ventajas   |  |  |
| <ul style="list-style-type: none"> <li>• Mayor distancia que los cables UTP o STP (500 mts).</li> <li>• Es más económica que la</li> </ul> | <ul style="list-style-type: none"> <li>• Bajo costo en su contratación.</li> <li>• Alto número de estaciones de trabajo por segmento.</li> </ul> | <ul style="list-style-type: none"> <li>• Una banda de paso muy ancha, lo que permite flujos muy elevados (del orden del GHz).</li> </ul> |

|  |   |  |
|--|---|--|
| <p>Fibra Óptica.</p> <ul style="list-style-type: none"> <li>• Tecnología masiva y muy conocida.</li> </ul> | <ul style="list-style-type: none"> <li>• Facilidad para el rendimiento y la solución de problemas.</li> <li>• Puede estar previamente cableado en un lugar o en cualquier parte.</li> </ul> | <ul style="list-style-type: none"> <li>• Pequeño tamaño, por tanto ocupa poco espacio.</li> <li>• Gran flexibilidad, el radio de curvatura puede ser inferior a 1 cm, lo que facilita la instalación enormemente.</li> <li>• Gran ligereza, el peso es del orden de algunos gramos por kilómetro, lo que resulta unas nueve veces menos que el de un cable convencional.</li> <li>• Inmunidad total a las perturbaciones de origen electromagnético, lo que implica una calidad de transmisión muy buena, ya que la señal es inmune a las tormentas, chisporroteo.</li> <li>• Gran seguridad: la intrusión en una fibra óptica es fácilmente detectable por el debilitamiento de la energía luminosa en recepción, además, no radia nada, lo que es particularmente interesante para aplicaciones que requieren alto nivel de confidencialidad.</li> </ul> |
|--|---|--|

|  |  |   |
|--|--|---|
|  |  | <ul style="list-style-type: none"> <li>• No produce interferencias.</li> <li>• Insensibilidad a los parásitos, lo que es una propiedad principalmente utilizada en los medios industriales fuertemente perturbados (por ejemplo, en los túneles del metro). Esta propiedad también permite la coexistencia por los mismos conductos de cables ópticos no metálicos con los cables de energía eléctrica.</li> <li>• Atenuación muy pequeña independiente de la frecuencia, lo que permite salvar distancias importantes sin elementos activos intermedios.</li> <li>• Gran resistencia mecánica (resistencia a la tracción, lo que facilita la instalación).</li> <li>• Resistencia al calor, frío, corrosión.</li> <li>• Facilidad para localizar los cortes gracias a un proceso basado en la telemetría, lo que permite detectar rápidamente el lugar y posterior reparación de la avería, simplificando la labor de</li> </ul> |
|--|--|---|

|  |  | mantenimiento.   |
|--|--|--|
| Desventajas  |  |  |
| <ul style="list-style-type: none"> <li>• Su rigidez dificulta la instalación.</li> <li>• Se debe considerar su grosor al momento de la canalización.</li> <li>• Si se instala sin respetar las normas el aislante se puede convertir en un medio con altas tasa de ruidos eléctricos.</li> </ul> | <ul style="list-style-type: none"> <li>• Altas tasas de error a altas velocidades.</li> <li>• Ancho de banda limitado.</li> <li>• Baja inmunidad al ruido.</li> <li>• Baja inmunidad al efecto crosstalk (diafonía).</li> <li>• Alto costo de los equipos.</li> <li>• Distancia limitada (100 metros por segmento).</li> </ul> | <ul style="list-style-type: none"> <li>• La alta fragilidad de las fibras.</li> <li>• Necesidad de usar transmisores y receptores más caros.</li> <li>• Los empalmes entre fibras son difíciles de realizar, especialmente en el campo, lo que dificulta las reparaciones en caso de ruptura del cable.</li> <li>• No puede transmitir electricidad para alimentar repetidores intermedios.</li> <li>• La necesidad de efectuar, en muchos casos, procesos de conversión eléctrica-óptica.</li> <li>• La fibra óptica convencional no puede transmitir potencias elevadas.</li> <li>• Ancho de Banda de los Medios de Trasmisión de Datos Guiados o Alámbricos.</li> </ul> |

**Según Cisco, ¿qué significa CCENT, CCNA y CCNP? Descripción breve del Track Routing & Switching y de algún otro a elección (ej. Wireless, Security, Cloud, etc).**

## CCENT

**Cisco Certified Entry Networking Technician** es una certificación de nivel de entrada ofrecida por Cisco Systems. Como su nombre indica, esta certificación está diseñada para personas que recién comienzan su carrera en redes de computadoras. CCENT es un punto de partida excelente para quienes desean adentrarse en el mundo de las redes y aprender los conceptos básicos.

## CCNA

**Cisco Certified Network Associate**, es una certificación de nivel intermedio que se centra en una variedad más amplia de temas de redes. CCNA es una de las certificaciones más populares y respetadas en la industria de las tecnologías de la información. Ofrece una base sólida en redes y prepara a los profesionales para roles más avanzados en el campo de las redes.

## CCNP

**Cisco Certified Network Professional**, es una certificación avanzada que valida la capacidad de planificar, implementar, verificar y solucionar problemas en redes empresariales complejas.

A diferencia de las certificaciones de nivel básico, CCNP está diseñada para profesionales con experiencia que buscan escalar en su carrera y adquirir habilidades más avanzadas en redes.

## Track Routing & Switching

Los switches son piezas de construcción clave para cualquier red. Conectan varios dispositivos, como computadoras, access points inalámbricos, impresoras y servidores; en la misma red dentro de un edificio o campus. Un switch permite a los dispositivos conectados compartir información y comunicarse entre sí.



- **Switches no administrados:** un switch de red no administrado está diseñado para que pueda simplemente conectarlo y funcione, sin necesidad de configuración. Los switches no administrados se usan generalmente para conectividad básica. En general, se verán en redes domésticas o donde sea que se necesiten unos cuantos puertos más, como en su escritorio, en un laboratorio o en una sala de conferencias.
- **Switches administrados:** los switches administrados ofrecen mayor seguridad, más funciones y flexibilidad, dado que, pueden configurarse para que se adapten a la red. Con este mayor control, puede proteger mejor su red y mejorar la calidad del servicio para los que acceden a ella.
- **Concentradores y switches de red:** un concentrador de red es un punto de conexión central para los dispositivos de una red de área local, o LAN. Pero existe un límite para la cantidad de ancho de banda que los usuarios pueden compartir en una red basada en concentradores. Cuantos más dispositivos se agreguen al concentrador de red, más tiempo tardarán los datos en llegar a su destino. Un switch evita estas y otras limitaciones de los concentradores de red.

Una gran red puede incluir varios switches, que conectan diferentes grupos de sistemas informáticos entre sí. En general, estos switches están conectados a un router que permite a los dispositivos conectados acceder a Internet.

- **Routers:** los routers permiten que se comuniquen diferentes redes entre sí. Pueden conectar computadoras en red a Internet, de modo que varios usuarios puedan compartir una conexión. Los routers permiten conectar redes dentro de una organización o conectar las redes de varias ubicaciones de las sucursales. Funcionan como un distribuidor, dirigiendo el tráfico de datos y eligiendo la mejor ruta para que la información viaje a través de la red, de modo que se transmita de la manera más eficiente posible.

### Componentes claves

- **Enrutamiento:** se refiere a la selección de caminos en una red para enviar datos desde un origen hasta un destino. Implica el uso de protocolos de enrutamiento

como OSPF (Open Shortest Path First), BGP (Border Gateway Protocol) y EIGRP (Enhanced Interior Gateway Routing Protocol).

- **Conmutación:** involucra el envío de paquetes de datos dentro de una misma red local (LAN) utilizando switches. Se centra en la creación de VLANs (Virtual Local Area Networks) y el manejo del tráfico a través de técnicas como Spanning Tree Protocol (STP).
- **Optimización de la red:** incluye la implementación de Quality of Service (QoS) para garantizar que el tráfico crítico reciba prioridad, mejorando el rendimiento general de la red.
- **Seguridad de la red:** involucra medidas de seguridad en routers y switches, como listas de control de acceso (ACL) y la segmentación de redes para proteger contra amenazas.
- **Escalabilidad y redundancia:** se diseñan redes que pueden crecer sin perder rendimiento y que cuentan con caminos alternativos en caso de fallos.

## Explique el modelo OSI

El modelo de interconexión de sistemas abiertos (**Open Systems Interconnection, OSI**) es un marco conceptual que divide las funciones de comunicaciones de red en siete capas. El envío de datos a través de una red es complejo porque varias tecnologías de hardware y software deben funcionar de manera consistente a través de las fronteras geográficas y políticas. El modelo de datos OSI proporciona un lenguaje universal para las redes informáticas, de modo que diversas tecnologías pueden comunicarse mediante protocolos o reglas de comunicación estándar. Cada tecnología de una capa específica debe proporcionar ciertas capacidades y realizar funciones específicas para ser útil en las redes. Las tecnologías de las capas superiores se benefician de la abstracción, ya que pueden utilizar tecnologías de nivel inferior sin tener que preocuparse por los detalles de implementación subyacentes.

## Capas del modelo OSI

- **Capa física:** se refiere al medio de comunicación físico y a las tecnologías para transmitir datos a través de ese medio. En esencia, la comunicación de datos es la transferencia de señales digitales y electrónicas a través de varios canales físicos, como cables de fibra óptica, cableado de cobre y aire. La capa física incluye estándares para tecnologías y métricas estrechamente relacionadas con los canales, como Bluetooth, NFC y velocidades de transmisión de datos.
- **Capa de enlace de datos:** se refiere a las tecnologías utilizadas para conectar dos máquinas a través de una red donde la capa física ya existe. Gestiona los marcos de datos, que son señales digitales encapsuladas en paquetes de datos. El control del flujo y el control de errores de los datos suelen ser los enfoques clave de la capa de enlace de datos. Ethernet es un ejemplo de un estándar a este nivel. La capa de enlace de datos a menudo se divide en dos subcapas: la **capa de control de acceso a los medios (MAC)** y la **capa de control de enlace lógico (LLC)**.
- **Capa de red:** se ocupa de conceptos como el enrutamiento, el reenvío y el direccionamiento a través de una red dispersa o de múltiples redes conectadas de nodos o máquinas. La capa de red también puede gestionar el control de flujo. En Internet, el Protocolo de Internet v4 (IPv4) y el IPv6 se utilizan como protocolos de capa de red principales.
- **Capa de transporte:** el objetivo principal de esta capa es garantizar que los paquetes de datos lleguen en el orden correcto, sin pérdidas ni errores, o que se puedan recuperar sin problemas si es necesario. El control del flujo, junto con el control de errores, suele ser un objetivo en la capa de transporte. En esta capa, los protocolos de uso común incluyen el **Protocolo de Control de Transmisión (TCP)**, un protocolo basado en conexiones casi sin pérdidas y el **Protocolo de datagramas de usuario (UDP)**, un protocolo sin conexiones con pérdidas. TCP se suele utilizar cuando todos los datos deben estar intactos (por ejemplo, cuando se comparten

archivos), mientras que UDP se utiliza cuando retener todos los paquetes es menos crítico (por ejemplo, streaming de vídeo).

- **Capa de sesión:** es responsable de la coordinación de la red entre dos aplicaciones independientes en una sesión. Una sesión gestiona el inicio y el final de los conflictos de sincronización y conexión de una aplicación uno a uno. **Network File System (NFS)** y **Server Message Block (SMB)** son protocolos de uso común en la capa de sesión.
- **Capa de presentación:** se ocupa principalmente de la sintaxis de los datos en sí para que las aplicaciones los envíen y consuman. Por ejemplo, el lenguaje de marcas de hipertexto (HTML), la notación de objetos JavaScript (JSON) y los valores separados por comas (CSV) son lenguajes de modelado para describir la estructura de los datos en la capa de presentación.
- **Capa de aplicación:** se refiere al tipo específico de aplicación en sí y a sus métodos de comunicación estandarizados. Por ejemplo, los navegadores pueden comunicarse mediante el Protocolo seguro de transferencia de hipertexto (HTTPS) y los clientes de correo electrónico y HTTP pueden comunicarse mediante POP3 (Protocolo de oficina de correo versión 3) y SMTP (Protocolo simple de transferencia de correo).

### ¿Cómo se produce la comunicación en el modelo OSI?

Las capas del modelo de interconexión de sistemas abiertos (OSI) están diseñadas para que una aplicación pueda comunicarse a través de una red con otra aplicación en un dispositivo diferente sin importar la complejidad de la aplicación y los sistemas subyacentes. Para ello, se utilizan varios estándares y protocolos para comunicarse con la capa superior o inferior. Cada una de las capas es independiente y solo conoce las interfaces para comunicarse con la capa superior e inferior.



Al encadenar todas estas capas y protocolos, se pueden enviar comunicaciones de datos complejas de una aplicación de alto nivel a otra. El proceso funciona de la siguiente manera:

1. La capa de aplicación del remitente transfiere la comunicación de datos a la siguiente capa inferior.
2. Cada capa añade sus propios encabezados y direccionamientos a los datos antes de transmitirlos.
3. La comunicación de datos desciende por las capas hasta que finalmente se transmite a través del medio físico.
4. En el otro extremo del medio, cada capa procesa los datos de acuerdo con los encabezados relevantes en ese nivel.
5. En el extremo receptor, los datos suben por la capa y se desempaquetan gradualmente hasta que la aplicación del otro extremo los recibe.

## **28- Realizar cuestionario online y copiar el resultado: (1 por cada integrante)**

**[https://es.educaplay.com/es/recursoseducativos/706834/test\\_de\\_redes\\_y\\_comunicaciones.htm](https://es.educaplay.com/es/recursoseducativos/706834/test_de_redes_y_comunicaciones.htm)**

**Martín Esperon**

|   |  |               |
|---|--|---------------|
| <b>PUNTOS</b>   |  | <b>60.000</b> |
|            |  |               |
| Compartir  |  |               |
| PUNTOS  |  | <b>60</b>     |
| TIEMPO  |  | <b>02:12</b>  |
| ACIERTOS  |  | <b>6 / 10</b> |

**Maryangelin quintero**



Leonardo Buján



## 29- Explicar el estándar IEEE 802.3 regula la red. Cómo se implementa, ventajas y desventajas.

El estándar IEEE 802.3 regula las redes de área local (LAN) que utilizan Ethernet, especificando cómo se debe transmitir la información a través de cables. Este estándar cubre varios aspectos técnicos, incluyendo la codificación de datos, la detección de colisiones y el acceso al medio de transmisión.

| Implementación | Ventajas | Desventajas |
|----------------|----------|-------------|
|----------------|----------|-------------|

|  |   |  |
|--|---|--|
| <ul style="list-style-type: none"> <li>• <b>Tipos de Medios:</b> el estándar define diferentes tipos de medios de transmisión, como cables de par trenzado (Cat 5e, Cat 6), fibra óptica y coaxial.</li> <li>• <b>Topologías:</b> permite la implementación de topologías en estrella, donde los dispositivos están conectados a un switch central, o en bus, donde todos los dispositivos comparten un único medio de transmisión.</li> <li>• <b>Protocolos:</b> utiliza el protocolo <b>CSMA/CD</b> (Carrier Sense Multiple Access with Collision Detection) para gestionar el acceso al medio, evitando colisiones entre paquetes de datos.</li> <li>• <b>Velocidades:</b> el estándar ha evolucionado para soportar diversas velocidades de</li> </ul> | <ul style="list-style-type: none"> <li>• <b>Amplia compatibilidad:</b> es un estándar ampliamente adoptado, lo que asegura la interoperabilidad entre diferentes dispositivos y fabricantes.</li> <li>• <b>Costo Efectivo:</b> los equipos Ethernet, como switches y cables, son relativamente económicos y fáciles de instalar.</li> <li>• <b>Escalabilidad:</b> permite la expansión de la red sin problemas significativos, ya que se pueden agregar más dispositivos de manera sencilla.</li> <li>• <b>Rendimiento:</b> ofrece velocidades de transmisión altas y una latencia baja, lo que es ideal para aplicaciones críticas.</li> </ul> | <ul style="list-style-type: none"> <li>• <b>Colisiones en cables compartidos:</b> en redes más antiguas que utilizan topologías de bus, pueden ocurrir colisiones, lo que afecta el rendimiento. Sin embargo, esto se ha mitigado en topologías en estrella.</li> <li>• <b>Limitaciones de Distancia:</b> la distancia máxima entre dispositivos puede ser un limitante, especialmente en cables de par trenzado, que generalmente no superan los 100 metros.</li> <li>• <b>Interferencia:</b> en entornos con mucha interferencia electromagnética, la calidad de la señal puede verse afectada, especialmente en cables de cobre.</li> </ul> |
|--|---|--|

|  |  |  |
|--|--|--|
| transmisión, desde 10 Mbps (10Base-T) hasta 100 Gbps y más (como 100GBase-SR). |  |  |
|--|--|--|

## Explicar el estándar IEEE 802.4 regula la red

El IEEE 802.4 (token bus) es un protocolo para redes de área local que implementa una red lógica en anillo con paso de testigo sobre una red física de cable coaxial en forma de bus. La estructura token bus se desarrolló con el fin de minimizar las colisiones en la red y se extendió rápidamente por su fácil instalación.

| Ventajas  | Desventajas   |
|---|---|
| <ul style="list-style-type: none"> <li>Minimiza el tráfico de colisiones al permitir que un nodo reserve el uso del canal.</li> <li>Tiene las ventajas físicas de la topología en bus y las lógicas de una red de anillo.</li> <li>Puede enviar marcos más cortos.</li> <li>Buen rendimiento y eficiencia en alta carga.</li> </ul> | <ul style="list-style-type: none"> <li>Inestabilidad, como en una red en anillo cuando cae un nodo cae toda la red. Aunque esto fue solucionado aplicando una red de doble anillo pero lo que implica la necesidad de más recursos.</li> <li>No es conveniente al usarse fibra óptica.</li> <li>Vulnerabilidad de cable, una sola avería es fatal.</li> </ul> |

## ¿Qué protocolos se usan para enviar y recibir correo?

El protocolo que se usa es el "SMTP", de tipo TCP/IP, que funciona como una simple transferencia de correo. Garantiza la autenticación de los socios de comunicación, la integridad y confidencialidad de los datos. También, utiliza métodos como sockets seguros (SSL) o capas de seguridad de transporte (Transport Layer Security).



## ¿Qué protocolo puede usarse para leer correo recibido?

Para leer el correo recibido, se utilizan principalmente dos protocolos:

### IMAP (Internet Message Access Protocol)

- Este protocolo permite acceder y gestionar los correos directamente en el servidor, sin necesidad de descargarlos. Los cambios que realices, como mover o eliminar correos, se reflejan en todos los dispositivos que uses.
- Es útil cuando accedes a tu correo desde múltiples dispositivos, ya que mantiene los mensajes sincronizados en tiempo real.

### POP3 (Post Office Protocol versión 3)

- Este protocolo descarga los correos del servidor al dispositivo local y, por lo general, los elimina del servidor después de la descarga.
- Es útil si solo accedes al correo desde un único dispositivo o si deseas mantener una copia local de tus correos.

## Diferencias entre IPV4 e IPV6

Los paquetes IPv4 e IPv6 se componen de manera diferente, ya que IPv6 tiene encabezados diferentes y un espacio de encabezado más corto en general. IPv6 también ofrece paquetes de encabezados separados como una característica para ampliar las opciones de enrutamiento. Las siguientes son tres diferencias principales desde la perspectiva del usuario.

### Espacio de direcciones

El espacio de direcciones completo de IPv4 es de  $2^{32}$  o 4 294 967 296 direcciones IP. IPv6 tiene un espacio de direcciones considerablemente mayor,  $2^{128}$ , o  $3403 \times 10^{38}$ , o 340 282 366

920 938 000 000 000 000 000 000 000 direcciones IP únicas. Ese número, en inglés, se traduce en alrededor de 340 undecillones, 300 decillones.

De las direcciones de Internet IPv4, hay alrededor de 588 millones de direcciones IP reservadas, y el resto está disponible públicamente. Debido a la expansión de los dispositivos de Internet, las direcciones de Internet IPv4 no asignadas se agotaron en 2011. Si bien IPv6 resuelve este espacio de direcciones agotado, la solución actual es la abstracción mediante la superposición de otros sistemas de direccionamiento, como la traducción de direcciones de red (NAT), sobre IPv4.

IPv6 también tiene una gran cantidad de direcciones IP reservadas; sin embargo, con un espacio de direcciones mucho mayor en general, este número no es significativo en comparación. Dadas las estimaciones actuales, el espacio de direcciones es inagotable.

## Nomenclatura

En IPv4, el nombre de la dirección se representa mediante una dirección numérica de cuatro números decimales (en el rango de 0 a 255), cada uno de los cuales representa ocho bits, separados por tres puntos: **197.0.0.1**

En IPv6, el nombre de la dirección se representa mediante ocho números hexadecimales compuestos de números (0-9) y letras (A-F), cada uno de los cuales representa cuatro bits, separados por dos puntos: **2600:1400:d:5a3::3bd4**

## Tipos de comunicación

Para mejorar la eficiencia de la comunicación, tanto IPv4 como IPv6 admiten diferentes tipos de direcciones para que un dispositivo se pueda comunicar con varios dispositivos de una red simultáneamente. IPv4 admite el direccionamiento uno a uno (monodifusión), uno a todos (transmisión) y uno a muchos (multidifusión) con enrutamiento de paquetes múltiples. Como alternativa, IPv6 admite el direccionamiento de monodifusión, multidifusión y difusión por proximidad con enrutamiento de paquetes múltiples. En la comunicación de difusión por proximidad, los paquetes de datos se envían desde un remitente al receptor más cercano

de los múltiples receptores que comparten la misma dirección de difusión por proximidad. El “más cercano” lo determinan los protocolos de enrutamiento que calculan la ruta más corta o el costo más bajo para llegar al destino.

### **34- (Individual para cada integrante del grupo) ¿Qué experiencia tienen en redes?**

**Ejemplos.: Accedo y configuro el router de mi casa como admin, en mi trabajo hago tareas relacionadas a networking, configuro una PAN hogareña para mi o mi familia, amigos/as etc (Personal Area Network, todo dispositivo Wireless o no), no tengo ninguna experiencia, etc.**

**Martín Esperon:** Hice múltiples veces una LAN para jugar videojuegos con amigos y accedí al router de mi casa para chequear que la compañía de internet haya dejado todo bien.

**Maryangelin Quintero:** Accedo y configuro el router de mi casa como administrador. En este proceso, he manejado varias configuraciones como establecer el nombre de la red (SSID) y la contraseña para asegurar la conexión inalámbrica en mi hogar, cambiar las contraseñas predeterminadas del router, revisar y gestionar los dispositivos conectados a la red.

**Leonardo Buján:** He armado un cable par trenzado UTP según la norma, accedo al router de mi casa como administrador, he cambiado la configuración de la tarjeta de red inalámbrica para que funcione mejor.