Conmutación y Enrutamiento

Ing. En Sistemas Computacionales – 7mo Semestre agosto – diciembre 2023

JOSE ARTURO BUSTAMANTE LAZCANO

Contenido

[Semana 1 – Unidad 1 - Direccionamiento IP y Enrutamiento. 3](#_Toc151988502)

[Semana 2 – Unidad 1 - Enrutamiento estático y dinámico. 13](#_Toc151988503)

[Semana 3 – Unidad 1 – Router RIP. 18](#_Toc151988504)

[Semana 4 – Unidad 1 – Clasificación de Señales. 20](#_Toc151988505)

[Examen unidad 1: 23](#_Toc151988506)

[Semana 5 – Unidad 2 – Segmentación de dominio de colisión y broadcast 24](#_Toc151988507)

[Segmentación de dominio de colisión y broadcast 24](#_Toc151988508)

[¿Qué es el switch Capa 2? 25](#_Toc151988509)

[¿Cuál es el Switch Capa 3? 26](#_Toc151988510)

[La diferencia entre un switch capa 2 vs capa 3 27](#_Toc151988511)

[¿ Cómo elegir entre un switch Capa 2 y un switch Capa 3? 29](#_Toc151988512)

[Consideraciones de uso inicial 29](#_Toc151988513)

[Requerimientos de enrutamiento Inter-VLAN 29](#_Toc151988514)

[Comparación con routers 29](#_Toc151988515)

[Uso de switch capa 3 29](#_Toc151988516)

[Uso de router capa 3 30](#_Toc151988517)

[¿ Cómo comprar switches Capa 2 y switches Capa 3? 30](#_Toc151988518)

[Velocidad de Reenvío (Throughput) 30](#_Toc151988519)

[Ancho de Banda del Backplane (Switch Fabric) 30](#_Toc151988520)

[Otros Parámetros Clave 31](#_Toc151988521)

[Resumen 31](#_Toc151988522)

[Semana 6 – Unidad 2 - Vlans 32](#_Toc151988523)

[Semana 7 – Unidad 2 – Vlans - Practica 34](#_Toc151988524)

[Semana 8 – Unidad 2 – Vlans - Practica 43](#_Toc151988525)

[Examen Unidad 2: 46](#_Toc151988526)

[Semana 9 – Unidad 3 - Tecnologías WAN 47](#_Toc151988527)

[Redes Wan 47](#_Toc151988528)

[Enlaces Dedicados 49](#_Toc151988529)

[Semana 10 – Unidad 3 – Tecnologías WAN 52](#_Toc151988530)

[Enlaces dedicados: qué son y cómo funcionan 52](#_Toc151988531)

[Enlaces dedicados. 53](#_Toc151988532)

[Semana 11 – Unidad 3 –Topologías WAN. 57](#_Toc151988533)

[Semana 12 – Unidad 3 –Topologías WAN. 63](#_Toc151988534)

[Examen Unidad 3: 65](#_Toc151988535)

[Semana 13 – Unidad 4 – Tecnologías inalámbricas. 66](#_Toc151988536)

[Semana 14 – Unidad 4 – Estándares y protocolos: bluetooth, Infrarrojo, Wi-Fi, Wi-Max.. 68](#_Toc151988537)

[Semana 15 – Unidad 4 – Estándares y protocolos: bluetooth, Infrarrojo, Wi-Fi, Wi-Max.. 70](#_Toc151988538)

[Semana 16 – Unidad 4 – Estándares y protocolos: bluetooth, Infrarrojo, Wi-Fi, Wi-Max.. 72](#_Toc151988539)

[Examen unidad 4: 74](#_Toc151988540)

# Semana 1 – Unidad 1 - Direccionamiento IP y Enrutamiento.

21, 23 y 24 de agosto.

El direccionamiento IP es el sistema de direcciones que identifica de forma única cada dispositivo conectado a una red de computadoras que utiliza el protocolo de Internet (IP). Una dirección IP es un número de 32 bits que se asigna a cada dispositivo en una red de computadoras.

Existen dos tipos de direcciones IP: públicas y privadas. Las direcciones IP públicas son únicas en todo el mundo y se utilizan para identificar dispositivos en Internet. Las direcciones IP privadas no son únicas en todo el mundo y se utilizan para identificar dispositivos en redes privadas.

Las direcciones IP se suelen escribir en notación decimal punteada, con cuatro números separados por puntos. Por ejemplo, la dirección IP 192.168.1.1 se compone de los cuatro números 192, 168, 1 y 1.

Las direcciones IP se utilizan para enviar y recibir datos entre dispositivos en una red de computadoras. Cuando un dispositivo desea enviar datos a otro dispositivo, utiliza la dirección IP del dispositivo de destino para encontrar el dispositivo en la red.

El direccionamiento IP es una parte esencial de Internet. Sin direcciones IP, no sería posible enviar ni recibir datos entre dispositivos en Internet.

Ejemplo y Práctica

Escenario Sistema de comunicación entre 2 máquinas que usan el protocolo ip en una dirección privada

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Interfaz de usuario gráfica, Gráfico

Descripción generada automáticamente

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Ejercicio 2 Red Publica Sistema con Router

Interfaz de usuario gráfica, Gráfico, Aplicación

Descripción generada automáticamente

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Interfaz de usuario gráfica

Descripción generada automáticamente

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Interfaz de usuario gráfica, Gráfico, Aplicación

Descripción generada automáticamente

1.1.1 Direccionamiento con clase (VLSM).

El direccionamiento con clase (VLSM) es una técnica de direccionamiento IP que permite a los administradores de redes asignar subredes de tamaño variable a diferentes segmentos de red. Esto puede ayudar a mejorar la eficiencia del direccionamiento y reducir el desperdicio de direcciones IP.

El direccionamiento con clase tradicional asigna direcciones IP en función de tres clases: A, B y C. Las direcciones de clase A se asignan a grandes redes, las direcciones de clase B se asignan a redes de tamaño mediano y las direcciones de clase C se asignan a redes pequeñas. Esto puede ser ineficiente para redes que no se ajustan a estas clases estándar.

El VLSM permite a los administradores de redes asignar subredes de tamaño variable a diferentes segmentos de red. Esto se puede hacer utilizando máscaras de subred de longitud variable (VLSM). Las máscaras de subred VLSM permiten a los administradores de redes especificar el número de bits que se utilizan para identificar la red y el número de bits que se utilizan para identificar los hosts de la red.

Por ejemplo, una máscara de subred de 24 bits identifica una red con 256 hosts. Una máscara de subred de 25 bits identifica una red con 64 hosts. Una máscara de subred de 26 bits identifica una red con 16 hosts.

El VLSM puede ayudar a mejorar la eficiencia del direccionamiento de varias maneras. En primer lugar, puede ayudar a reducir el desperdicio de direcciones IP. En segundo lugar, puede ayudar a mejorar el rendimiento de la red al reducir el tamaño de los dominios de difusión. En tercer lugar, puede ayudar a mejorar la seguridad de la red al aislar los segmentos de red.

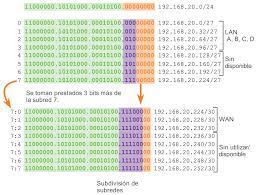
El VLSM es una técnica compleja que requiere una planificación cuidadosa. Sin embargo, puede ser una herramienta valiosa para los administradores de redes que desean mejorar la eficiencia y el rendimiento de sus redes.

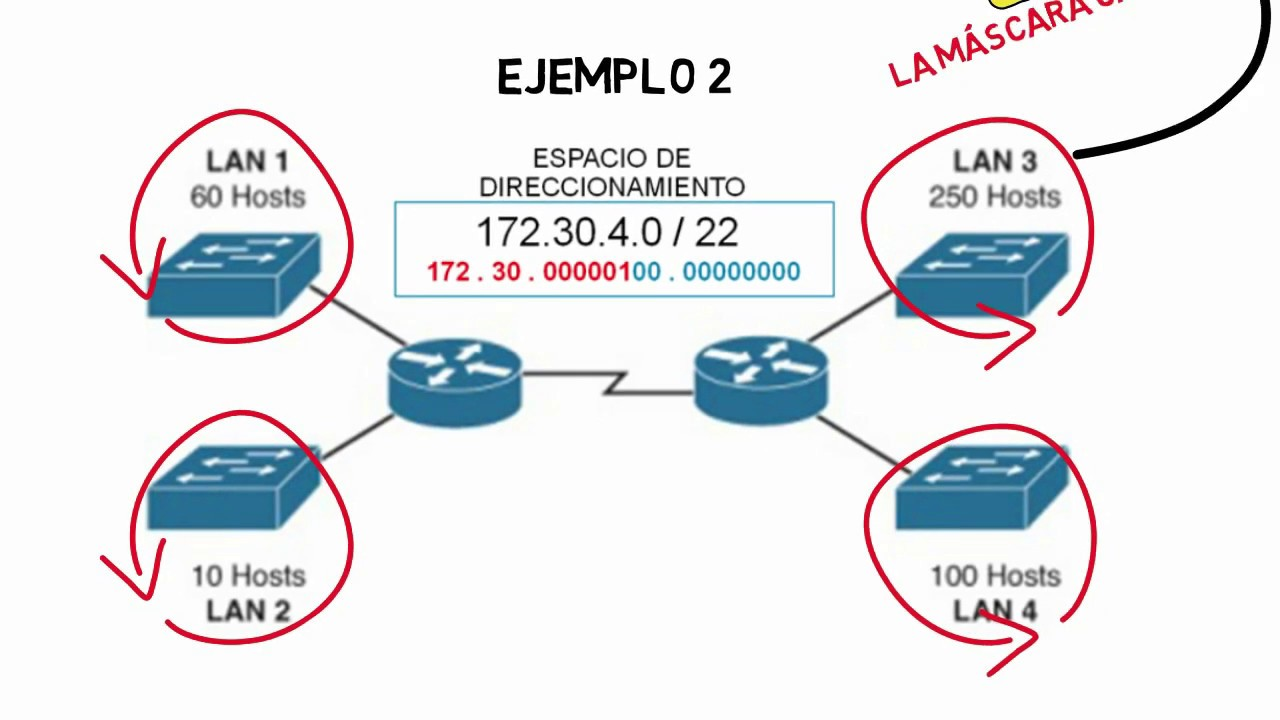
Aquí hay algunos ejemplos de cómo se puede utilizar el VLSM:

Una empresa puede utilizar el VLSM para asignar subredes de tamaño variable a sus diferentes oficinas. Esto puede ayudar a garantizar que cada oficina tenga la cantidad adecuada de direcciones IP y que los hosts en cada oficina puedan comunicarse entre sí de manera eficiente.

Un proveedor de servicios de Internet (ISP) puede utilizar el VLSM para asignar subredes de tamaño variable a sus clientes. Esto puede ayudar a garantizar que cada cliente tenga la cantidad adecuada de direcciones IP y que sus hosts puedan comunicarse con otros clientes de manera eficiente.

Una organización gubernamental puede utilizar el VLSM para asignar subredes de tamaño variable a sus diferentes departamentos. Esto puede ayudar a mejorar la seguridad y el control de acceso a los datos.





1.1.2. Direccionamiento sin clase (CIDR).

El direccionamiento sin clase (CIDR) es un método para asignar direcciones IP que mejora la eficiencia del enrutamiento de datos en Internet. En el direccionamiento sin clase, las direcciones IP se dividen en redes y subredes. Las redes son grupos de dispositivos que se pueden alcanzar entre sí directamente, mientras que las subredes son subdivisiones de una red que se pueden utilizar para mejorar la seguridad y el rendimiento.

El direccionamiento sin clase se introdujo en 1993 para resolver los problemas de agotamiento de direcciones IP que estaban ocurriendo en ese momento. El sistema de direccionamiento anterior, conocido como direccionamiento con clase, asignaba direcciones IP en función de tres clases: A, B y C. Las direcciones de clase A se asignaban a grandes redes, las direcciones de clase B se asignaban a redes de tamaño mediano y las direcciones de clase C se asignaban a redes pequeñas.

El direccionamiento sin clase elimina el concepto de clases de direcciones y permite que las direcciones IP se asignen de forma más flexible. Esto ayuda a evitar el agotamiento de direcciones IP y permite que más dispositivos se conecten a Internet.

Las direcciones CIDR se expresan en forma de notación CIDR, que es una combinación de la dirección IP y la máscara de subred. La máscara de subred indica cuántos bits de la dirección IP se utilizan para identificar la red y cuántos se utilizan para identificar los hosts de la red.

Por ejemplo, la dirección CIDR 192.168.1.0/24 indica que la dirección IP es 192.168.1.0 y la máscara de subred es 255.255.255.0. Esto significa que los primeros 24 bits de la dirección IP identifican la red y los últimos 8 bits identifican los hosts de la red.

El direccionamiento sin clase ofrece una serie de ventajas sobre el direccionamiento con clase, incluidas:

Mayor eficiencia del enrutamiento

Menor probabilidad de agotamiento de direcciones IP

Mayor flexibilidad en la asignación de direcciones IP

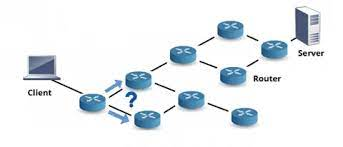
El direccionamiento sin clase es el método de direccionamiento IP estándar en la actualidad y se utiliza en todas las redes de Internet.

# Semana 2 – Unidad 1 - Enrutamiento estático y dinámico.

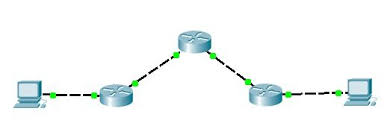
28, 30 y 31 de agosto.

Enrutamiento estático y dinámico (vector-distancia, de enlace).

El enrutamiento es el proceso de determinar la mejor ruta para enviar paquetes de datos a través de una red. Los routers son dispositivos de red que se utilizan para enrutar paquetes de datos. Los routers utilizan tablas de enrutamiento para almacenar información sobre las redes a las que están conectados. Cuando un router recibe un paquete de datos, consulta su tabla de enrutamiento para encontrar la mejor ruta para enviar el paquete al destino.



El enrutamiento es un proceso importante para garantizar que los paquetes de datos se entreguen correctamente a su destino. Sin enrutamiento, los paquetes de datos se perderían o se entregarían a la ruta incorrecta.

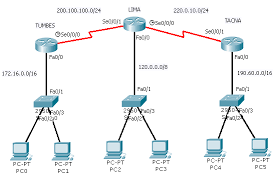


Hay dos tipos principales de enrutamiento: estático y dinámico.

Enrutamiento estático: El enrutamiento estático es un método simple y eficiente para el enrutamiento de paquetes de datos. En el enrutamiento estático, el administrador de la red configura manualmente las rutas en los routers. Esto significa que el router conoce la ruta óptima para enviar paquetes a cualquier red de destino.

Enrutamiento dinámico: El enrutamiento dinámico es un método más complejo y eficiente para el enrutamiento de paquetes de datos. En el enrutamiento dinámico, los routers intercambian información de enrutamiento entre sí. Esto permite a los routers aprender la topología de la red y determinar la mejor ruta para enviar paquetes a cualquier red de destino.

Los protocolos de enrutamiento son conjuntos de reglas que especifican cómo los routers intercambian información de enrutamiento. Hay muchos protocolos de enrutamiento diferentes disponibles, cada uno con sus propias ventajas y desventajas.



Algunos de los protocolos de enrutamiento más comunes incluyen:

RIP (Routing Information Protocol): RIP es un protocolo de enrutamiento vector distancia simple. RIP utiliza un algoritmo de Bellman-Ford para determinar la mejor ruta para enviar paquetes a cualquier red de destino.

OSPF (Open Shortest Path First): OSPF es un protocolo de enrutamiento vector distancia. OSPF utiliza un algoritmo de Dijkstra para determinar la mejor ruta para enviar paquetes a cualquier red de destino.

BGP (Border Gateway Protocol): BGP es un protocolo de enrutamiento exterior. BGP se utiliza para intercambiar información de enrutamiento entre redes que no están directamente conectadas.

El enrutamiento es un proceso fundamental para el funcionamiento de Internet. Sin enrutamiento, no sería posible enviar paquetes de datos de un dispositivo a otro en Internet.

El enrutamiento estático y el dinámico son dos métodos diferentes para determinar la mejor ruta para enviar paquetes de datos a través de una red.

Enrutamiento estático

El enrutamiento estático es un método simple y eficiente para el enrutamiento de paquetes de datos. En el enrutamiento estático, el administrador de la red configura manualmente las rutas en los routers. Esto significa que el router conoce la ruta óptima para enviar paquetes a cualquier red de destino.

El enrutamiento estático tiene una serie de ventajas, incluidas:

Es simple y fácil de configurar.

Es eficiente, ya que no requiere que los routers intercambien información de enrutamiento.

Es seguro, ya que las rutas no cambian a menos que el administrador de la red las actualice manualmente.

Sin embargo, el enrutamiento estático también tiene algunas desventajas, incluidas:

No se ajusta a los cambios en la topología de la red.

No puede utilizar los mejores caminos disponibles.

Enrutamiento dinámico

El enrutamiento dinámico es un método más complejo y eficiente para el enrutamiento de paquetes de datos. En el enrutamiento dinámico, los routers intercambian información de enrutamiento entre sí. Esto permite a los routers aprender la topología de la red y determinar la mejor ruta para enviar paquetes a cualquier red de destino.

El enrutamiento dinámico tiene una serie de ventajas, incluidas:

Se ajusta a los cambios en la topología de la red.

Puede utilizar los mejores caminos disponibles.

Es escalable, ya que puede soportar redes grandes y complejas.

Sin embargo, el enrutamiento dinámico también tiene algunas desventajas, incluidas:

Es más complejo que el enrutamiento estático.

Requiere más recursos de los routers.

Puede ser menos seguro que el enrutamiento estático.

Protocolos de enrutamiento dinámico

Hay muchos protocolos de enrutamiento dinámico diferentes disponibles. Algunos de los protocolos de enrutamiento dinámico más comunes incluyen:

OSPF (Open Shortest Path First): OSPF es un protocolo de enrutamiento vector distancia. OSPF utiliza un algoritmo de Dijkstra para determinar la mejor ruta para enviar paquetes a cualquier red de destino.

BGP (Border Gateway Protocol): BGP es un protocolo de enrutamiento exterior. BGP se utiliza para intercambiar información de enrutamiento entre redes que no están directamente conectadas.

RIP (Routing Information Protocol): RIP es un protocolo de enrutamiento vector distancia simple. RIP utiliza un algoritmo de Bellman-Ford para determinar la mejor ruta para enviar paquetes a cualquier red de destino.

Enrutamiento de vector distancia

Los protocolos de enrutamiento vector distancia son un tipo de protocolo de enrutamiento dinámico que utiliza una tabla de enrutamiento para almacenar la información de enrutamiento. La tabla de enrutamiento contiene una lista de redes de destino, la distancia a cada red y el siguiente salto para llegar a cada red.

Los protocolos de enrutamiento vector distancia actualizan sus tablas de enrutamiento de forma periódica. Cuando un router recibe una actualización de enrutamiento, actualiza su tabla de enrutamiento con la información de enrutamiento nueva o actualizada.



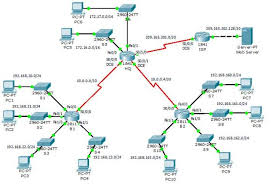
Enrutamiento de estado de enlace

Los protocolos de enrutamiento de estado de enlace son un tipo de protocolo de enrutamiento dinámico que utiliza una base de datos de estado de enlace para almacenar la información de enrutamiento. La base de datos de estado de enlace contiene una lista de enlaces entre routers, la capacidad de cada enlace y el estado de cada enlace.

Los protocolos de enrutamiento de estado de enlace actualizan sus bases de datos de estado de enlace de forma periódica. Cuando un router recibe una actualización de estado de enlace, actualiza su base de datos de estado de enlace con la información de estado de enlace nueva o actualizada.

Enrutamiento estático vs. dinámico

El enrutamiento estático y el dinámico son dos métodos diferentes para determinar la mejor ruta para enviar paquetes de datos a través de una red. El enrutamiento estático es simple y eficiente, pero no se ajusta a los cambios en la topología de la red. El enrutamiento dinámico es más complejo y eficiente, pero requiere más recursos de los routers.



# Semana 3 – Unidad 1 – Router RIP.

04, 06 y 07 de septiembre.

Router RIP

El Router RIP es un protocolo de enrutamiento dinámico que utiliza el conteo de saltos como su métrica principal. RIP se utiliza para compartir información de enrutamiento entre routers en una red IP.

RIP es un protocolo de vector distancia, lo que significa que cada router mantiene una tabla de enrutamiento que enumera las rutas a redes remotas. La tabla de enrutamiento se actualiza periódicamente a medida que los routers intercambian información entre sí.

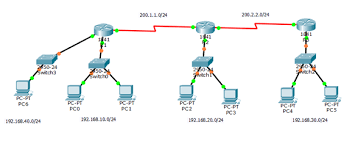
El conteo de saltos es la métrica utilizada por RIP para determinar la mejor ruta a una red remota. El router con el menor número de saltos al destino se considera la mejor ruta.

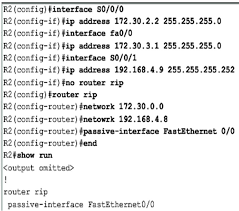
RIP tiene un límite de 15 saltos. Esto significa que un paquete IP no puede viajar más de 15 routers para llegar a su destino. Si un paquete debe viajar más de 15 routers, se considera inalcanzable.

RIP se utiliza a menudo en redes pequeñas y medianas. No es adecuado para redes grandes o complejas, ya que no puede manejar grandes cantidades de tráfico o cambios frecuentes en la topología de la red.

En la actualidad, RIP está siendo reemplazado por protocolos de enrutamiento más eficientes, como OSPF o EIGRP. Sin embargo, RIP todavía se utiliza en algunas redes pequeñas y medianas, donde la simplicidad y facilidad de configuración son más importantes que el rendimiento.

En resumen, el Router RIP es un protocolo de enrutamiento dinámico que utiliza el conteo de saltos como su métrica principal. RIP es adecuado para redes pequeñas y medianas, pero no para redes grandes o complejas.





# Semana 4 – Unidad 1 – Clasificación de Señales.

11, 13, 14 de septiembre

Las señales se pueden clasificar de diversas maneras según sus propiedades y características. Aquí te presento una clasificación básica de señales:

Por su naturaleza:

Señales analógicas: Representan información de manera continua en el tiempo y pueden tomar cualquier valor dentro de un rango determinado. Ejemplos incluyen señales de audio y voltajes eléctricos en circuitos analógicos.

Señales digitales: Representan información en forma discreta, generalmente en forma de 0 y 1 (bits). Ejemplos incluyen señales binarias en sistemas digitales y datos almacenados en computadoras.

Por su dominio:

Señales en el dominio del tiempo: La información se representa en función del tiempo. Esto es común en señales analógicas como las señales de audio.

Señales en el dominio de la frecuencia: La información se representa en función de la frecuencia. Esto implica transformar una señal en el dominio del tiempo en el dominio de la frecuencia mediante transformadas como la Transformada de Fourier. Esto se utiliza en análisis de espectro de señales.

Por su periodicidad:

Señales periódicas: Se repiten a intervalos regulares de tiempo. Ejemplos incluyen señales sinusoidales y muchas señales de naturaleza cíclica.

Señales aperiódicas (no periódicas): No tienen un patrón regular de repetición. Ejemplos incluyen ruido aleatorio y señales transitorias.

Por su simetría:

Señales simétricas: Tienen simetría en relación con un punto o un eje. Por ejemplo, una señal coseno es simétrica respecto a su punto medio.

Señales asimétricas (antisimétricas): No tienen simetría en relación con un punto o un eje. Por ejemplo, una señal diente de sierra es asimétrica.

Por su amplitud:

Señales de banda base: Tienen amplitudes que varían continuamente dentro de un rango específico. Ejemplos incluyen señales de audio.

Señales moduladas: Tienen una portadora que se modula en amplitud, frecuencia o fase para transportar información. Ejemplos incluyen señales de radio FM y AM.

Por su energía o potencia:

Señales de energía finita: Tienen una energía total finita y suelen ser señales de duración limitada en el tiempo.

Señales de potencia finita: Tienen una potencia promedio finita y pueden ser señales que se extienden infinitamente en el tiempo.

Por su dirección:

Señales unidireccionales: Se propagan en una sola dirección. Ejemplos incluyen señales de radio o TV que se transmiten desde una estación emisora hacia receptores.

Señales bidireccionales: Se propagan en ambas direcciones. Ejemplos incluyen comunicaciones bidireccionales como llamadas telefónicas.

Estas son algunas de las formas en que las señales se pueden clasificar. La elección de la clasificación depende de la aplicación específica y las propiedades que se deseen analizar o utilizar en un sistema particular.

Señales Analógicas, digitales, eléctricas y ópticas.

Las señales pueden clasificarse en función de su naturaleza (analógicas o digitales) y su medio de transmisión (eléctricas u ópticas). Aquí tienes una descripción de estas cuatro categorías:

Señales Analógicas Eléctricas:

Naturaleza Analógica: Las señales analógicas son continuas en el tiempo y pueden tomar cualquier valor dentro de un rango específico. Esto significa que pueden variar su amplitud de manera suave y continua.

Medio Eléctrico: Estas señales se transmiten a través de corrientes eléctricas o voltajes en circuitos eléctricos. Ejemplos comunes incluyen señales de audio en un cable de audio analógico o señales eléctricas en un sensor de temperatura analógico.

Señales Digitales Eléctricas:

Naturaleza Digital: Las señales digitales son discretas en el tiempo y se representan mediante valores discretos, generalmente 0 y 1 (bits). No tienen variaciones suaves y continuas.

Medio Eléctrico: Estas señales se transmiten a través de cambios en voltajes o corrientes eléctricas que representan los valores binarios. Ejemplos incluyen señales digitales en circuitos integrados, redes de computadoras y sistemas de comunicación digital.

Señales Analógicas Ópticas:

Naturaleza Analógica: Al igual que las señales analógicas eléctricas, las señales analógicas ópticas son continuas en el tiempo y pueden variar su intensidad de manera continua.

Medio Óptico: Estas señales se transmiten a través de pulsos de luz en medios ópticos, como fibras ópticas. Ejemplos incluyen señales de audio transmitidas como señales de luz a través de fibras ópticas.

Señales Digitales Ópticas:

Naturaleza Digital: Las señales digitales ópticas son discretas en el tiempo y se representan mediante pulsos de luz que pueden ser interpretados como 0 o 1 (bits).

Medio Óptico: Estas señales se transmiten utilizando pulsos de luz que representan datos binarios. Son comunes en sistemas de comunicación de alta velocidad, como redes de fibra óptica y en la transmisión de datos a largas distancias.

En resumen, las señales analógicas tienen una naturaleza continua y pueden tomar cualquier valor en un rango dado, mientras que las señales digitales son discretas y representan información en forma de bits. Además, estas señales pueden ser transmitidas a través de medios eléctricos (como cables o circuitos) o medios ópticos (como fibras ópticas o señales de luz). La elección entre señales analógicas y digitales y entre medios eléctricos u ópticos depende de la aplicación y las necesidades específicas de transmisión y procesamiento de datos.

## Examen unidad 1:

# Semana 5 – Unidad 2 – Segmentación de dominio de colisión y broadcast

18, 20, 21 Septiembre

# Segmentación de dominio de colisión y broadcast

La segmentación de dominio de colisión y la difusión (broadcast) son dos conceptos relacionados con las redes de computadoras y la forma en que los dispositivos de red se comunican entre sí. Estos conceptos se originan en las redes Ethernet, que han sido ampliamente utilizadas en entornos de redes locales (LAN) y se basan en el protocolo de acceso múltiple con detección de portadora y detección de colisiones (CSMA/CD).

Segmentación de dominio de colisión (Collision Domain): Un dominio de colisión es un segmento o parte de una red en la que varios dispositivos compiten por el acceso al medio de transmisión compartido. En una red Ethernet tradicional, todos los dispositivos conectados a un segmento (por ejemplo, un cable compartido o un concentrador) están en el mismo dominio de colisión. Esto significa que si dos dispositivos transmiten datos al mismo tiempo en ese segmento, se produce una colisión y ambos deben volver a intentar la transmisión después de un período de espera aleatorio. La segmentación de dominio de colisión implica dividir la red en segmentos más pequeños o utilizar conmutadores (switches) en lugar de concentradores (hubs) para reducir la cantidad de dispositivos en un dominio de colisión. Esto mejora la eficiencia y el rendimiento de la red al reducir la probabilidad de colisiones.

Difusión (Broadcast): La difusión es un método de comunicación en una red en el que un dispositivo envía un paquete de datos a todos los dispositivos en la red, sin importar su dirección MAC (dirección de control de acceso al medio). En Ethernet, la difusión se realiza utilizando la dirección MAC especial llamada "dirección de difusión" (broadcast address), que es una dirección en la que todos los bits son 1. Cuando un dispositivo envía un paquete a la dirección de difusión, todos los dispositivos en la misma red lo recibirán y procesarán. Esto se utiliza para fines como la resolución de direcciones IP en una red local (ARP, Address Resolution Protocol), donde un dispositivo necesita conocer la dirección MAC de otro dispositivo para comunicarse con él.

En resumen, la segmentación de dominio de colisión se refiere a la división de una red en segmentos más pequeños para reducir la probabilidad de colisiones, mientras que la difusión implica enviar datos a todos los dispositivos en una red. Ambos conceptos son importantes para comprender cómo funcionan las redes Ethernet y cómo se gestionan las comunicaciones en entornos compartidos.

Para conectar todos los dispositivos de red y clientes en una red, necesitas un switch capa 2. Este switch es esencial para la conexión de dispositivos. A medida que la diversidad de aplicaciones de red aumenta y se implementan redes convergentes, se vuelven necesarios switches más avanzados. Pongamos por ejemplo el switch capa 3:

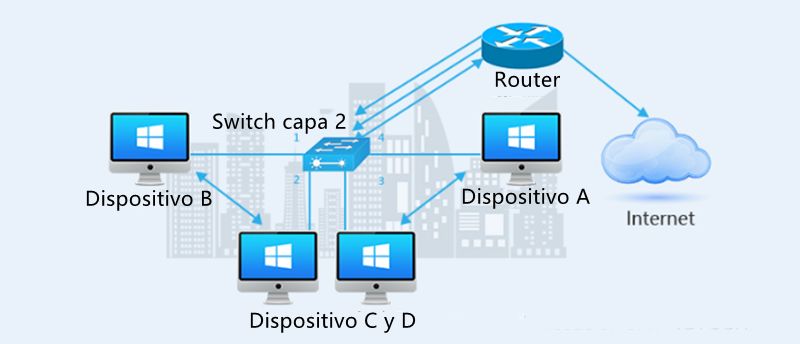
Este switch es cada vez más relevante en centros de procesamiento de datos, redes corporativas complejas, aplicaciones de negocios y proyectos sofisticados para clientes.

[](https://www.fs.com/es/products/108710.html?c_site=community_es&c_ctype=knowledge&c_from=picturelink&c_cat=BMCS230002-Enterprise_Switches-Wiki-ES&c_rel=21408)

## ¿Qué es el switch Capa 2?

El modelo OSI es un modelo de referencia para describir las comunicaciones de red. Para comprender el origen de los términos "Capa 2" o "Capa 3", es necesario revisar las especificaciones del modelo OSI (Open System Interconnection).

Las especificaciones están compuestas por siete capas: Capa física, Capa de enlace de datos, Capa de red, Capa de transporte, Capa de sesión, Capa de presentación y Capa de aplicación. Cuando digamos "Capa 2", nos referimos a la Capa de enlace de datos. Y cuando digamos "Capa 3", hablamos de la Capa de red.



La Capa 2 permite que los dispositivos en una red local (LAN) se comuniquen directamente entre sí. Un switch capa 2 facilita esta comunicación al utilizar una tabla de direcciones MAC. En esta tabla, el switch guarda las direcciones MAC de los dispositivos que ha identificado, junto con el puerto físico donde los vio por última vez.

Los paquetes de información se envían y reciben usando direcciones MAC solo dentro de la red LAN. Fuera de la LAN, estas direcciones no son reconocidas.

Además, un switch capa 2 tiene la capacidad de asignar VLANs (redes virtuales) a puertos específicos del switch. Esto permite que dispositivos en diferentes VLANs se comuniquen entre sí, incluso si están en subredes distintas en la Capa 3.

## ¿Cuál es el Switch Capa 3?

La Capa 3 se ocupa del enrutamiento de paquetes a través de direcciones lógicas y el control de subredes. Uno de los dispositivos más comunes en la Capa 3 es el router (también conocido como router). Este se encarga de dirigir los paquetes hacia sus respectivas direcciones IP (Protocolo de Internet).

En la Capa 3, se verifica la dirección IP de origen y destino de cada paquete. Esto se hace en la tabla de enrutamiento IP. Luego, se decide el siguiente paso en la ruta del paquete. Este puede ser hacia otro router o hacia un switch.

Si la dirección IP de destino no se encuentra en la tabla, el paquete se descarta a menos que haya una dirección IP predeterminada configurada. Por esta razón, el proceso de enrutamiento a menudo es sensible a la latencia.

Si quiere saber más, puede leer este artículo: [Switch capa 3 vs el router](https://community.fs.com/es/blog/layer-3-switch-vs-router-what-is-your-best-bet.html)

[](https://www.fs.com/es/products/69404.html?c_site=community_es&c_ctype=knowledge&c_from=picturelink&c_cat=BMCS230002-Enterprise_Switches-Wiki-ES&c_rel=21408)

Un switch capa 3, como se muestra en la imagen, también conocido como switch multicapa, combina algunas de las funciones de un switch capa 2 y las de un router. Estos tres dispositivos diferentes están diseñados para diversas aplicaciones y dependen en gran medida de las funciones que pueden ofrecer. A pesar de sus diferencias, comparten algunas similitudes en sus funciones.

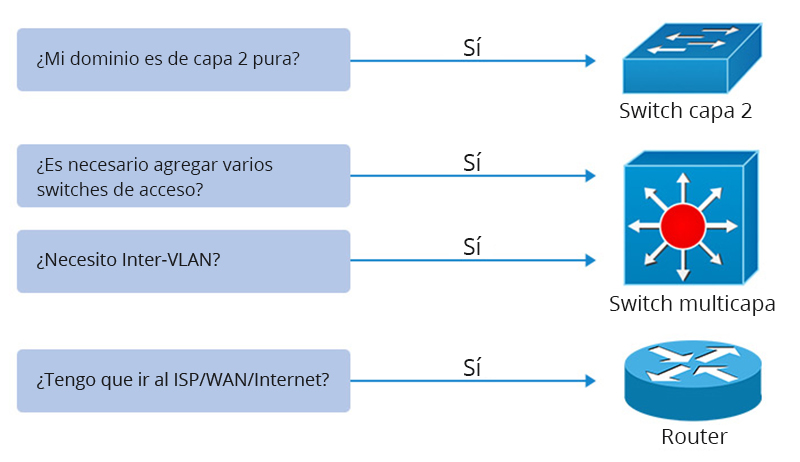
## La diferencia entre un switch capa 2 vs capa 3

La principal diferencia entre la Capa 2 y la Capa 3 se encuentra en su función de enrutamiento. Un switch de Capa 2 trabaja exclusivamente con direcciones MAC y no se preocupa por las [direcciones IP](https://community.fs.com/es/blog/know-ip-address-and-subnet-mask.html) ni otros elementos de niveles superiores.

Por otro lado, un switch capa 3 realiza todas las tareas de un switch capa 2, pero también puede llevar a cabo enrutamiento estático y dinámico.

En términos sencillos, un switch de capa 3 posee tanto una tabla de direcciones MAC como una tabla de rutas IP. Además de esto, controla la comunicación dentro de las VLAN y el enrutamiento de paquetes entre VLANs diferentes.

Un switch que solo agrega enrutamiento estático se conoce como "Layer 2+" o "Layer 3 Lite". Los switches capa 3 hacen más cosas y pueden entender la información de la dirección IP en los datos que pasan por el switch. Por ejemplo, pueden identificar el tráfico de VLAN utilizando la dirección IP en lugar de requerir configuraciones manuales en los puertos. En resumen, los switches capa 3 ofrecen mayor potencia y seguridad según sea necesario.



| **Modelo** | **Switch capa 2** | **Switch capa 3** |
| --- | --- | --- |
| Función de enrutamiento | Sólo Dirección Mac | Admite varios tipos de enrutamiento, como enrutamiento estático y enrutamiento dinámico |
| Etiquetado de VLAN basado en la dirección IP | No | Sí |
| Inter-VLAN | No | Sí |
| Escenas utilizanas | Capa 2 | Agregar switches de acceso múltiples |

## ¿ Cómo elegir entre un switch Capa 2 y un switch Capa 3?

### Consideraciones de uso inicial

Al momento de elegir entre un switch de Capa 2 y un switch capa 3, es importante pensar en el contexto del uso. Si tu red se basa principalmente en operaciones de Capa 2, como la conexión de servidores, un switch capa 2 es suficiente. Esto se conoce como la capa de acceso en la topología de red.

### Requerimientos de enrutamiento Inter-VLAN

Si necesitas que los dispositivos de diferentes grupos se comuniquen entre sí a través de diferentes VLANs, necesitará un switch capa 3. Esta función se encuentra en la capa de distribución en la topología de red.

### Comparación con routers

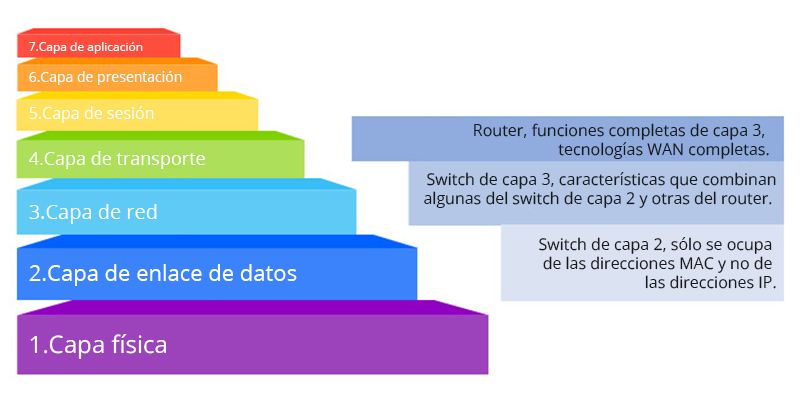
Si bien tanto los switches capa 3 como los routers pueden realizar enrutamiento, la elección entre ellos depende de tus necesidades específicas. No es tanto cuál es la mejor opción de enrutamiento en general, sino cuál es la más adecuada para la aplicación.

### Uso de switch capa 3

Si quieres conectar varias redes y permitir el enrutamiento entre ellas sin necesidad de rutas externas, el switch capa 3 es la mejor opción.

### Uso de router capa 3

Si necesitas enrutamiento hacia ISP o en entornos con funciones avanzadas de Capa 3, elige un router con más capacidad y funcionalidades de capa 3.



## ¿ Cómo comprar switches Capa 2 y switches Capa 3?

Si estás considerando la compra de un switch capa 2 vs capa 3, es importante tener en cuenta varios parámetros clave, como la velocidad de reenvío, el ancho de banda del backplane, el número de VLANs, la memoria de la dirección MAC y la latencia.

### Velocidad de Reenvío (Throughput)

La velocidad de reenvío, también conocida como tasa de rendimiento, se refiere a la capacidad de reenvío de un backplane o tejido de conmutación. Cuando esta capacidad de reenvío es mayor que la suma de las velocidades de todos los puertos, se considera un backplane no bloqueante. La velocidad de reenvío se mide en paquetes por segundo (pps). Puede calcularse utilizando la siguiente fórmula:

Velocidad de Reenvío (pps) = Número de Puertos de 10 Gbit/s \* 14.880.950 pps + Número de Puertos de 1 Gbit/s \* 1.488.095 pps + Número de Puertos de 100Mbit/s \* 148.809 pps.

### Ancho de Banda del Backplane (Switch Fabric)

El ancho de banda del backplane o la capacidad del tejido de conmutación es la suma de las velocidades de todos los puertos. Esta suma se cuenta dos veces, una para la dirección de transmisión (Tx) y otra para la dirección de recepción (Rx). El ancho de banda del backplane se mide en bits por segundo (bps o bit/s) y se calcula de la siguiente manera:

Ancho de Banda del Backplane (bps) = Número de Puertos \* Velocidad de Datos del Puerto \* 2.

### Otros Parámetros Clave

* Número de VLANs: Este parámetro se refiere a la cantidad de VLANs que pueden configurarse. Normalmente, 1K (equivalente a 1024 VLANs) es suficiente para un switch de Capa 2, mientras que un switch de Capa 3 suele admitir alrededor de 4k (4096) VLANs.
* Memoria de la Tabla de Direcciones MAC: Indica la cantidad de direcciones MAC que un switch puede almacenar. Por lo general, se expresa en capacidades como 8k o 128k.
* Latencia: La latencia se refiere al tiempo de retraso que experimenta una transferencia de datos. En general, se busca que la latencia sea lo más baja posible y se mide en nanosegundos (ns).

Es importante considerar estos parámetros al elegir un switch capa 2 o capa 3 para asegurarte de que se ajuste a tus necesidades de red.

## Resumen

En este artículo, hemos explicado las características de los diagramas de las capas 2 y 3 y los dispositivos comunes utilizados en estas capas. Esto incluye el switch capa 2, el switch capa 3 y el router. Es importante destacar que no siempre el dispositivo más avanzado es la mejor opción. En su lugar, es esencial seleccionar el dispositivo más adecuado para tu aplicación específica.

# Semana 6 – Unidad 2 - Vlans

25, 27, 28 Septiembre

Las VLAN (Virtual LAN) son una tecnología de redes que permite segmentar una red física en múltiples redes lógicas separadas. Estas redes lógicas se crean para mejorar la administración, la seguridad y el rendimiento de una red. Las VLAN se utilizan comúnmente en entornos empresariales para dividir una red en grupos lógicos de dispositivos, incluso si están conectados a la misma infraestructura física.

Los tipos más comunes de VLAN son:

1. VLAN basada en puertos: En este tipo de VLAN, se asignan puertos específicos de un switch a una VLAN en función de la configuración del puerto. Los dispositivos conectados a estos puertos pertenecerán automáticamente a la VLAN correspondiente.

2. VLAN basada en etiquetas 802.1Q: En este enfoque, se utiliza el estándar IEEE 802.1Q para etiquetar los tráficos de red con información de VLAN. Cada trama de red incluye una etiqueta VLAN que indica a qué VLAN pertenece. Los switches y routers pueden interpretar estas etiquetas para enrutar y conmutar el tráfico de manera adecuada.

3. VLAN basada en IP: En lugar de asignar VLANs según puertos o etiquetas, se pueden configurar VLANs basadas en direcciones IP. Esto permite agrupar dispositivos en función de sus direcciones IP, lo que puede simplificar la administración de la red, especialmente en redes virtuales o en la nube.

4. VLAN de voz: Estas VLAN se utilizan para priorizar y segmentar el tráfico de voz en una red, lo que es crucial para la calidad de las llamadas VoIP (Voz sobre IP). Ayudan a garantizar que el tráfico de voz tenga prioridad sobre otros tipos de datos en la red.

5. VLAN de gestión: Estas VLAN se utilizan para la administración de dispositivos de red, como switches y routers. Ayudan a asegurar que el tráfico de administración de red esté separado del tráfico de datos normal para mejorar la seguridad y el control.

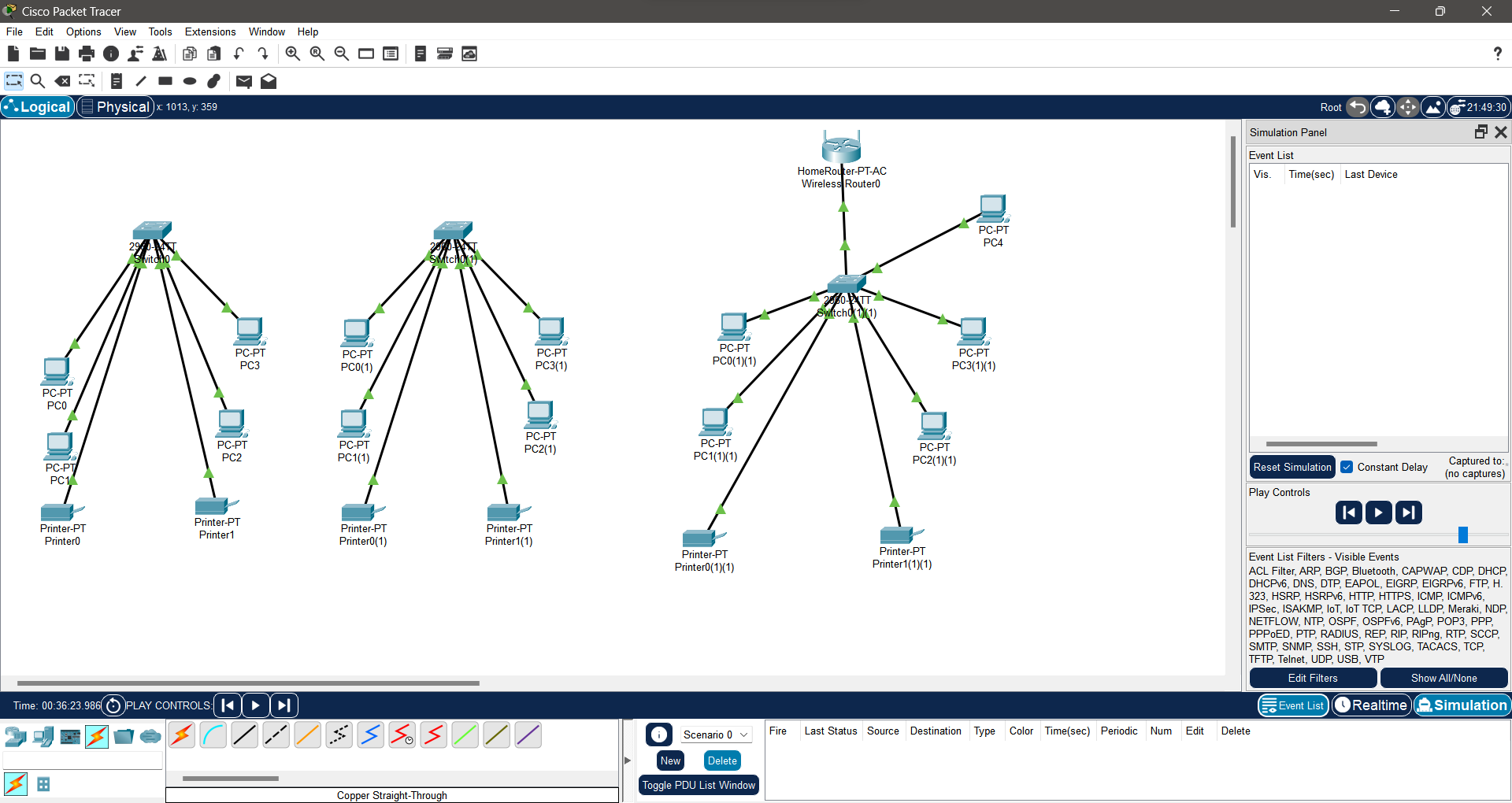
6. VLAN nativa: Cada trama 802.1Q tiene una VLAN nativa, que es la VLAN predeterminada a la que pertenecerá una trama si no tiene una etiqueta VLAN. Por lo general, se utiliza para el tráfico que ingresa o sale de la red VLAN etiquetada.

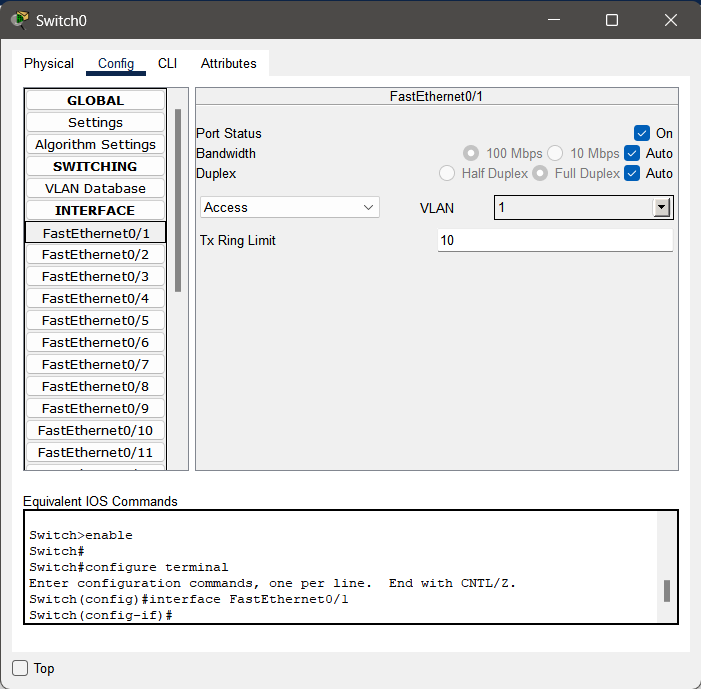
7. VLAN de invitados: Las VLAN de invitados se utilizan comúnmente en entornos empresariales o de hospitalidad para aislar el tráfico de los dispositivos de invitados de la red principal, proporcionando así seguridad y limitando el acceso a recursos críticos.

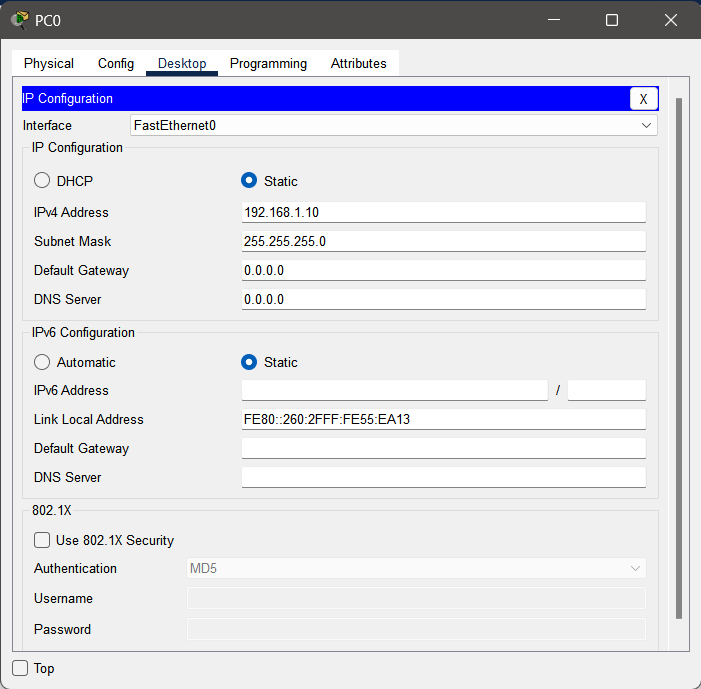
Estos son algunos de los tipos de VLAN más comunes, y las organizaciones pueden implementar varias VLANs según sus necesidades específicas para segmentar y gestionar eficazmente su tráfico de red.

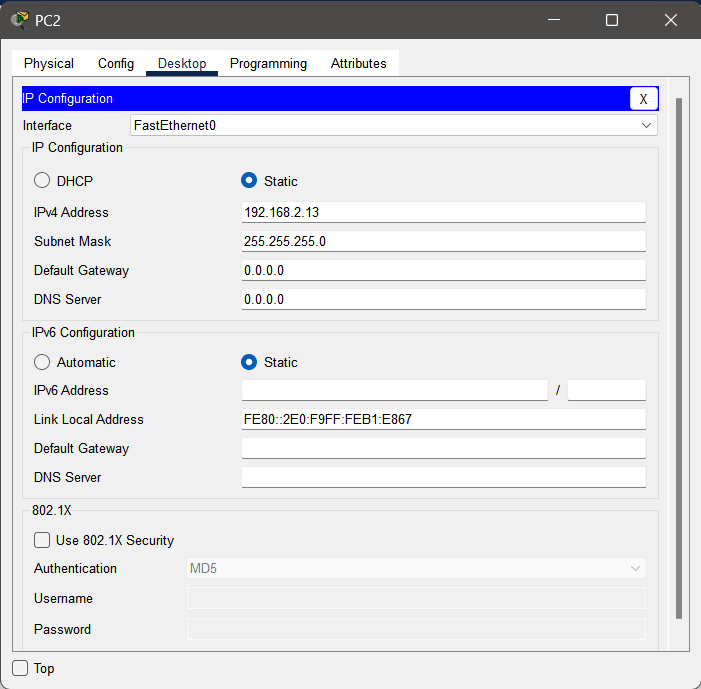
# Semana 7 – Unidad 2 – Vlans - Practica

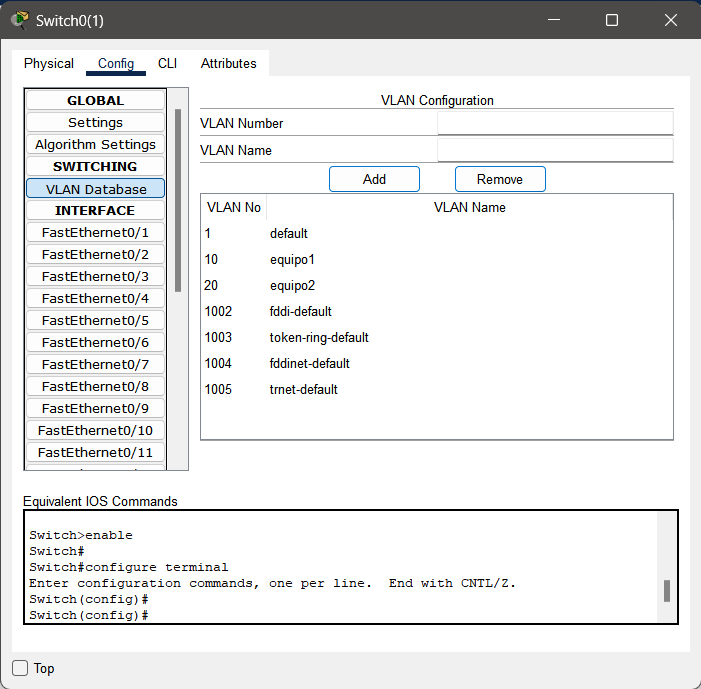
02, 04, 05 Octubre

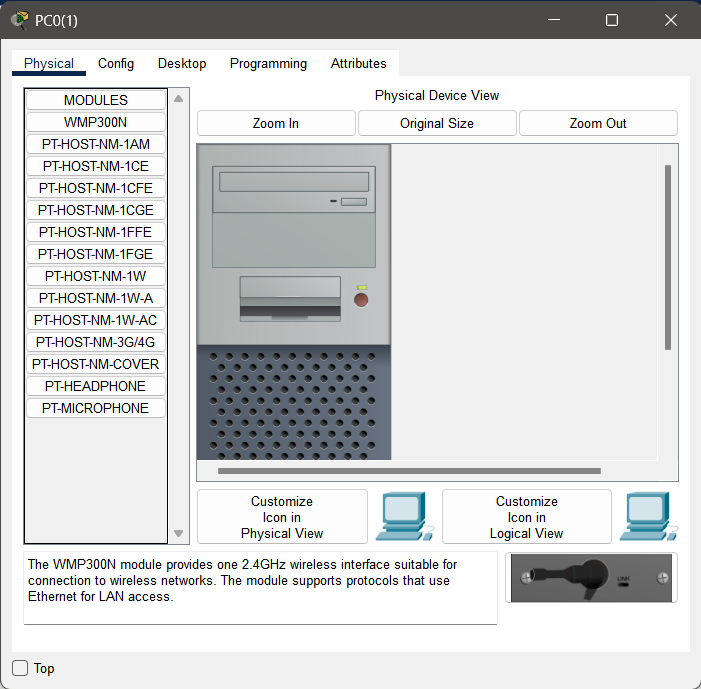


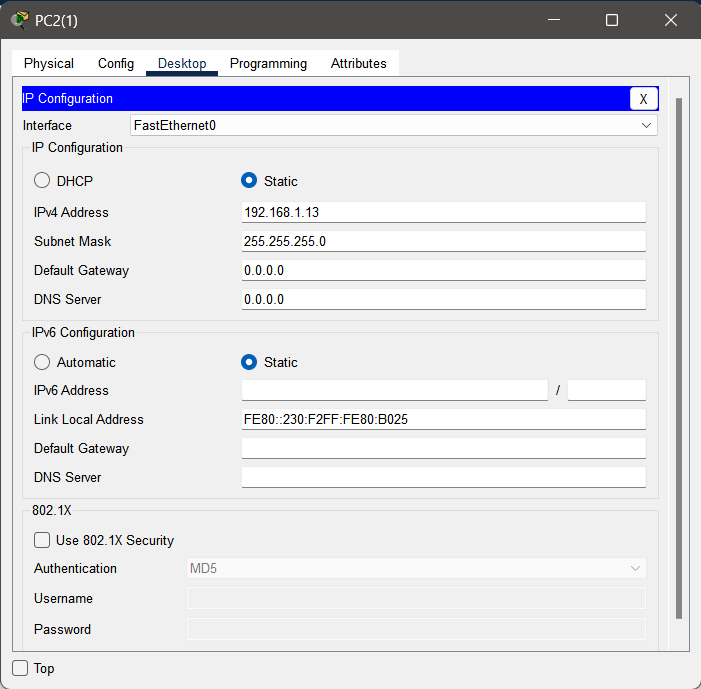


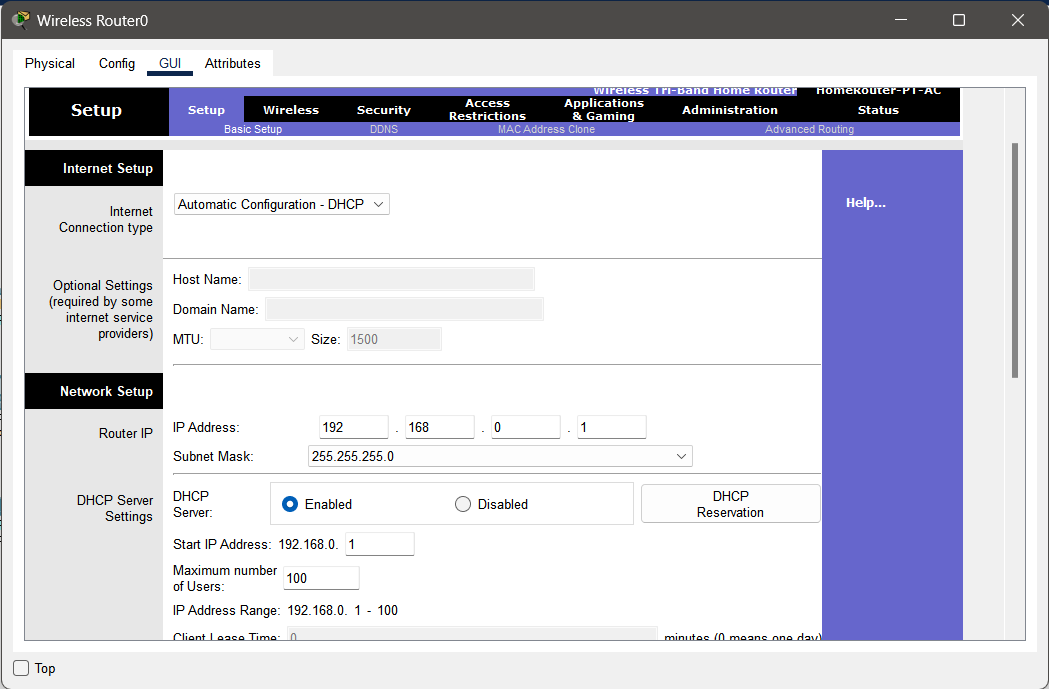


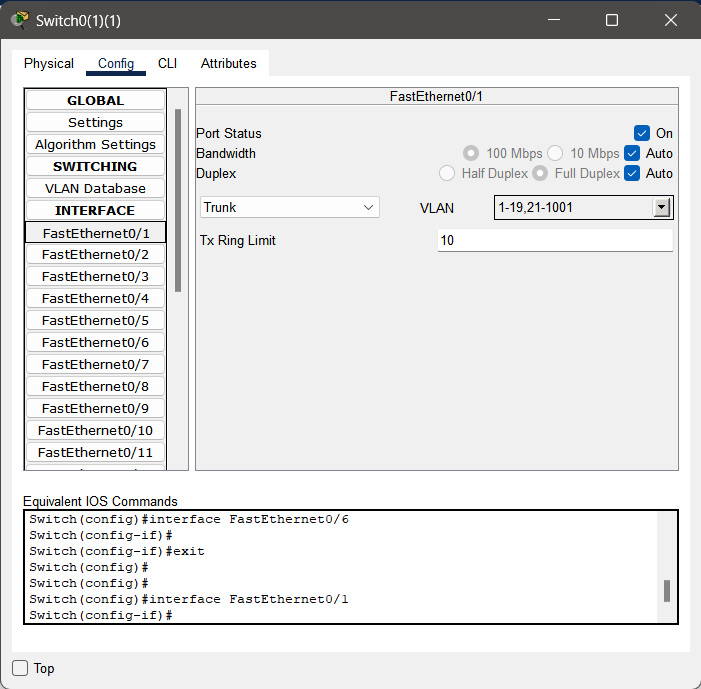












# Semana 8 – Unidad 2 – Vlans - Practica

09, 11, 12 Octubre

Tecnologías de conmutación (VLAN, VTP, STP)

La conmutación de redes es un componente esencial en el mundo de la tecnología de la información. Las redes modernas dependen de diversas tecnologías para garantizar que los datos se transmitan de manera eficiente y segura. Entre estas tecnologías, se encuentran las VLAN (Redes de Área Local Virtuales), VTP (Protocolo de Trunking VLAN) y STP (Spanning Tree Protocol). En este artículo, exploraremos estas tecnologías de conmutación y cómo contribuyen al funcionamiento óptimo de las redes.

Introducción a las Tecnologías de Conmutación

Las tecnologías de conmutación son fundamentales para la creación de redes eficientes y escalables. Permiten la segmentación de redes, el control de tráfico y la redundancia, lo que garantiza la disponibilidad de la red. Aquí, analizaremos las tres tecnologías clave: VLAN, VTP y STP.

VLAN: Redes de Área Local Virtuales

Las VLAN son una forma de segmentar una red física en múltiples redes lógicas. Esto se logra etiquetando los paquetes de datos con información adicional que indica a qué VLAN pertenecen. Las VLAN ofrecen varios beneficios:

1. Seguridad

Permiten aislar grupos de dispositivos, mejorando la seguridad al evitar el acceso no autorizado a ciertas partes de la red.

2. Eficiencia

Facilitan la administración al agrupar dispositivos con necesidades similares en una VLAN específica.

3. Escalabilidad

Las VLAN permiten expandir fácilmente la red sin necesidad de reconfigurar la infraestructura física.

VTP: Protocolo de Trunking VLAN

El Protocolo de Trunking VLAN (VTP) es una herramienta crucial en redes que utilizan VLAN. Su función principal es la sincronización automática de la información de VLAN entre dispositivos de red. Veamos sus ventajas:

4. Simplificación de la configuración

VTP reduce la necesidad de configurar manualmente cada switch de la red al propagar la información de VLAN automáticamente.

5. Evita errores humanos

Al minimizar la configuración manual, se reducen los errores de configuración, lo que mejora la estabilidad de la red.

6. Mayor eficiencia

VTP permite un despliegue más rápido de nuevas VLAN en toda la red.

STP: Spanning Tree Protocol

El Protocolo de Árbol de Expansión (STP) es una tecnología vital para prevenir bucles en la topología de red, lo que podría provocar un colapso en la comunicación. STP logra esto seleccionando el camino más eficiente para el tráfico y bloqueando otros caminos redundantes.

7. Redundancia segura

STP permite la redundancia en la red sin el riesgo de bucles, garantizando la continuidad de la comunicación incluso en caso de fallos.

8. Automatización

STP es una tecnología autónoma que selecciona automáticamente los caminos más eficientes sin intervención humana.

9. Estabilidad

Evita problemas de congestión y pérdida de datos al optimizar la ruta de los paquetes de datos.

Conclusión

En resumen, las tecnologías de conmutación, como las VLAN, VTP y STP, son fundamentales para la gestión eficiente y segura de las redes modernas. La segmentación de redes, la sincronización de VLAN y la prevención de bucles son aspectos críticos para garantizar un rendimiento óptimo de la red.

La segmentación del dominio de colisión y de broadcast son dos conceptos clave en redes de computadoras y se utilizan para mejorar el rendimiento y la eficiencia de la comunicación en una red. Aquí te explico cada uno de ellos:

1. \*\*Segmentación del Dominio de Colisión\*\*:

- \*\*Definición\*\*: Un dominio de colisión es un segmento de una red en la que varios dispositivos comparten el mismo medio físico de transmisión, como un cable Ethernet. Cuando dos dispositivos transmiten datos al mismo tiempo en un dominio de colisión, se produce una colisión y los datos se corrompen, lo que requiere una retransmisión.

- \*\*Segmentación\*\*: La segmentación del dominio de colisión implica dividir la red en segmentos más pequeños o dominios de colisión más pequeños. Esto se logra utilizando dispositivos como conmutadores (switches) en lugar de hubs. Los hubs retransmiten datos a todos los dispositivos en el segmento, lo que puede dar lugar a colisiones. Los conmutadores, por otro lado, analizan la dirección de destino de los datos y envían los datos solo al dispositivo correspondiente, lo que reduce las colisiones.

- \*\*Ventajas\*\*: La segmentación del dominio de colisión mejora el rendimiento y la eficiencia de la red al reducir las colisiones y permitir que varios dispositivos transmitan datos simultáneamente en diferentes segmentos sin interferencias.

2. \*\*Segmentación del Dominio de Broadcast\*\*:

- \*\*Definición\*\*: El dominio de broadcast se refiere a la porción de una red en la que los dispositivos pueden recibir y procesar paquetes de difusión (broadcast) enviados por otros dispositivos. Los paquetes de difusión son mensajes que se envían a todas las estaciones en la red. En redes grandes, el exceso de difusiones puede consumir ancho de banda innecesariamente.

- \*\*Segmentación\*\*: La segmentación del dominio de broadcast implica dividir la red en segmentos o dominios más pequeños utilizando enrutadores o subredes. Los enrutadores separan los dominios de broadcast y permiten un control más preciso sobre qué dispositivos pueden comunicarse entre sí.

- \*\*Ventajas\*\*: La segmentación del dominio de broadcast reduce la cantidad de tráfico de difusión que los dispositivos deben procesar y limita la propagación de paquetes de difusión innecesarios en toda la red. Esto mejora la eficiencia de la red y reduce la congestión.

En resumen, la segmentación del dominio de colisión y de broadcast son estrategias clave para optimizar el rendimiento y la eficiencia de las redes de computadoras. La segmentación del dominio de colisión se logra mediante el uso de conmutadores para reducir las colisiones, mientras que la segmentación del dominio de broadcast se logra mediante el uso de enrutadores para controlar y limitar la difusión de paquetes en la red.

## Examen Unidad 2:

# Semana 9 – Unidad 3 - Tecnologías WAN

16, 18, 19 octubre

## Redes Wan

Una Red de Área Amplia (WAN, por sus siglas en inglés, Wide Area Network) es una red de computadoras que cubre una amplia área geográfica, conectando múltiples redes locales (LAN) o dispositivos dispersos a lo largo de una región, un país o incluso a nivel mundial. Las WAN se utilizan para interconectar diferentes sitios geográficos, permitiendo la comunicación y el intercambio de datos entre ellos.

A continuación, te proporcionaré una introducción a las redes WAN destacando sus características y componentes clave:

\*\*Características de las WAN:\*\*

1. \*\*Gran Área Geográfica:\*\* Las WAN abarcan una amplia extensión geográfica, lo que las diferencia de las redes LAN que se limitan a un área más localizada.

2. \*\*Utilizan Infraestructura Pública y Privada:\*\* Las WAN pueden utilizar tanto infraestructura pública, como Internet, como redes privadas dedicadas. Las organizaciones pueden optar por una red WAN pública o construir su propia WAN privada según sus necesidades y requisitos de seguridad.

3. \*\*Enrutadores y Conmutadores:\*\* Los dispositivos como enrutadores y conmutadores desempeñan un papel fundamental en la gestión del tráfico en una WAN. Los enrutadores se utilizan para encaminar los datos entre diferentes redes, mientras que los conmutadores gestionan la conectividad dentro de una red local.

4. \*\*Topologías Variadas:\*\* Las WAN pueden tener diversas topologías, como estrella, malla, anillo o híbridos, dependiendo de la organización y sus necesidades.

5. \*\*Transmisión de Datos de Larga Distancia:\*\* Las WAN permiten la transmisión de datos a larga distancia, lo que las hace ideales para conectar sucursales de una empresa, oficinas remotas, data centers y usuarios ubicados en diferentes lugares geográficos.

\*\*Componentes Clave:\*\*

1. \*\*Nodos:\*\* Los nodos son puntos de conexión en una WAN, como computadoras, servidores, enrutadores o conmutadores, que permiten la transmisión de datos.

2. \*\*Medios de Transmisión:\*\* Los medios de transmisión incluyen cables de fibra óptica, cables coaxiales, líneas de teléfono, satélites y enlaces inalámbricos, que se utilizan para transportar datos a través de la WAN.

3. \*\*Protocolos de Comunicación:\*\* Para garantizar la comunicación efectiva en una WAN, se utilizan protocolos de comunicación, como el Protocolo de Internet (IP), para enrutar datos y el Protocolo de Control de Transmisión (TCP) para asegurar la entrega confiable de datos.

4. \*\*Dispositivos de Red:\*\* Los enrutadores, conmutadores, firewalls y gateways son dispositivos comunes en una WAN que facilitan la gestión del tráfico y la seguridad de la red.

5. \*\*Acceso a Internet y Proveedores de Servicios:\*\* En muchas WAN, el acceso a Internet es proporcionado por proveedores de servicios de Internet (ISP), que conectan la red local con el mundo exterior.

Las redes WAN son esenciales para la comunicación empresarial y la conectividad global. Permiten a las organizaciones compartir recursos, aplicaciones y datos de manera eficiente, lo que las convierte en una parte fundamental de la infraestructura tecnológica moderna.

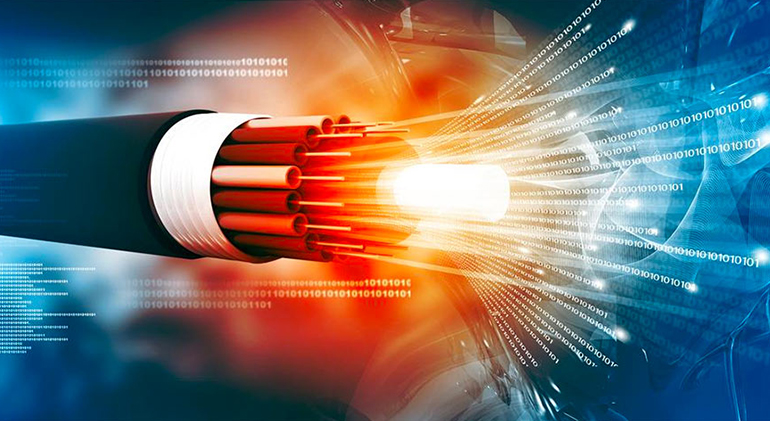
## Enlaces Dedicados

Los enlaces dedicados, ideales para empresas

En la actualidad, el mundo se mueve de manera digital. Cada vez es más necesario que las empresas tengan una conexión de internet estable, confiable y de alta velocidad y para eso existen los enlaces dedicados.

Seguramente has escuchado hablar alguna vez sobre este tipo de conexiones dedicada pero no sabes si este tipo de conexión a internet puede ser interesante para tu empresa.

A continuación, te contaremos todo lo que necesitas saber sobre este tipo de conexión avanzada para empresas, de manera que puedas usarla en tu negocio y olvidarte para siempre de los problemas de conexión a internet que hayas tenido hasta la fecha.



¿Qué son los enlaces dedicados?

Antes de continuar y mostrarte todas las ventajas de las líneas dedicadas es necesario que sepas bien qué son. De esa forma sabrás si es la solución ideal para tu negocio.

Los enlaces dedicados son un tipo de conexión a internet que permite a tu empresa estar conectada a la red global o internet de manera permanente, es decir, todas las horas de todos los días del año.

A diferencia de la conexión común de banda ancha, las líneas dedicadas no dependen de una conexión telefónica. Esta es una conexión directa y exclusiva entre el proveedor del servicio a internet y el cliente.

Las líneas dedicadas son directas y exclusivas entre el proveedor de internet y el cliente

Esto representa una gran ventaja. Ya que, a diferencia de una conexión de banda ancha, este tipo de internet para empresas garantiza una mayor seguridad y un porcentaje de problemas casi nulo.

¿Por qué necesitas un enlace dedicado?

Ahora que ya sabes de qué trata este tipo de conexión, seguramente te estarás preguntando: ¿por qué tu negocio necesita de un enlace dedicado de internet?

Las razones son múltiples y pueden variar dependiendo de cada caso pero, en general, muchas empresas deberían tener un servicio de internet dedicado. En especial, aquellas en las que el acceso a internet es crítico.

Empresas turísticas como hoteles o de servicios como bancos o gasolineras; así como aquellas que cuenten con varias sucursales conectadas, con tiendas online o plataformas de atención al público. Por no olvidar instituciones públicas o empresas privadas que solicitan datos personales; además de aseguradoras, empresas que emiten facturas en línea y un largo etcétera.

Estos son solo algunos ejemplos de empresas que deben usar una conexión dedicada para garantizar la continuidad de su negocio.

Sin embargo, estas no son las únicas compañias que pueden necesitar una conexión dedicada. Si la tuya cumple con alguna de las características que compartimos en el siguiente punto, seguramente lo mejor sea conseguir una conexión de internet por medio de los enlaces dedicados.

¿Cuáles son las características de las empresas que necesitan enlaces dedicados?

Necesitas compartir archivos de gran tamaño.

Estás constantemente subiendo y descargando archivos.

Tienes negocios internacionales y requieres tener videoconferencias con socios en todas partes del mundo.

El número de trabajadores conectados simultáneamente es alto y pueden colapsar cualquier red de banda ancha.

Compartes información confidencial entre áreas de la empresa y con el exterior.

Vendes a través de sistemas on-line.

Facturas a través de sistemas on-line.

Tratas datos personales de tus clientes de carácter privado.

Tienes varias sedes, sucursales o tiendas conectadas entre si por internet.

Cumplir con cualquiera de estas condiciones es suficiente para que tomes la decisión de usar una conexión con líneas dedicadas.

¿Qué ventajas traen los enlaces dedicados?

Este tipo de conexión de internet para empresas trae múltiples ventajas que tu negocio puede aprovechar.

Estabilidad en la conexión: Una de las mayores ventajas de los enlaces dedicados es la estabilidad que te proporcionan en el servicio. Contar con internet de calidad las 24 horas del día, los 365 días del año es algo primordial en la época actual.

Seguridad total: Al ser un tipo de red privada separada de la red de los otros clientes, es mucho menos probable que tu empresa sufra ataques de seguridad digital. Gracias a esto, los datos de tus productos, clientes y empleados van a estar muy seguros.

Mayor velocidad y ancho de banda: Vas a disfrutar de internet de alta velocidad. Lo que permitirá que puedas compartir archivos de gran tamaño, usar una VPN (red privada virtual) o transmitir streaming de video, es decir, videoconferencias de manera simultánea, con alta calidad de video, imagen fluida y sin cortes.

El control de la red: Este tipo de conexiones privadas son mucho más fáciles de monitorizar. Con esto, podrás tener un mayor control sobre el uso que le dan tus empleados a la red. De esta manera, la productividad en tu empresa aumentará.

Atención técnica por parte de especialistas: Por tratarse de una conexión de tipo Premium, desde ib-red ponemos a tu disposición técnicos altamente especializados con capacidad de respuesta y solución inmediata. De esta manera, tendrás la seguridad de que tu servicio siempre estará en funcionamiento y en las mejores manos.

# Semana 10 – Unidad 3 – Tecnologías WAN

23, 25, 26 octubre

## Enlaces dedicados: qué son y cómo funcionan

Un enlace dedicado es una conexión de red que se establece entre dos puntos específicos, sin compartirse con otros usuarios o dispositivos. Esto significa que el enlace tiene un ancho de banda garantizado y no está sujeto a las fluctuaciones de la carga de red.

Los enlaces dedicados se utilizan en una variedad de aplicaciones, que incluyen:

Comunicaciones empresariales

Servicios de transmisión de datos

Redes de área metropolitana (MAN)

Redes de área amplia (WAN)

Cómo funcionan los enlaces dedicados

Los enlaces dedicados se implementan utilizando una variedad de tecnologías, que incluyen:

Enlaces de fibra óptica

Enlaces de cobre

Enlaces inalámbricos

En el caso de los enlaces de fibra óptica, se utiliza un cable de fibra óptica para transportar los datos entre los dos puntos. Los enlaces de cobre utilizan cables de cobre para transportar los datos. Los enlaces inalámbricos utilizan ondas de radio para transportar los datos.

Ventajas de los enlaces dedicados

Los enlaces dedicados ofrecen una serie de ventajas sobre las conexiones de red compartidas, que incluyen:

Garantía de ancho de banda: El ancho de banda de un enlace dedicado está garantizado, lo que significa que los usuarios pueden esperar un rendimiento constante.

Fiabilidad: Los enlaces dedicados son más fiables que las conexiones de red compartidas, ya que no están sujetos a las fluctuaciones de la carga de red.

Seguridad: Los enlaces dedicados pueden ser más seguros que las conexiones de red compartidas, ya que el tráfico está cifrado.

Desventajas de los enlaces dedicados

Los enlaces dedicados también tienen algunas desventajas, que incluyen:

Costo: Los enlaces dedicados suelen ser más caros que las conexiones de red compartidas.

Disponibilidad: Los enlaces dedicados pueden no estar disponibles en todas las áreas.

Conclusión

Los enlaces dedicados son una opción de conexión de red ideal para aplicaciones que requieren un ancho de banda garantizado, fiabilidad y seguridad.

## Enlaces dedicados.

Un enlace dedicado es aquella conexión permanente que se lleva a cabo a través de líneas punto a punto. Uno de los beneficios que tenemos es que la empresa o casa particular que lo utiliza tiene acceso permanente a Internet.

Algo que si debemos tener muy en cuenta es que esta conexión es directa.

Pero, ¿qué queremos decir con esto?

Bueno que esta es exclusiva entre el cliente y el proveedor y por lo mismo no se comparte con otros usuarios.

Permitiéndonos administrar la comunicación desde cualquier servidor o puesto de trabajo.

Ventajas.

Las ventajas que nos puede ofrecer este tipo de servicio entre otras son que podemos tener conexión a [Internet](https://okhosting.com/blog/internet-satelital/) sin necesidad de tener líneas  de teléfono, que como dijimos al principio gozaremos del servicio de internet las 24 horas del día sin interrupción.

A la vez un punto muy importante es que contaremos con una velocidad 20 veces más rápida que una línea telefónica. Por lo mismo toda aquella aplicación que utilice la voz y el vídeo funcionara de forma óptima.

Velocidad simétrica.

Ahora hablemos un poco de su velocidad simétrica.

Para que puedas entender sus beneficios brevemente te explicaremos en que consiste.

Con esta modalidad contamos con la posibilidad de manejar una velocidad de subida y bajada similares, lo cual no podemos obtener con una conexión asimétrica ya que esta cuenta con una velocidad de descarga más alta que de subida. Entonces si lo que tú quieres es bajar/cargar o

compartir archivos de un tamaño extenso, hacer videos en directo sin problemas de calidad o de corte, trabajar de forma cómoda con una [VPN](https://okhosting.com/blog/virtual-host-servidores-virtuales-vpn/) y las VoIP, tu mejor opción es este tipo de red.

Imagina que tu como empresa o usuario tengas que por fuerza tener una conexión estable y segura las 24 horas del día los 365 días del año pues tu negocio depende de ello,  pero, de repente tu servicio cae por minutos o incluso horas. Seguramente será algo desastroso.

Pues todo este embrollo te lo puedes evitar utilizando la conexión enlace dedicado.

Además ofrece la posibilidad de instalar servidores Web, de [correo electrónico](https://okhosting.com/blog/3-razones-para-crear-correo-electronico/), tener sus propias páginas de Internet, etc.

De hecho es considerada una opción robusta, segura y confiable por lo mismo es la que más se requiere en cuanto a empresas e instituciones hablamos.

Enlace asimétrico.

Arriba te hablamos un poco de este sistema. En este no contamos con los mismos beneficios que el primero, puesto que aquí la velocidad de subida y bajada no es la misma.

Quedamos entonces en que la velocidad de descarga es superior a la de carga, y si hacemos o más bien intentamos bajar y cargar datos al mismo tiempo definitivamente experimentaremos lentitud en las dos acciones.

[](https://okhosting.com/resources/uploads/2019/03/enlaces-asimetricos.jpeg)

No obstante, este sigue siendo el sistema más utilizado. Puesto que no todos los usuarios necesitan de una velocidad rápida para subir archivos.

Sin embargo, no todo es malo.

Podemos contar con los siguientes beneficios:

Buena velocidad de descarga.

Cuidar de nuestra economía debido al precio del servicio.

Otra cosa es que tienen diferentes anchos de banda para cada línea de comunicación.  Esto es precisamente funcional cuando hacemos uso de [aplicaciones](https://okhosting.com/blog/tu-empresa-en-aplicaciones-moviles/) en Internet, puesto que trabajan con una cantidad de datos más grande en una línea que en otra.

Enlace punto a punto.

Este tipo de enlace se usa en un tipo de red específica.

¿Qué queremos decir con esto?

Pues que este canal de datos que utilizaremos solo es óptimo para que dos nodos se comuniquen.

Otra característica de este tipo de enlace es que en la red los nodos actúan como iguales no uno superior al otro. El único problema es que a medida de que las relaciones aumentan es más difícil llevar a cabo este sistema. Por qué el trabajo de administrar y operar se vuelve arduo y en algo punto ineficaz.

Ahora hay tres formas en las que se intercambian datos entre sí.

Simplex: Aquí la transmisión se hace de un solo lado.

Half-dúplex: Por otra parte la transmisión en half-dúplex es en ambos lados, pero no al mismo tiempo es decir que solo un lado puede enviar información. Así que en este caso uno se debe de convertir en transmisor y el otro debe recibir.

Full-dúplex: Al igual que en el de arriba podemos transmitirlo  en ambos lados. No obstante, aquí  podemos hacerlo de forma simultánea. Sin embargo tiene sus particularidades. Es decir en esta pueden implementarse las dos formas que están arriba.

Una empresa es un organismo que para ser productivo debe estar en constante crecimiento, sin embargo, esto también implica cambios en sus necesidades. Por lo mismo se deben de evaluar los objetivos que queremos alcanzar y que nuestras herramientas en este caso nuestra red nos ayude y no más bien nos complique las cosas.

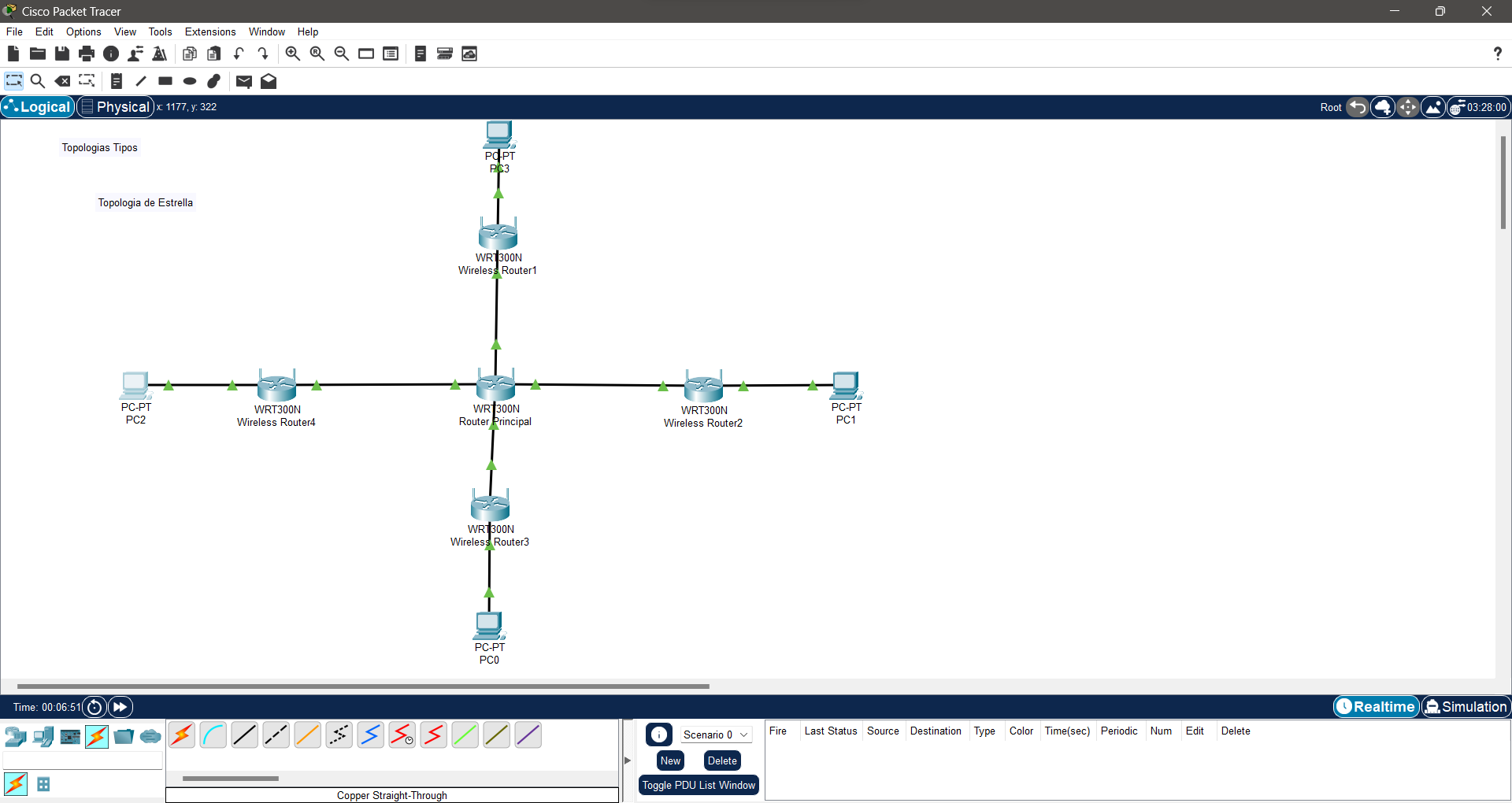
[](https://okhosting.com/resources/uploads/2019/03/empresas-redes-punto-a-punto.jpeg)

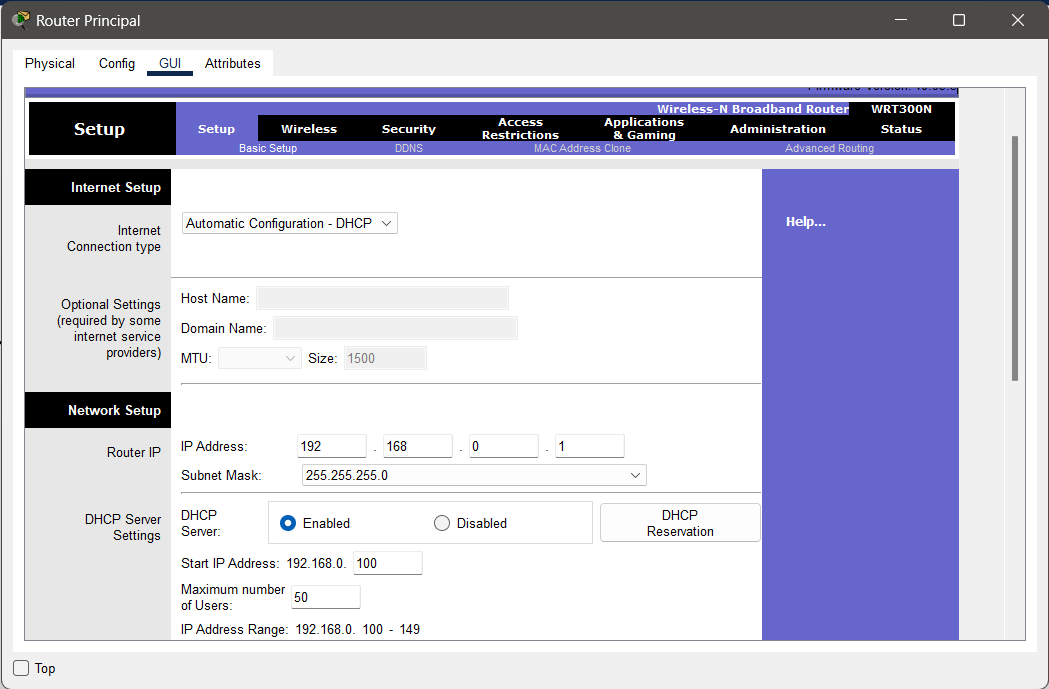
# Semana 11 – Unidad 3 –Topologías WAN.

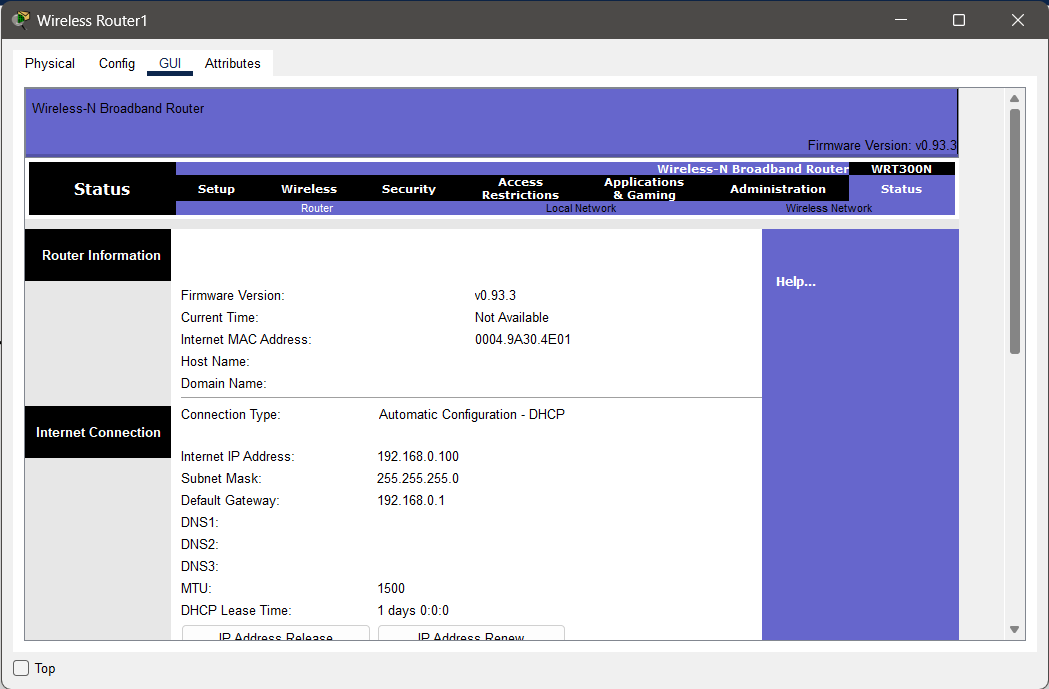
30, 1, 2 noviembre

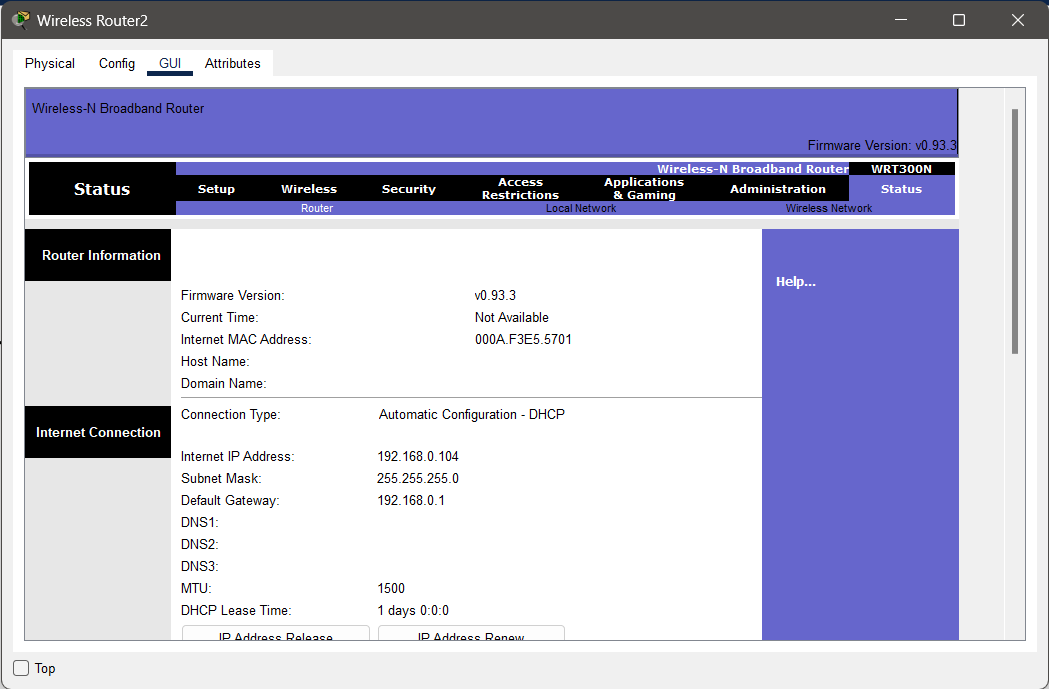
Las topologías WAN (Wide Area Network o Red de Área Amplia) se refieren a la forma en que se organizan y conectan las redes de área amplia para permitir la comunicación entre dispositivos y sitios geográficamente dispersos. A continuación, se describen algunas de las topologías WAN más comunes:

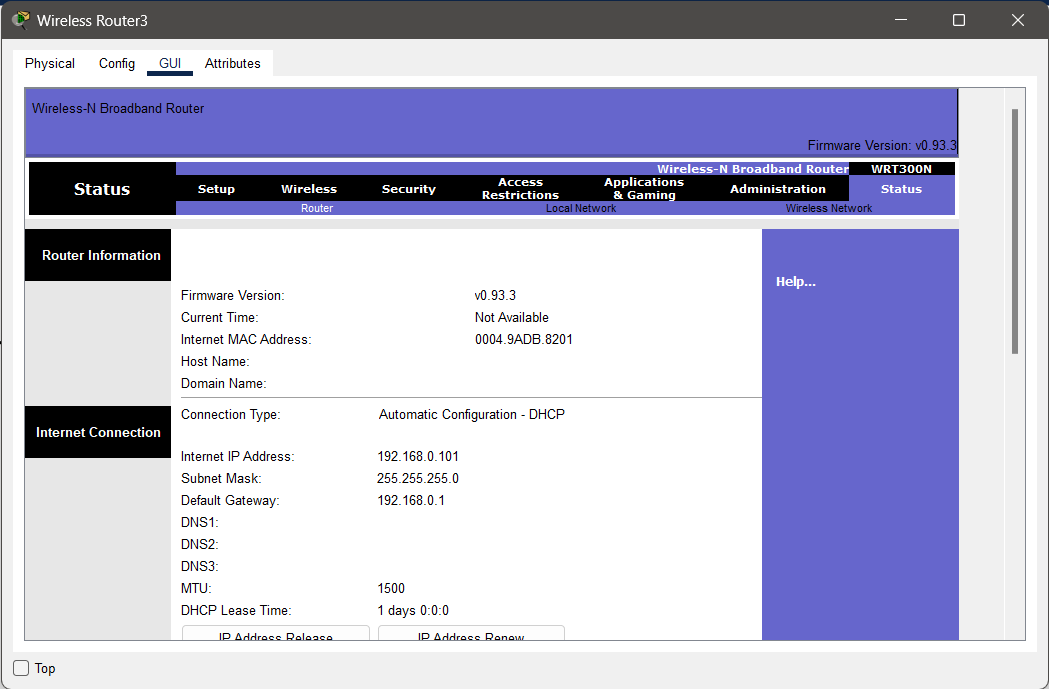
1. \*\*Topología de estrella:\*\* En una topología de estrella, todos los sitios o dispositivos en la WAN están conectados a un punto central, como un concentrador o un enrutador principal. Esta configuración facilita la administración y el control centralizados, pero si el concentrador central falla, toda la red puede verse afectada.

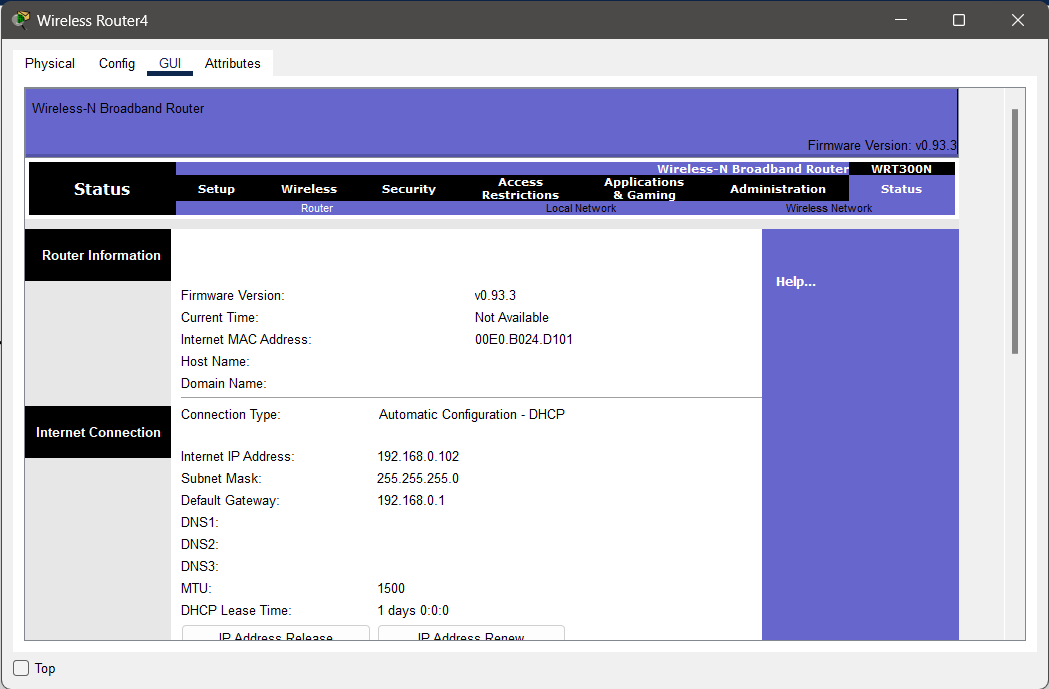


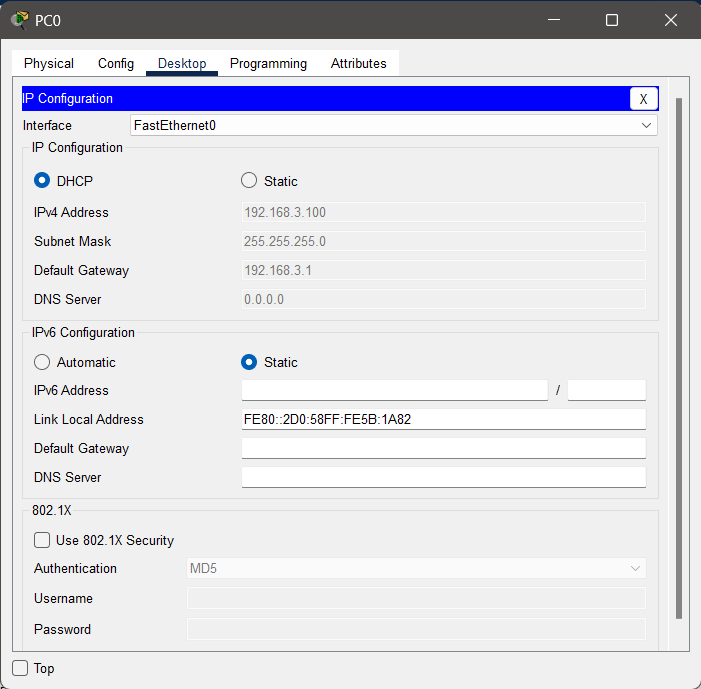












2. \*\*Topología de malla:\*\* En una topología de malla, todos los sitios están conectados entre sí. Cada sitio tiene una conexión directa con todos los demás sitios, lo que proporciona redundancia y resiliencia. Esta topología es costosa de implementar debido a la gran cantidad de conexiones necesarias, pero es altamente confiable.

3. \*\*Topología de anillo:\*\* En una topología de anillo, cada sitio está conectado al menos a otros dos sitios, formando un anillo de conexiones. Los datos se transmiten de un sitio a otro en una dirección circular. Si un enlace falla, la comunicación puede reenrutarse en la dirección opuesta. Esta topología es eficiente en cuanto a la cantidad de cableado necesario, pero una falla en el anillo puede interrumpir la comunicación.

4. \*\*Topología de árbol:\*\* En una topología de árbol, los sitios se organizan en una estructura jerárquica similar a un árbol. Hay un sitio raíz que se conecta a varios sitios secundarios, y cada sitio secundario puede a su vez conectar a sitios adicionales. Esta topología es escalable y permite la expansión de la red, pero la caída del nodo raíz puede afectar a todos los nodos descendientes.

5. \*\*Topología de bus:\*\* En una topología de bus, todos los sitios se conectan a una única línea principal de comunicación. Cada sitio puede comunicarse con los demás transmitiendo datos a través de la línea principal. Es una topología simple y económica, pero una falla en la línea principal puede afectar a toda la red.

6. \*\*Topología de punto a punto:\*\* En esta topología, cada sitio se conecta directamente a uno o varios otros sitios mediante enlaces dedicados. Es común en conexiones WAN de punto a punto, como conexiones de línea alquilada, y se utiliza para la comunicación exclusiva entre dos ubicaciones.

Cada topología WAN tiene sus propias ventajas y desventajas, y la elección de la topología depende de los requisitos de la red, la escalabilidad, la redundancia, el presupuesto y otros factores específicos de la organización. La combinación de estas topologías puede usarse para crear una red WAN que cumpla con los requisitos de conectividad de una organización.

# Semana 12 – Unidad 3 –Topologías WAN.

06, 7, 9 noviembre

Las tecnologías WAN (Wide Area Network) son fundamentales para conectar redes de área local (LAN) ubicadas en diferentes lugares geográficos. Aquí hay una breve descripción de algunas de las tecnologías WAN mencionadas:

1. \*\*PPP (Point-to-Point Protocol):\*\*

- \*\*Descripción:\*\* PPP es un protocolo de comunicación utilizado para establecer una conexión directa entre dos nodos. Es comúnmente utilizado para conectar un usuario a través de una línea telefónica a un ISP (Proveedor de Servicios de Internet).

- \*\*Características:\*\* Proporciona autenticación, compresión y encriptación de datos. Es versátil y puede ser utilizado sobre diversas interfaces, como líneas telefónicas, conexiones seriales y conexiones de banda ancha.

2. \*\*XDSL (Digital Subscriber Line):\*\*

- \*\*Descripción:\*\* XDSL es una familia de tecnologías de transmisión digital de datos a través de líneas telefónicas de cobre. Incluye variantes como ADSL (Asymmetric DSL), SDSL (Symmetric DSL) y VDSL (Very high-speed DSL).

- \*\*Características:\*\* Proporciona velocidades de transmisión asimétricas o simétricas, lo que significa que la velocidad de descarga puede ser diferente de la velocidad de carga. Es comúnmente utilizado para proporcionar servicios de banda ancha a usuarios domésticos y empresariales.

3. \*\*Frame Relay:\*\*

- \*\*Descripción:\*\* Frame Relay es un servicio de conmutación de paquetes utilizado en redes WAN. Permite la transmisión de datos en forma de "frames" (tramas) a través de una red conmutada.

- \*\*Características:\*\* Ofrece una conexión virtual permanente entre los nodos y utiliza la conmutación de paquetes para el transporte de datos. Fue ampliamente utilizado en el pasado, pero ha sido en gran medida reemplazado por tecnologías más modernas, como MPLS.

4. \*\*ISDN (Integrated Services Digital Network):\*\*

- \*\*Descripción:\*\* ISDN es una tecnología de comunicación digital que utiliza líneas telefónicas para transmitir voz y datos simultáneamente.

- \*\*Características:\*\* Proporciona canales B (Bearer) para la transmisión de datos y canales D (Delta) para señalización. Aunque ha sido desplazado en gran medida por tecnologías de banda ancha, como DSL, fue importante en las décadas de 1980 y 1990.

5. \*\*ATM (Asynchronous Transfer Mode):\*\*

- \*\*Descripción:\*\* ATM es una tecnología de conmutación de celdas que transmite datos en pequeñas unidades llamadas celdas. Fue diseñada para integrar voz, datos y video en una red única.

- \*\*Características:\*\* Ofrece una alta velocidad de transmisión y es adecuada para aplicaciones que requieren un ancho de banda constante. Aunque fue promocionada como una tecnología avanzada, su implementación generalizada ha sido limitada en comparación con otras tecnologías.

Estas tecnologías han evolucionado con el tiempo, y en la actualidad, tecnologías más modernas, como MPLS (Multiprotocol Label Switching) y tecnologías basadas en IP, son comúnmente utilizadas para implementar redes WAN.

## Examen Unidad 3:

# Semana 13 – Unidad 4 – Tecnologías inalámbricas.

13, 14, 16 noviembre

Las tecnologías inalámbricas han experimentado un rápido avance en las últimas décadas, permitiendo la conectividad sin necesidad de cables físicos. Aquí tienes una descripción de algunas de las tecnologías inalámbricas más comunes:

1. \*\*Wi-Fi (802.11):\*\*

- \*\*Descripción:\*\* Wi-Fi es una tecnología de red inalámbrica que permite la conexión de dispositivos a una red local (LAN) mediante ondas de radio.

- \*\*Características:\*\* Se basa en el estándar IEEE 802.11 y proporciona diferentes velocidades de transmisión (como 802.11n, 802.11ac, y 802.11ax). Es ampliamente utilizado para redes locales en hogares, empresas y lugares públicos.

2. \*\*Bluetooth:\*\*

- \*\*Descripción:\*\* Bluetooth es una tecnología de comunicación inalámbrica de corto alcance que facilita la transferencia de datos entre dispositivos cercanos.

- \*\*Características:\*\* Se utiliza comúnmente para la conexión de dispositivos como auriculares, teclados, ratones, impresoras y teléfonos móviles. Bluetooth 5 es una versión más reciente que ofrece mejoras en el alcance y la velocidad de transferencia.

3. \*\*NFC (Near Field Communication):\*\*

- \*\*Descripción:\*\* NFC es una tecnología de comunicación inalámbrica de corto alcance que permite la transferencia de datos entre dispositivos cuando están muy cerca entre sí.

- \*\*Características:\*\* Se utiliza en aplicaciones como pagos móviles, transferencia de archivos y conexiones rápidas entre dispositivos. Es común en tarjetas de crédito y teléfonos móviles para transacciones sin contacto.

4. \*\*4G LTE (Long-Term Evolution):\*\*

- \*\*Descripción:\*\* LTE es una tecnología de comunicación móvil de alta velocidad que proporciona conectividad de datos para dispositivos móviles.

- \*\*Características:\*\* Ofrece velocidades de descarga y carga significativamente más rápidas que las tecnologías anteriores. LTE ha sido ampliamente adoptado para la conectividad de datos móviles y es un componente clave de las redes 4G.

5. \*\*5G (Quinta Generación):\*\*

- \*\*Descripción:\*\* 5G es la última generación de tecnología móvil que ofrece velocidades de conexión aún más rápidas, menor latencia y mayor capacidad que 4G.

- \*\*Características:\*\* Diseñado para admitir una amplia gama de aplicaciones, desde comunicaciones móviles hasta Internet de las cosas (IoT) y vehículos autónomos. Proporciona una conectividad más eficiente y mejorada.

6. \*\*Satélite:\*\*

- \*\*Descripción:\*\* Las comunicaciones satelitales utilizan satélites en órbita para transmitir señales a través de distancias largas.

- \*\*Características:\*\* Se utiliza en áreas donde otras formas de conectividad no son prácticas, como zonas rurales o lugares remotos. Proporciona cobertura global pero puede tener latencias más altas que otras tecnologías.

Estas tecnologías inalámbricas se utilizan en una variedad de aplicaciones y entornos, desde redes locales en hogares y oficinas hasta tecnologías móviles para comunicación en movimiento.

# Semana 14 – Unidad 4 – Estándares y protocolos: bluetooth, Infrarrojo, Wi-Fi, Wi-Max..

20, 21, 24 noviembre

Cada una de las tecnologías inalámbricas mencionadas utiliza estándares y protocolos específicos para garantizar la interoperabilidad entre dispositivos. Aquí hay una descripción de los estándares y protocolos asociados con Bluetooth, Infrarrojo, Wi-Fi y WiMAX:

1. \*\*Bluetooth:\*\*

- \*\*Estándar/Protocolo:\*\* Bluetooth se rige por el conjunto de estándares IEEE 802.15.

- \*\*Protocolos específicos:\*\*

- \*\*L2CAP (Logical Link Control and Adaptation Protocol):\*\* Proporciona servicios de multiplexación y segmentación de datos para aplicaciones sobre la capa base de Bluetooth.

- \*\*RFCOMM (Radio Frequency Communication):\*\* Emula una línea serie y se utiliza para proporcionar emulación de puerto serie sobre Bluetooth.

- \*\*HID (Human Interface Device):\*\* Permite la conexión de dispositivos de interfaz humana, como teclados y ratones.

- \*\*A2DP (Advanced Audio Distribution Profile):\*\* Utilizado para la transmisión de audio de alta calidad entre dispositivos.

2. \*\*Infrarrojo:\*\*

- \*\*Estándar/Protocolo:\*\* El infrarrojo (IR) no está definido por un estándar IEEE específico, pero utiliza principios de transmisión de luz infrarroja para la comunicación.

- \*\*Protocolos específicos:\*\*

- \*\*IrDA (Infrared Data Association):\*\* Establece estándares para la comunicación inalámbrica por infrarrojos entre dispositivos, como impresoras, teléfonos móviles y computadoras.

3. \*\*Wi-Fi:\*\*

- \*\*Estándar/Protocolo:\*\* Wi-Fi se basa en los estándares IEEE 802.11.

- \*\*Protocolos específicos:\*\*

- \*\*802.11a/b/g/n/ac/ax:\*\* Cada uno de estos protocolos define diferentes estándares para velocidades de transmisión y frecuencias de operación.

- \*\*WPA (Wi-Fi Protected Access) y WPA2:\*\* Protocolos de seguridad para proteger las redes Wi-Fi.

- \*\*WEP (Wired Equivalent Privacy):\*\* Un protocolo de seguridad más antiguo que ha sido en gran medida reemplazado por WPA y WPA2.

4. \*\*WiMAX:\*\*

- \*\*Estándar/Protocolo:\*\* WiMAX se basa en los estándares IEEE 802.16.

- \*\*Protocolos específicos:\*\*

- \*\*802.16d (WiMAX fijo):\*\* Utilizado para implementaciones de WiMAX fijo.

- \*\*802.16e (WiMAX móvil):\*\* Diseñado para proporcionar conectividad WiMAX en movimiento.

- \*\*802.16m (WiMAX avanzado):\*\* Una mejora que ofrece mayores velocidades y eficiencia.

Estos estándares y protocolos aseguran que los dispositivos que utilizan estas tecnologías puedan comunicarse de manera efectiva y brindan un marco común para el desarrollo y la implementación de dispositivos compatibles. Es importante destacar que la tecnología inalámbrica continúa evolucionando, y nuevos estándares y protocolos pueden surgir con el tiempo para mejorar el rendimiento y la seguridad.

# Semana 15 – Unidad 4 – Estándares y protocolos: bluetooth, Infrarrojo, Wi-Fi, Wi-Max..

27, 28, 30 noviembre

Cada una de las tecnologías inalámbricas mencionadas utiliza estándares y protocolos específicos para garantizar la interoperabilidad entre dispositivos. Aquí hay una descripción de los estándares y protocolos asociados con Bluetooth, Infrarrojo, Wi-Fi y WiMAX:

1. \*\*Bluetooth:\*\*

- \*\*Estándar/Protocolo:\*\* Bluetooth se rige por el conjunto de estándares IEEE 802.15.

- \*\*Protocolos específicos:\*\*

- \*\*L2CAP (Logical Link Control and Adaptation Protocol):\*\* Proporciona servicios de multiplexación y segmentación de datos para aplicaciones sobre la capa base de Bluetooth.

- \*\*RFCOMM (Radio Frequency Communication):\*\* Emula una línea serie y se utiliza para proporcionar emulación de puerto serie sobre Bluetooth.

- \*\*HID (Human Interface Device):\*\* Permite la conexión de dispositivos de interfaz humana, como teclados y ratones.

- \*\*A2DP (Advanced Audio Distribution Profile):\*\* Utilizado para la transmisión de audio de alta calidad entre dispositivos.

2. \*\*Infrarrojo:\*\*

- \*\*Estándar/Protocolo:\*\* El infrarrojo (IR) no está definido por un estándar IEEE específico, pero utiliza principios de transmisión de luz infrarroja para la comunicación.

- \*\*Protocolos específicos:\*\*

- \*\*IrDA (Infrared Data Association):\*\* Establece estándares para la comunicación inalámbrica por infrarrojos entre dispositivos, como impresoras, teléfonos móviles y computadoras.

3. \*\*Wi-Fi:\*\*

- \*\*Estándar/Protocolo:\*\* Wi-Fi se basa en los estándares IEEE 802.11.

- \*\*Protocolos específicos:\*\*

- \*\*802.11a/b/g/n/ac/ax:\*\* Cada uno de estos protocolos define diferentes estándares para velocidades de transmisión y frecuencias de operación.

- \*\*WPA (Wi-Fi Protected Access) y WPA2:\*\* Protocolos de seguridad para proteger las redes Wi-Fi.

- \*\*WEP (Wired Equivalent Privacy):\*\* Un protocolo de seguridad más antiguo que ha sido en gran medida reemplazado por WPA y WPA2.

4. \*\*WiMAX:\*\*

- \*\*Estándar/Protocolo:\*\* WiMAX se basa en los estándares IEEE 802.16.

- \*\*Protocolos específicos:\*\*

- \*\*802.16d (WiMAX fijo):\*\* Utilizado para implementaciones de WiMAX fijo.

- \*\*802.16e (WiMAX móvil):\*\* Diseñado para proporcionar conectividad WiMAX en movimiento.

- \*\*802.16m (WiMAX avanzado):\*\* Una mejora que ofrece mayores velocidades y eficiencia.

Estos estándares y protocolos aseguran que los dispositivos que utilizan estas tecnologías puedan comunicarse de manera efectiva y brindan un marco común para el desarrollo y la implementación de dispositivos compatibles. Es importante destacar que la tecnología inalámbrica continúa evolucionando, y nuevos estándares y protocolos pueden surgir con el tiempo para mejorar el rendimiento y la seguridad.

# Semana 16 – Unidad 4 – Estándares y protocolos: bluetooth, Infrarrojo, Wi-Fi, Wi-Max..

04, 05, 07 noviembre

Aquí hay una descripción de algunos aspectos de seguridad relacionados con redes Wi-Fi, incluyendo los protocolos y técnicas mencionados:

1. \*\*WEP (Wired Equivalent Privacy):\*\*

- \*\*Descripción:\*\* WEP fue uno de los primeros protocolos de seguridad para redes Wi-Fi. Sin embargo, ha demostrado ser vulnerable y no es seguro. Se puede comprometer relativamente fácilmente mediante ataques de "fuerza bruta".

- \*\*Estado actual:\*\* Se recomienda no utilizar WEP debido a sus debilidades de seguridad. Es preferible utilizar protocolos más seguros, como WPA2 o WPA3.

2. \*\*WPA (Wi-Fi Protected Access):\*\*

- \*\*Descripción:\*\* WPA fue introducido como una mejora de seguridad sobre WEP. Introdujo mejoras en la encriptación y la autenticación. WPA utiliza el protocolo TKIP (Temporal Key Integrity Protocol).

- \*\*Estado actual:\*\* Aunque más seguro que WEP, WPA también ha demostrado vulnerabilidades con el tiempo. Se recomienda utilizar WPA2 o WPA3 en lugar de WPA.

3. \*\*WPA2 (Wi-Fi Protected Access 2):\*\*

- \*\*Descripción:\*\* WPA2 es una mejora significativa en comparación con WPA. Utiliza el protocolo AES (Advanced Encryption Standard) para proporcionar una mayor seguridad en la encriptación de datos.

- \*\*Estado actual:\*\* WPA2 ha sido ampliamente adoptado y sigue siendo una opción segura para proteger redes Wi-Fi. Sin embargo, se recomienda migrar a WPA3 cuando sea posible para beneficios adicionales de seguridad.

4. \*\*WPA3 (Wi-Fi Protected Access 3):\*\*

- \*\*Descripción:\*\* WPA3 es la última versión de los protocolos de seguridad para Wi-Fi. Introduce mejoras significativas en la seguridad, incluida la protección contra ataques de fuerza bruta y una mayor seguridad para conexiones abiertas.

- \*\*Estado actual:\*\* WPA3 proporciona el más alto nivel de seguridad disponible en la actualidad. Se recomienda su implementación siempre que sea posible.

5. \*\*Filtrado de MAC (Control de Acceso basado en direcciones MAC):\*\*

- \*\*Descripción:\*\* El filtrado de direcciones MAC implica permitir o bloquear el acceso a una red Wi-Fi en función de las direcciones MAC de los dispositivos. Cada dispositivo tiene una dirección MAC única.

- \*\*Estado actual:\*\* Aunque el filtrado de MAC puede agregar una capa adicional de seguridad, no es una medida infalible, ya que las direcciones MAC pueden ser spoofeadas (falsificadas). No se considera una defensa robusta por sí sola y se recomienda usar en conjunto con otros protocolos de seguridad.

Es importante tener en cuenta que la seguridad de una red Wi-Fi se fortalece mediante la combinación de varias capas de protección. Se recomienda utilizar WPA3, si es posible, junto con otras medidas de seguridad como contraseñas fuertes, actualizaciones regulares de firmware y la segmentación de la red para maximizar la seguridad de la red inalámbrica.

## Examen unidad 4: