Compás
capacitación e investigación

Redes y Telecomunicaciones:
Diseño, Implementación, Gestión y Aplicaciones

Redes y Telecomunicaciones: Diseño, Implementación, Gestión y Aplicaciones

Lara Guijarro Elva Gioconda
Beltrán Ruiz José Andrés
Jorque Rea Abrahan Mesias
Lozada Calle Wilson Sebastián
Valencia Lucero Jonathan Daniel
Veintimilla Muñoz Rodrigo Gabriel
Montesdeoca Orozco Hilda Jacqueline
Almeida Montenegro German Mauricio
Quishpe Sacancela Ernesto
Sánchez Olmedo Omar Fernando

ISBN: 978-9942-53-155-1
Primera edición, 2026

Lara Guijarro Elva Gioconda
Beltrán Ruiz José Andrés
Jorque Rea Abrahan Mesias
Lozada Calle Wilson Sebastián
Valencia Lucero Jonathan Daniel
Veintimilla Muñoz Rodrigo Gabriel
Montesdeoca Orozco Hilda Jacqueline
Almeida Montenegro German Mauricio
Quishpe Sacancela Ernesto
Sánchez Olmedo Omar Fernando

ISBN: 978-9942-53-155-1
Distribución online
Acceso abierto

Guayaquil, Ecuador
www.grupocompas.com
http://repositorio.grupocompas.com

Diseño y diagramación:
Ing. Hilda Jacqueline Montesdeoca Orozco

Primera edición, 2026

Esta obra ha sido sometida a un proceso de evaluación bajo el sistema de arbitraje doble ciego (double-blind peer review), garantizando el anonimato tanto de los autores como de los evaluadores externos. El dictamen favorable certifica que el contenido cumple con los más altos estándares de rigor científico, calidad editorial y originalidad exigidos por la comunidad académica internacional para su indexación y reconocimiento científico.

Cita
Lara, E., Beltrán, J., Jorque, A., Lozada, W., Valencia, J., Veintimilla, R., Montesdeoca, H., Almeida, G., Quishpe, E., Sánchez, O. (2026) Redes y Telecomunicaciones: Diseño, Implementación, Gestión y Aplicaciones. Editorial Grupo Compás

CONTENIDOS

PRÓLOGO

El propósito de este libro es proporcionar una guía comprensiva sobre la asignatura de Redes de Datos, abordando tanto los fundamentos teóricos como las aplicaciones prácticas. A través de los cuales, se pretende ofrecer a los lectores una comprensión profunda de los principios y técnicas que subyacen al proceso de Telecomunicaciones, así como las habilidades necesarias para aplicar estos conocimientos en sus propios estudios.

Las Redes de Datos es una parte de las Telecomunicaciones que es fundamental en el avance de la tecnología. Este libro, " Redes y Telecomunicaciones: Diseño, implementación, gestión y aplicaciones", ha sido elaborado con el propósito de proporcionar una guía clara y accesible sobre los principios, tipos de redes de datos, se incluye prácticas completas que apoyará a los interesados del área en sus tareas, indicándoles que la asignatura es interesante, importante y base para la interconexión de dispositivos de redes, tanto en la parte de hardware como de software.

A lo largo de sus capítulos, se explorará los fundamentos teóricos de las telecomunicaciones, haciendo énfasis en la parte de Redes de Datos, se detalla los tipos de redes, IPs, Máscaras, Enrutamiento y todo lo referente al proceso real del funcionamiento y la implementación de una Red de Área Local. Desde los dispositivos base terminando en la seguridad de la información y la utilización de HW adecuado para el tipo de red a implementar. Se parte de lo teórico a lo práctico, de lo simple a lo complejo, de esta forma las personas que lean este libro, aún sin conocimientos previos, podrán terminar entendiendo lo que es el mundo real de las Telecomunicaciones y las Redes de Datos.

Uno de los objetivos principales es desmitificar el mundo de las redes y las telecomunicaciones. A menudo, el diseño, la implementación y gestión de infraestructuras de comunicación pueden parecer tareas intimidantes y complejas; sin embargo, con las herramientas, metodologías y conocimientos adecuados, cualquier profesional puede abordarlas de manera efectiva. Hemos incorporado estudios de caso y ejemplos prácticos para mostrar cómo los principios teóricos se aplican en escenarios reales: desde el diseño de redes campus y la segmentación mediante VLAN y routing, hasta la implementación de servicios sobre IP, la seguridad perimetral y el aseguramiento de la calidad de servicio.

De igual forma, se ha puesto un énfasis especial en la ética, la seguridad y la confiabilidad en redes. En una era en la que la integridad de los datos, la privacidad y la transparencia operativa son más importantes que nunca, es crucial que los profesionales comprendan y respeten las normativas y buenas prácticas que guían su trabajo. Este libro aborda estos aspectos con seriedad, ofreciendo orientación para desplegar y administrar redes de forma responsable, segura, alineada con estándares y marcos de referencia.

Por último, expreso mi agradecimiento sincero a las autoridades, docentes y especialistas del ISUCT que, desde las diferentes áreas, han contribuido con sus experiencias y conocimientos a la elaboración de esta obra. Sus aportes han sido invaluables para construir un recurso que confiamos será de gran utilidad para la comunidad académica y el ámbito profesional.

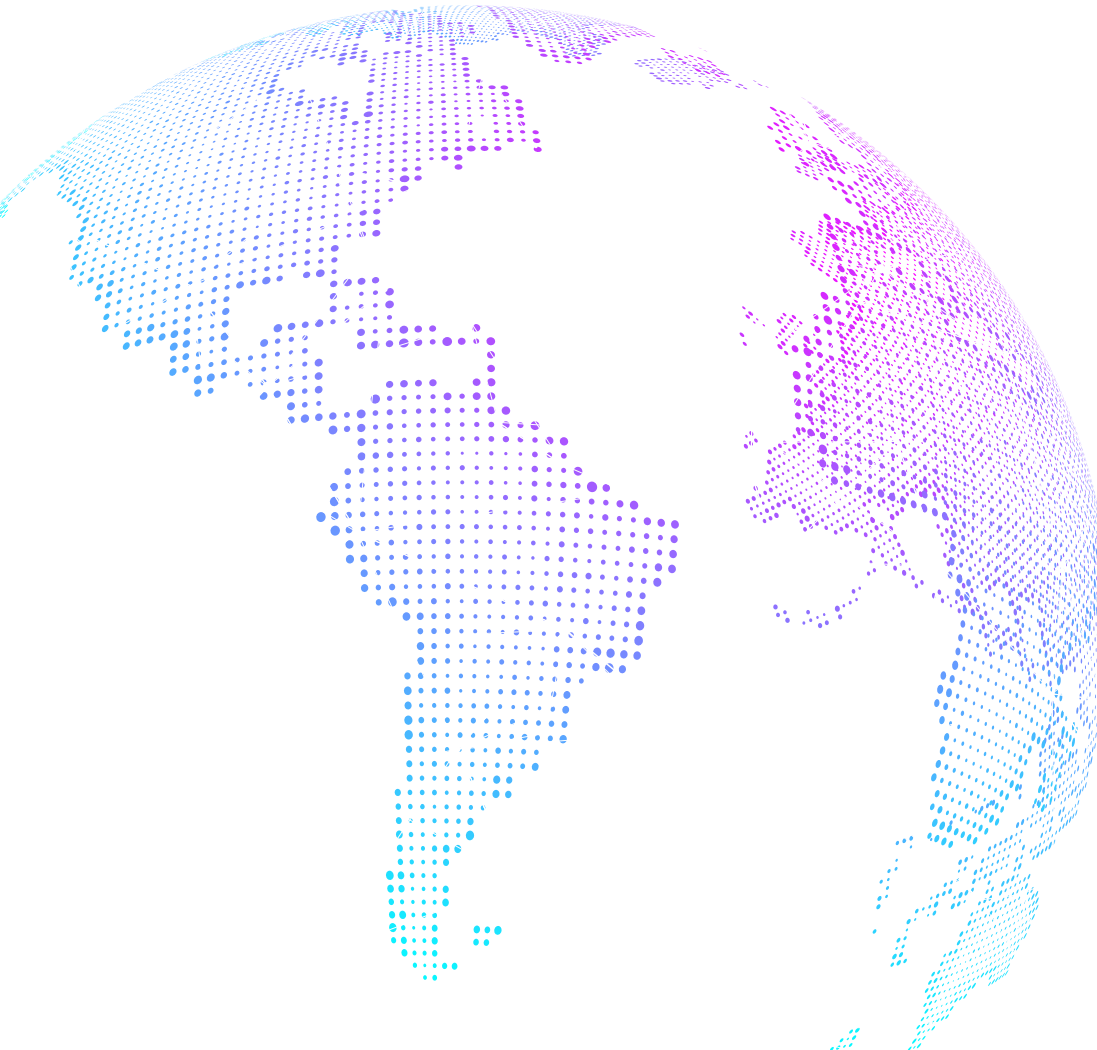
Esperamos que "Redes y Telecomunicaciones: Diseño, implementación, gestión y aplicaciones" sea una herramienta valiosa en el proceso de aprendizaje y práctica profesional. Que les inspire a explorar nuevas arquitecturas, cuestionar lo establecido y contribuir al avance tecnológico y a la excelencia operativa en campo que desempeñe.

"Aprender redes de datos no es solo entender cables y routers; es aprender a dominar los hilos invisibles que mueven al mundo moderno. ¡Conviértete en el arquitecto de la conectividad!"

Anónimo

PhD (c) Elva G. Lara Guijarro
Coordinadora de la Comisión de Investigación del ISU Central Técnico

CAPÍTULO I
FUNDAMENTOS DE TELECOMUNICACIONES



CAPÍTULO I

FUNDAMENTOS DE TELECOMUNICACIONES

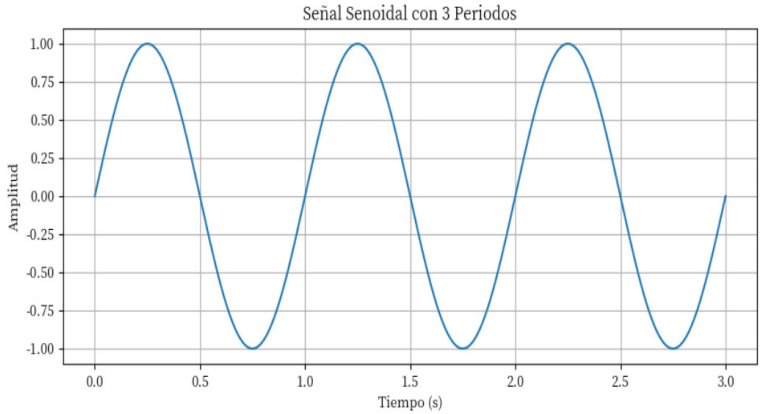
Los fundamentos de telecomunicaciones abarcan los principios y tecnologías esenciales que permiten la transmisión de información a través de distintos medios. Esto incluye señales, modulación, medios de transmisión, propagación y técnicas de multiplexado.

1. Teoría de señales

La teoría de señales estudia cómo se representan, analizan y procesan las señales que transportan información en telecomunicaciones. Estas pueden ser analógicas (continuas y con valores infinitos) o digitales (discretas y representadas por bits). También se pueden analizar en el dominio del tiempo (cómo varían en el tiempo) o en el dominio de la frecuencia, donde la Transformada de Fourier permite descomponerlas en distintas frecuencias.

El procesamiento de señales incluye técnicas como el filtrado (para eliminar ruido), la amplificación (para mejorar su potencia) y la modulación (para facilitar su transmisión). Estos principios son fundamentales en sistemas de comunicación como radio, televisión, telefonía e internet.

Figura 1. Señal sinoidal



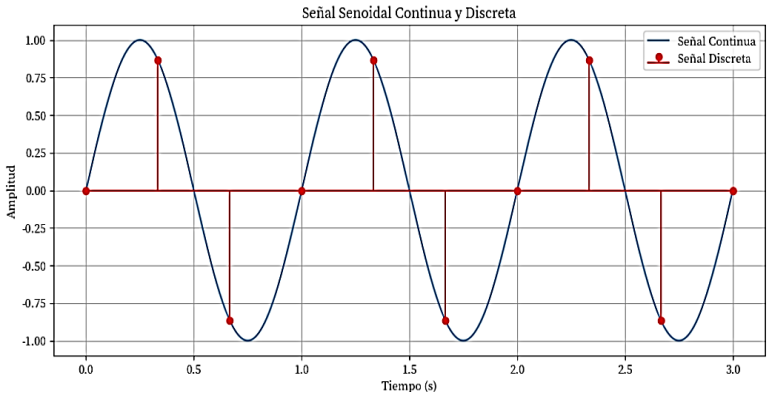
La figura anterior representa una señal senoidal con una amplitud de 1, 3 períodos, la frecuencia es de 5HZ, y un período de tiempo de 0 a 3 segundos. Las líneas de la cuadrícula están incluidas para facilitar la lectura, y los ejes están etiquetados como “Tiempo (s)” y “Amplitud”.

1.1. Tipos de señales:

1.1.1. Señales continuas y señales discretas

Las señales continuas son aquellas que varían de manera ininterrumpida en el tiempo y pueden tomar un número infinito de valores dentro de un rango determinado. Un ejemplo común es la señal de voz en una llamada telefónica analógica o las ondas de radio.

Figura 2. Señal continuo y discreto.



En la Figura 2 se puede ver la señal continua que está representada por el color azul y la señal discreta de color rojo. Está en base a 3 segundos y 3 períodos. La amplitud es de 1.

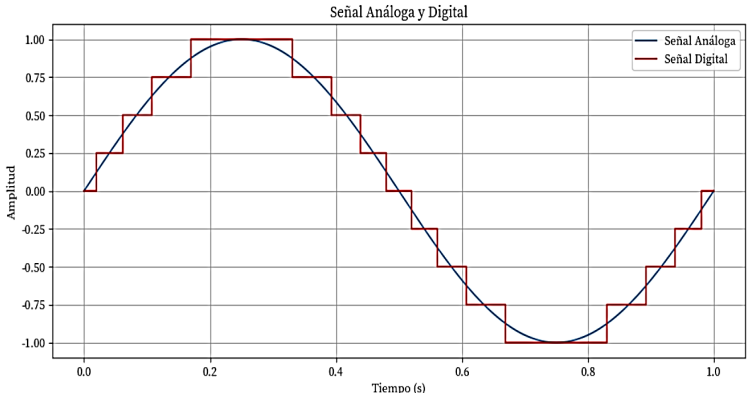
Las señales continuas se definen para cada instante de tiempo dentro de un intervalo, es decir son funciones continuas de tiempo que se representan matemáticamente. Por ejemplo, la temperatura, la presión y el voltaje en un circuito análogo. Una desventaja podría ser que son difíciles de almacenar y manipular digitalmente.

Las señales discretas se definen solo en instantes específicos de tiempo (funciones de tiempo discretas). Solo están definidas en ciertos instantes de tiempo y toman valores específicos. Estas señales se obtienen mediante un proceso de muestreo y son la base de los sistemas digitales, como el audio en formato MP3 o las imágenes en formato digital.

1.1.2. Análogas y digitales

Las señales análogas son continuas y pueden tomar infinitos valores dentro de un rango, representando información de manera natural, como el sonido captado por un micrófono o la imagen en una televisión tradicional. Su principal desventaja es la susceptibilidad al ruido y la degradación con la distancia.

Figura 3. Señal analógica y digital.



Las señales digitales, están compuestas por valores discretos (generalmente 0 y 1), lo que permite mayor precisión, facilidad de almacenamiento y transmisión sin pérdidas significativas. Ejemplos incluyen el audio en formato MP3, los videos en streaming y las telecomunicaciones modernas basadas en datos.

Las señales discretas no están cuantificadas y los valores pueden ser cualquier número real, en cambio en las señales digitales los valores son cuantificados a un conjunto finito de niveles. En la Tabla 1 se puede mirar las diferencias entre las señales discretas y digitales, estas son fundamentales en el campo del procesamiento de señales y determinan cómo se manejan y analizan las señales en diferentes aplicaciones.

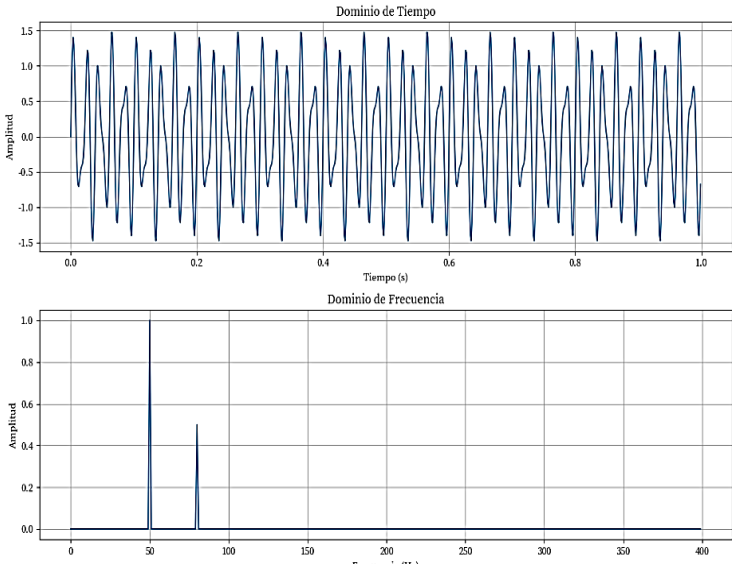
Tabla. Diferencias entre señales discretas y digitales

Característica	*Señales Discretas*	*Señales Digitales*
Definición	Valores en instantes específicos de tiempo	Valores discretos cuantificados
Valores	Continuos (cualquier valor real)	Cuantificados (niveles finitos)
Voltaje	Puede variar continuamente, dependiendo del uso	Niveles fijos (por ejemplo, 0V y 5V)
Representación	Secuencia de muestras	Secuencia de números binarios
Ejemplos	Muestras de temperatura sin redondear	Audio e imágenes digitales
Uso	Análisis antes de la cuantificación	Almacenamiento y procesamiento digital

1.2. Dominio de tiempo y dominio de frecuencia

El dominio de tiempo representa una señal en función del tiempo, mostrando cómo varía su amplitud en cada instante. Se usa para analizar la forma de onda de señales como el sonido o una corriente eléctrica, permitiendo estudiar su duración, periodicidad y comportamiento temporal. El dominio de frecuencia, en cambio, muestra las componentes de la señal en términos de sus frecuencias, lo que permite identificar qué rangos espectrales la conforman. La Transformada de Fourier es la herramienta matemática que convierte una señal del dominio del tiempo al dominio de frecuencia, facilitando el análisis de señales en telecomunicaciones, audio e imágenes. En la siguiente figura se puede ver el dominio de tiempo, cómo varía la amplitud de esta a lo largo del tiempo, las oscilaciones y el dominio de frecuencia, su distribución y las diferentes frecuencias que componen la señal, mediante la aplicación de la transformada de Fourier, de acuerdo a ello se observan los dos picos que indican las frecuencias presentes en la señal original.

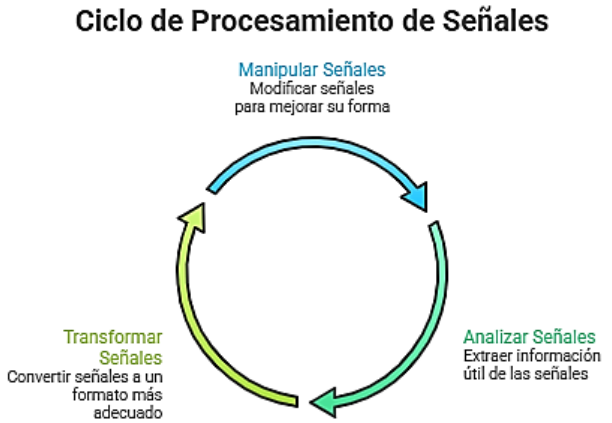
Figura 4. Dominio de tiempo y dominio de frecuencia.



1.3. Procesamiento de señales

El procesamiento de señales de datos es el conjunto de técnicas y etapas orientadas a extraer valor de señales analógicas o digitales, y suele seguir un ciclo continuo que incluye: transformar señales para convertirlas a un formato adecuado de análisis (por ejemplo, muestreo y cuantización de una señal analógica a digital, cambio de dominio tiempo–frecuencia con FFT, normalización o filtrado básico), manipular señales para mejorar su calidad o resaltar características de interés (como filtrado pasa bajo/alto, eliminación de ruido, realce, compresión o ecualización), y analizar señales para obtener información útil y tomar decisiones (detección de patrones, estimación de parámetros, clasificación, diagnóstico o monitoreo); este ciclo se aplica en comunicaciones, audio, imagen, biomédica, control industrial y otras áreas, donde la correcta transformación, mejora y análisis permiten sistemas más precisos, robustos y eficientes.

Figura 5. Etapas del procesamiento de las señales



1.3.1. Filtros

El filtrado es un proceso esencial en el procesamiento de señales que se utiliza para eliminar componentes no deseados de una señal o para extraer información relevante. Este proceso es fundamental en telecomunicaciones, donde las señales pueden estar contaminadas con ruido o interferencias. Los filtros son circuitos que permiten el paso de una determinada banda de frecuencias mientras atenúan todas las señales que no estén comprendidas dentro de esta banda. Existen filtros activos y pasivos. Los filtros pasivos sólo tienen resistencias, inductores y capacitores (ejemplo: filtro RC). En los filtros activos, se utilizan transistores o amplificadores operacionales además de resistencias, inductores y capacitores (filtro Sallen-Key). Los inductores no se emplean mucho en los filtros activos pues son voluminosos, caros y a veces tienen componentes resistivas de elevada magnitud.

Las funciones de los Filtros son:

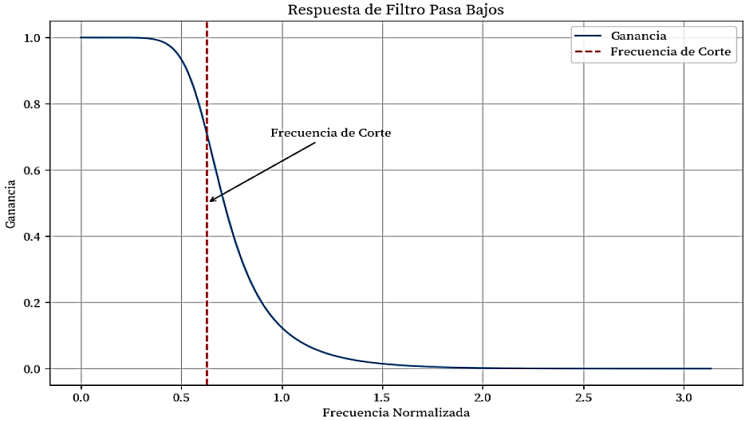
- ***Eliminar Ruido:*** Los filtros pueden reducir o eliminar el ruido presente en una señal.
- ***Aislar Frecuencias:*** Permiten seleccionar o atenuar ciertas frecuencias de interés.
- ***Mejorar la Calidad:*** Ayudan a mejorar la claridad y la calidad de la señal.

Existen cuatro tipos de filtros: pasa bajo, pasa alto, pasa banda y de eliminación de banda (también conocidos como de rechazo de banda o de muesca).

Filtro pasa bajo

Los filtros "pasa bajo" son dispositivos que permiten el paso de frecuencias bajas mientras atenúan las frecuencias altas. Se utilizan para suavizar señales, eliminando el ruido de alta frecuencia y preservando los componentes esenciales de baja frecuencia. Estos filtros son comunes en aplicaciones de audio y procesamiento de señales, donde es importante mantener la claridad de las frecuencias más bajas y reducir las interferencias no deseadas.

Figura 6. Filtro pasa bajo.

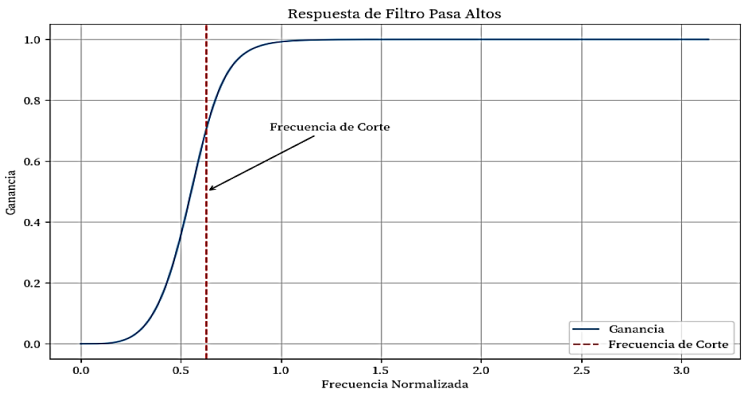


La Figura anterior, muestra la respuesta en frecuencia de un filtro pasa bajos. La línea roja discontinua indica la frecuencia de corte, que es el punto donde el filtro comienza a atenuar las frecuencias altas. Las frecuencias a la izquierda de la frecuencia de corte pasan sin atenuación significativa, mientras que las frecuencias a la derecha son reducidas progresivamente. La anotación resalta la importancia de la frecuencia de corte como parámetro clave en el diseño de filtros.

Filtro pasa alto

Los filtros "pasa alto" son herramientas que permiten que las frecuencias altas atraviesen mientras bloquean o reducen las frecuencias bajas. Su principal función es eliminar componentes de baja frecuencia, como ruidos de fondo, y destacar las señales de mayor frecuencia. Este tipo de filtro es ampliamente utilizado en sistemas de audio, comunicaciones y procesamiento de señales para mejorar la calidad o aislar información relevante en rangos altos de frecuencia.

Figura 7. Filtro pasa altos.

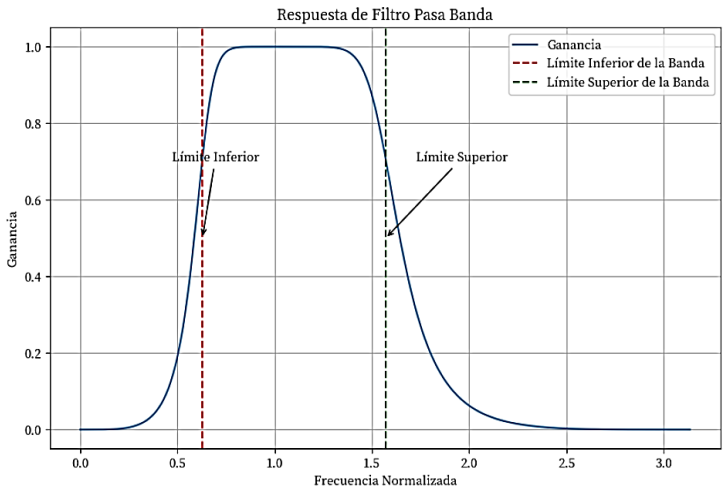


En la figura anterior se muestra cómo un "filtro pasa altos" permite que las frecuencias por encima de la frecuencia de corte pasen mientras atenúa las frecuencias más bajas. La línea roja discontinua marca la frecuencia de corte, donde el filtro comienza a permitir el paso de frecuencias altas. Las frecuencias a la derecha de la frecuencia de corte pasan sin atenuación significativa, mientras que las frecuencias a la izquierda son reducidas.

Filtro pasa banda

Un filtro pasa banda es un dispositivo que permite el paso de un rango específico de frecuencias mientras bloquea o reduce las frecuencias que están por debajo y por encima de ese rango. Su principal función es aislar señales dentro de una banda de interés, eliminando componentes indeseados fuera de ese intervalo. Este tipo de filtro se utiliza comúnmente en sistemas de comunicación y procesamiento de señales para captar información precisa en un rango definido de frecuencias.

Figura 8. Filtro pasa banda.



Este gráfico representa la respuesta en frecuencia de un filtro pasa banda. La línea roja discontinua indica el límite inferior de la banda, que marca el inicio del rango de frecuencias permitidas. La línea verde discontinua señala el límite superior de la banda, que marca el final del rango de frecuencias permitidas. Solo las frecuencias dentro de este rango pasan sin atenuación significativa, mientras que las frecuencias fuera de los límites son bloqueadas o reducidas. Este tipo de filtro es útil para captar señales específicas dentro de un rango de interés, como en sistemas de comunicación o análisis de espectros.

Filtros rechazo de banda

Un filtro rechazo de banda es un dispositivo que bloquea o atenúa las frecuencias dentro de un rango específico, permitiendo el paso de las frecuencias que están por debajo y por encima de dicho rango. Su principal función es eliminar señales no deseadas dentro de una banda de frecuencia defini-

da, mientras preserva el resto del espectro. Este tipo de filtro se utiliza comúnmente en aplicaciones como eliminación de interferencias o ruido en sistemas de comunicación y procesamiento de señales.

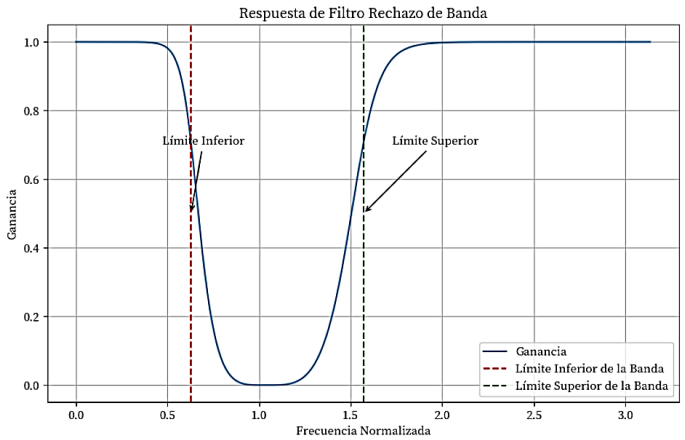
Este tipo de filtro son "coladores" de señales que dejan pasar casi todas las frecuencias excepto un tramo específico, al que le bajan la intensidad. Ese tramo que bloquean se llama banda de rechazo o "notch". Eliminan interferencias localizadas sin afectar demasiado el resto del contenido. Son útiles cuando hay un zumbido o tono molesto concentrado en una frecuencia concreta. Su funcionamiento en términos simples se puede explicar como que imaginamos una carretera con varios carriles (frecuencias), el filtro mantiene abiertos todos los carriles menos uno, el del rango problemático, que queda cerrado para que ese "tráfico" no pase.

A diferencia de los filtros pasa-bajos o pasa-altos que cortan todo por debajo o por encima de cierto punto, este solamente "saca" una franja estrecha o ancha del espectro, según cómo se diseñe.

Ejemplo

Audio en casa: si un sistema de sonido capta un zumbido de la red eléctrica a 50/60 Hz, se coloca un filtro de rechazo centrado en esa frecuencia. El resultado es que desaparece el zumbido, pero la música y la voz (que ocupan muchas otras frecuencias) se mantienen casi intactas. Es como usar un ecualizador para "silenciar" solo el tono molesto sin tocar el resto.

Figura 9. Filtro rechazo de banda.



1.3.2. Amplificación

El filtrado es un proceso esencial en el procesamiento de señales que encuentra diversas aplicaciones en el ámbito de las telecomunicaciones y otras áreas. Los "filtros pasa bajos" son utilizados principalmente en el ámbito del audio para eliminar el ruido de alta frecuencia, mejorando así la claridad del sonido, y también en el procesamiento de imágenes para suavizar detalles no deseados. Por otro lado, los filtros pasan altos son fundamentales en telecomunicaciones, ya que permiten eliminar ruidos de baja frecuencia, garantizando que las señales de comunicación sean más limpias y efectivas.

Estos filtros también son útiles en el análisis de señales, donde destacan cambios rápidos en los datos. En cuanto a los filtros pasa banda, se emplean en radiocomunicaciones para seleccionar señales dentro de un rango específico de frecuencias, como en la recepción de estaciones de radio o televisión, y en sistemas de sonido, donde se utilizan en ecualizadores para ajustar frecuencias determinadas. Finalmente, los filtros rechazan banda son ideales para eliminar interferencias en un rango específico de frecuencias, lo que resulta crucial en sistemas de comunicación donde hay señales no deseadas, así como en equipos de medición que operan en frecuencias específicas. En resumen, la elección del tipo de filtro depende de los requisitos particulares de cada aplicación, y su correcta implementación es clave para mejorar la calidad y eficacia de las señales procesadas.

Figura 10. Tipos de filtros

Comparación de tipos de filtros

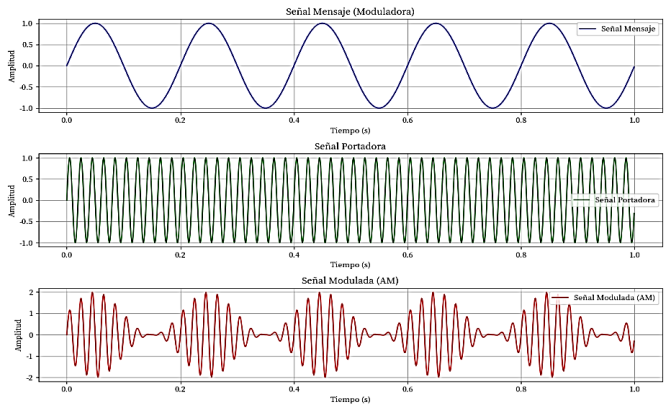
Característica	Filtro Pasa Bajos	Filtro Pasa Altos	Filtro Pasa Banda	Filtro Rechaza Banda
Aplicación Principal	Audio, Procesamiento de Imágenes	Telecomunicaciones, Análisis de Señales	Radiocomunicaciones, Sistemas de Sonido	Sistemas de Comunicación, Equipos de Medición
Función	Elimina ruido de alta frecuencia	Elimina ruido de baja frecuencia	Selecciona señales dentro de un rango	Elimina interferencias en un rango
Uso	Mejora la claridad del sonido	Garantiza señales de comunicación limpias	Ajusta frecuencias determinadas en ecualizadores	Crucial en sistemas de comunicación

Made with Napkin

1.3.3. Modulación

La modulación es un proceso fundamental en las comunicaciones que permite la transmisión eficiente de señales a través de diversos canales de comunicación. Este proceso consiste en adaptar una señal de información, como audio, video o datos, a un formato que sea más adecuado para su transmisión a largas distancias o a través de medios específicos, como cables, fibra óptica o el aire.

Figura 11. Modulación de una señal en telecomunicaciones.



El propósito principal de la modulación es modificar una señal portadora, que es una onda de alta frecuencia, para que transporte la señal de información deseada. Al hacerlo, se facilita la transmisión de la señal y se minimizan los efectos del ruido y las interferencias que pueden degradar la calidad de la comunicación.

Además, la modulación permite optimizar el uso del espectro de frecuencias disponible, lo que es crucial en entornos donde múltiples señales compiten por el mismo espacio de transmisión. Existen diferentes técnicas de modulación, como la modulación de amplitud (AM), la modulación de frecuencia (FM) y la modulación de fase (PM), cada una con sus propias características y aplicaciones. Por ejemplo, la modulación de amplitud es común en la transmisión de radio, mientras que la modulación de frecuencia se utiliza ampliamente en la transmisión de audio y televisión debido a su mayor resistencia al ruido.

- ***Señal Mensaje (Moduladora):*** Es la señal de baja frecuencia que contiene la información a transmitir.
- ***Señal Portadora:*** Es una señal de alta frecuencia que transporta la señal mensaje.
- ***Señal Modulada (AM):*** Es el resultado de combinar la señal mensaje con la portadora. En la modulación de amplitud (AM), la amplitud de la portadora varía de acuerdo con la señal mensaje.

1.4. Transformada de Fourier

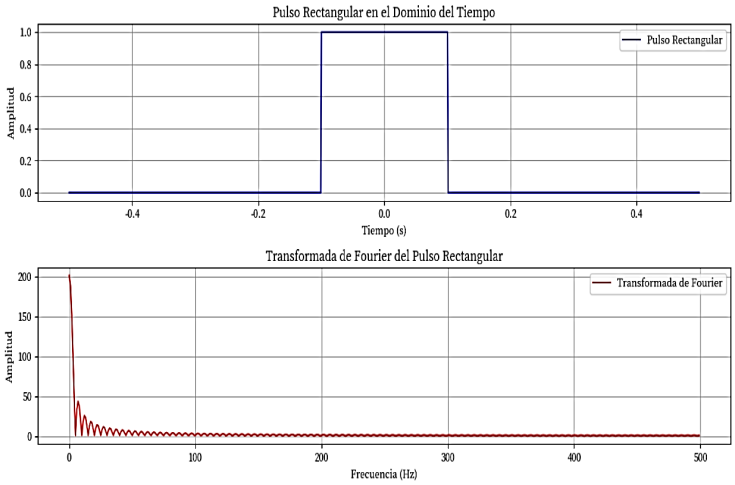
La Transformada de Fourier es una herramienta matemática utilizada para descomponer una señal en sus componentes de frecuencia. En términos sencillos, la transformada de Fourier convierte una señal en el dominio del tiempo en una representación en el dominio de la frecuencia. Esta es una de las herramientas más poderosas en el procesamiento de señales, ya que permite analizar las frecuencias presentes en una señal, lo cual es útil en muchas aplicaciones como la compresión de datos, la eliminación de ruido, y el análisis espectral.

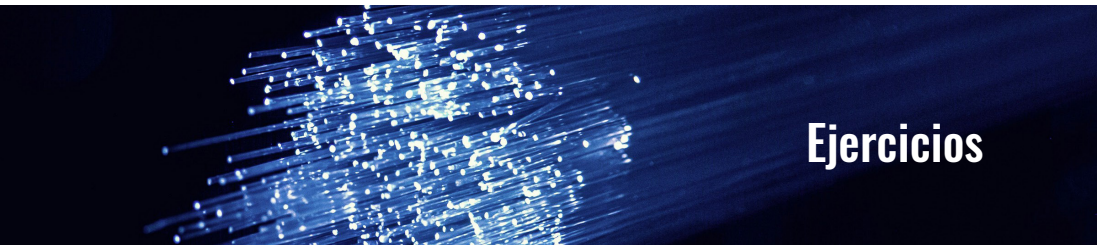
En la siguiente Figura se puede ver la transformada de Fourier de un pulso rectangular que es un ejemplo clásico para ilustrar la relación entre el tiempo y la frecuencia en el análisis de señales:

- ***Pulso Rectangular en el Dominio del Tiempo:*** La primera gráfica muestra un pulso rectangular centrado en el tiempo.
- ***Transformada de Fourier:*** La segunda gráfica muestra la transformada de Fourier del pulso rectangular, que es una función de tipo sin. Esta representación en el dominio de la frecuencia es fundamental para entender cómo las señales rectangulares se descomponen en sus componentes de frecuencia.

Figura 12.

Transformada de Fourier de un pulso rectangular en el dominio del tiempo.





Ejercicio de procesamiento de Señales

Considera la siguiente señal de audio:

$$s(t) = 3\ sen(2\Pi\ 500t) + 2\ sen\ (2\Pi\ 1000t) + nt$$

donde n(t) es ruido blanco que afecta la señal.

Parte 1: Identificación de Componentes

Identificación de Frecuencias

La señal s(t) está compuesta por dos componentes sinusoidales:

1. $3\ sen(2\Pi\ 500t)$ → frecuencia de 500 Hz
2. $2\ sen\ (2\Pi\ 1000t) +$ → frecuencia de 1000 Hz

Las frecuencias fundamentales presentes en la señal son ***500 Hz*** y ***1000 Hz.***

Parte 2: Aplicación de la Transformada de Fourier

Transformada de Fourier

La Transformada de Fourier de una señal s(t)s(t) se define como:

$$S(f) = \int_{-\infty}^{\infty} s(t) e^{-j2\Pi ft} dt$$

Para nuestra señal s(t)s:

$$S(f) = \int_{-\infty}^{\infty} (3\ sen(2\Pi\ 500t) + 2\ sen\ (2\Pi\ 1000t) + nt) e^{-j2\Pi ft} dt$$

Aplicando la propiedad de la Transformada de Fourier para funciones sinusoidales, se sabe que:

La Transformada de Fourier de $Sen\ (2\Pi f_0 t)$ es:

$$\frac{j}{2}(\delta(f - f_0) - \delta(f + f_0))$$

Por lo tanto, para nuestra señal:

$$S(f) = 3\ \frac{j}{2}\big(\delta(f - 500) - \delta(f + 500)\big) + 2\ \frac{j}{2}\big(\delta(f - 1000) - \delta(f + 1000)\big)$$

Simplificando, se obtiene:

$$S(f) = \frac{3j}{2}\big(\delta(f - 500) - \delta(f + 500)\big) + j\big(\delta(f - 1000) - \delta(f + 1000)\big)$$

Parte 3: Interpretación del Espectro

Interpretación del Espectro

El espectro de frecuencia S(f) mostrará picos en las siguientes frecuencias:

- En ***500 Hz*** con una amplitud de
- En ***1000 Hz*** con una amplitud de 1

Habrá picos en las frecuencias negativas (-500 Hz y -1000 Hz) debido a la simetría de la Transformada de Fourier para señales reales.

Parte 4: Filtrado

Filtrado de Ruido

Supongamos que deseamos eliminar el ruido n(t) utilizando un filtro pasa-bajos con una frecuencia de corte de ***800 Hz.***

Este filtro permitirá que pasen las frecuencias de 500 Hz y atenuará la componente de 1000 Hz.

- ***Componente a 500 Hz:*** Pasará sin cambios.
- ***Componente a 1000 Hz:*** Será atenuada o eliminada.

Después de aplicar el filtro pasa-bajos, la señal resultante contendrá principalmente la componente de ***500 Hz.***

1.5. Sistemas de modulación

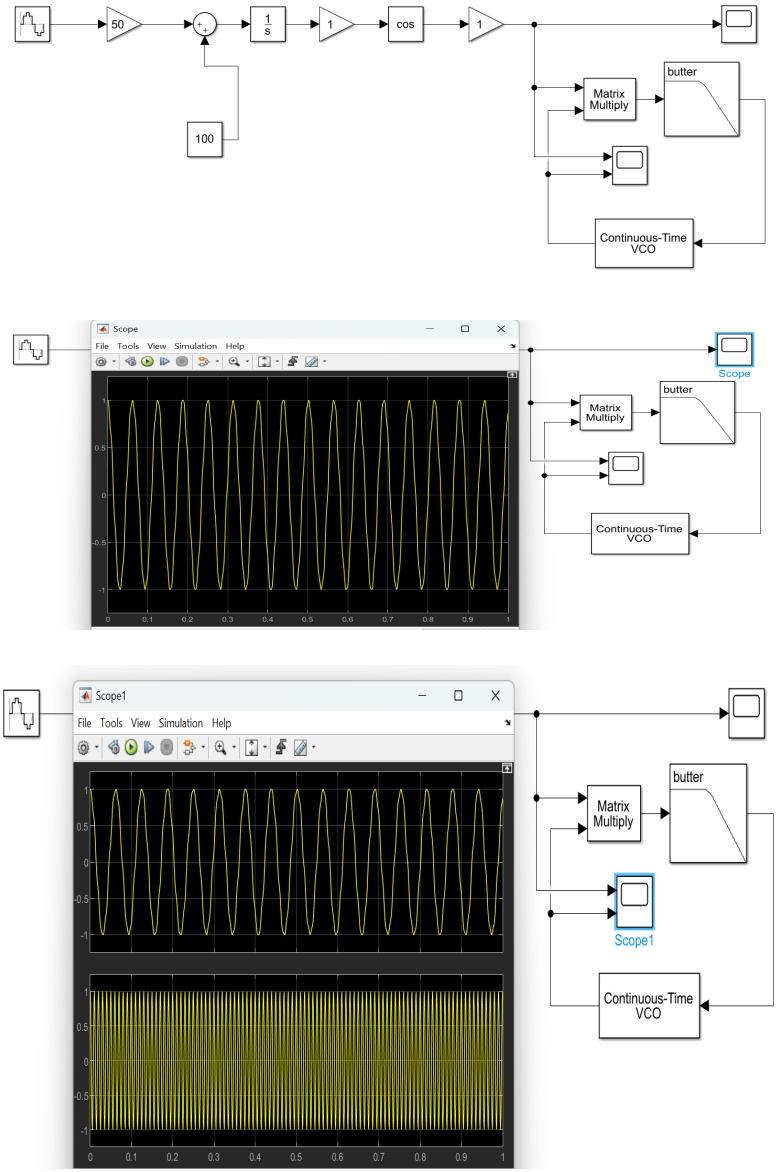
Los sistemas de modulación son técnicas utilizadas para transmitir señales de información (como voz, datos o video) a través de un medio de comunicación, como el aire (en radiofrecuencia) o cables (en comunicaciones alámbricas). La modulación consiste en alterar una señal portadora (que generalmente es una onda de alta frecuencia) en función de la señal de información (también llamada señal moduladora).

Modulación analógica

La modulación analógica es un proceso en el que una señal de información, como audio o video, se superpone a una señal portadora de alta frecuencia, modificando sus características (amplitud, frecuencia o fase) para facilitar la transmisión efectiva de la información. Este método incluye tres tipos principales: la modulación de amplitud (AM), donde varía la amplitud de la portadora, utilizada en la radio AM; la modulación de frecuencia (FM), que cambia la frecuencia de la portadora y es común en la radio FM y sistemas de audio por su mayor resistencia al ruido; y la modulación de fase (PM), que ajusta la fase de la portadora, aunque es menos común. Aunque la modulación analógica ha sido en gran medida reemplazada por métodos digitales más eficientes, sigue siendo un concepto fundamental en las comunicaciones, especialmente en aplicaciones tradicionales.

Ejemplo de circuito realizado en Simulink de Matlab.

Figura 13. Simulación de una modulación en SImulink.



En la Figura anterior se puede mirar los resultados de la simulación de una modulación realizada en el simulador SIMULIK de Matlab.

AM (Amplitud Modulated)

La modulación AM (Amplitud Modulada) es una técnica de transmisión donde la amplitud de una señal portadora de alta frecuencia se varía en función de la señal de información, como voz o música, mientras la frecuencia permanece constante. Es fácil de implementar y se utiliza en radios AM, aunque es sensible al ruido y menos eficiente que otros métodos como la modulación FM.

AM es un método para transportar información (voz, música, datos) haciendo que la "altura" de una onda rápida y estable, llamada portadora, suba y baje siguiendo el contorno del mensaje. Para la construcción se toma una portadora de alta frecuencia y se le ajusta su amplitud de acuerdo con la forma del audio o señal a enviar. La frecuencia de la portadora no cambia; lo que cambia es su amplitud.

En el espectro, además de la portadora, surgen dos "copias" del contenido alrededor de ella (bandas laterales superior e inferior). El espacio ocupado en frecuencia (ancho de banda) es, de forma aproximada, el doble de la frecuencia más alta del mensaje.

En AM, el receptor recupera el mensaje siguiendo la envolvente de la señal modulada: puede hacerlo con un detector de envolvente (diodo y filtro RC) o con un demodulador síncrono para reconstruir el audio original; esta técnica destaca por su simplicidad de circuitos, receptores de bajo costo y amplia cobertura en radiodifusión, aunque es poco eficiente en potencia porque la portadora no transporta información y resulta sensible al ruido que también altera la amplitud; por ello se emplea principalmente en radiodifusión AM, comunicaciones aeronáuticas y enlaces sencillos donde se privilegia la simplicidad sobre la eficiencia.

Ejemplo: Modulación de Amplitud (AM)

La modulación de amplitud se utiliza en la transmisión de radio AM. En este caso, una emisora de radio genera una señal de audio (como música o voz) que se convierte en una señal eléctrica. Esta señal de audio modula la amplitud de una onda portadora de alta frecuencia. Cuando se transmite, los receptores de radio captan esta señal y demodulan la información, reproduciendo el sonido original. La simplicidad de la AM la hace fácil de implementar, aunque sufre de interferencias y ruido, lo que puede afectar la calidad del sonido.

FM (Frecuencia Modulated)

La modulación FM (Frecuencia Modulada) es una técnica en la que se varía la frecuencia de la señal portadora en función de los cambios de la señal de información (como la voz o la música), mientras que su amplitud permanece constante. Esto permite una transmisión más resistente al ruido y a las interferencias en comparación con la AM, por lo que se usa ampliamente en la radiodifusión de alta fidelidad (radios FM) y en sistemas de comunicación como walkie-talkies y televisión. Aunque requiere un equipo más complejo para su generación y recepción, ofrece mejor calidad de sonido.

Ejemplo: Modulación de Frecuencia (FM)

La modulación de frecuencia es común en la transmisión de radio FM. En este caso, la información de audio modula la frecuencia de una señal portadora. Por ejemplo, cuando un locutor habla, la varia-

ción en la frecuencia de la portadora permite que se transmitan las diferentes tonalidades y matices de la voz. Los receptores de radio FM son capaces de desmodular esta señal, ofreciendo una calidad de sonido superior y una mayor resistencia a las interferencias en comparación con la AM. Este tipo de modulación es ampliamente utilizado en emisoras de música y programas de entretenimiento.

PM (Fase Modulated)

La modulación PM (Fase Modulada) es un tipo de modulación en la que se varía la fase de la señal portadora según los cambios de la señal de información, mientras su amplitud y frecuencia se mantienen constantes. Es similar a la modulación FM, ya que ambas pertenecen a la categoría de modulación angular, pero en PM los cambios ocurren directamente en la fase. Aunque es menos común en aplicaciones comerciales, se usa en sistemas digitales avanzados como las comunicaciones por satélite y ciertos estándares de telecomunicaciones debido a su capacidad para transmitir datos con alta precisión.

Ejemplo: Modulación de Fase (PM)

Imaginemos un sistema de comunicación que utiliza modulación de fase (PM) para transmitir datos binarios. Supongamos que queremos enviar la secuencia de bits: 101100.

Definición de fases:

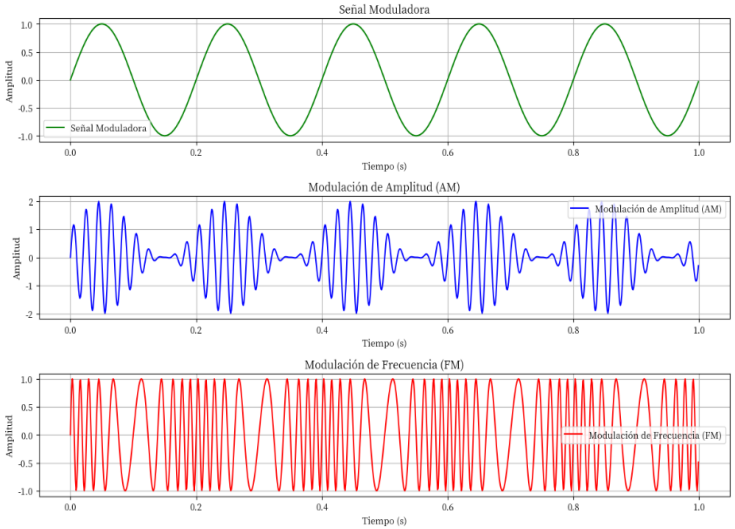
- 0° representa el bit 0.
- 180° representa el bit 1.
- Transmisión de la secuencia:
- Bit 1: Se transmite un 1, cambiamos la fase a 180°.
- Bit 0: Se transmite un 0, volvemos a 0°.
- Bit 1: Se transmite un 1, cambiamos la fase a 180°.
- Bit 1: Se transmite un 1, mantenemos la fase en 180°.
- Bit 0: Se transmite un 0, cambiamos a 0°.
- Bit 0: Se transmite un 0, mantenemos la fase en 0°.

Representación de la señal resultante alternará entre 0° y 180° de acuerdo con la secuencia de bits, como sigue:

- Desde 0° (0) a 180° (1)
- De 180° (1) a 0° (0)
- De 0° (0) a 180° (1)
- Desde 180° (1) se mantiene en 180° (1)
- De 180° (1) a 0° (0)
- Desde 0° (0) se mantiene en 0° (0)

Este cambio de fase permite al receptor interpretar la secuencia de bits correctamente. La modulación de fase es efectiva para la transmisión de datos debido a su capacidad para proporcionar una buena resistencia al ruido y a las interferencias.

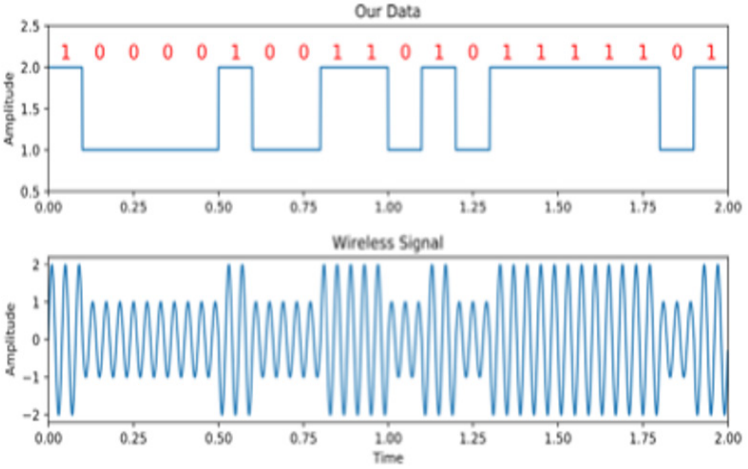
Figura 14. Modulación de amplitud y de frecuencia



1.6. Modulación digital

La modulación digital es una técnica que permite transmitir datos digitales (ceros y unos) a través de medios de comunicación analógicos, modificando características de una señal portadora, como la amplitud, frecuencia o fase. A diferencia de la modulación analógica, donde se transmite una señal continua (como la voz), en la modulación digital se transmite información binaria. Los métodos más comunes son ASK (modulación por amplitud), FSK (modulación por frecuencia) y PSK (modulación por fase), así como QAM, que combina amplitud y fase para aumentar la velocidad de transmisión. Estas técnicas son esenciales en redes de computadoras, telefonía móvil, Wi-Fi, televisión digital y sistemas de comunicación modernos.

Figura 15. Modulación digital



Ejercicios

Ejercicio de aplicación de la Modulación Digital.

Se presume que se está diseñando un sistema de comunicación digital que utiliza Modulación por Desplazamiento de Fase (PSK) para transmitir datos binarios. Se quiere enviar la siguiente secuencia de bits: 110101.

Paso 1: Definición de Fases aso 1: Definición de Fases

Definimos dos fases para la modulación:

- 0° representa el bit 0.
- 180° representa el bit 1.

Paso 2: Transmisión de la Secuencia

La secuencia por enviar es 110101. A continuación, se muestra cómo se modifica la fase de la señal portadora para cada bit:

- Bit 1: Fase 180°
- Bit 1: Fase 180° (se mantiene)
- Bit 0: Fase 0°
- Bit 1: Fase 180°
- Bit 0: Fase 0°
- Bit 1: Fase 180°

Paso 3: Representación de la Señal

La señal resultante alternará entre 0° y 180° de acuerdo con la secuencia de bits, como sigue:

Inicio: 0° (sin señal)

- 1: Cambia a 180°
- 1: Mantiene en 180°
- 0: Cambia a 0°
- 1: Cambia a 180°
- 0: Cambia a 0°
- 1: Cambia a 180°

Paso 4: Demodulación

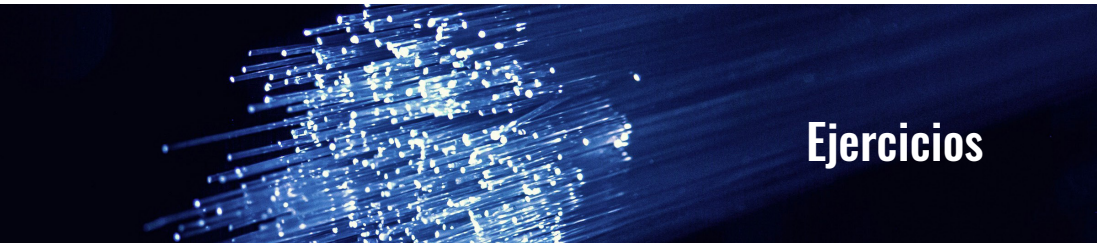
El receptor debe demodular la señal para recuperar la secuencia de bits original. Al detectar los cambios de fase, el receptor interpretará:

- 180° como 1
- 0° como 0

Al seguir la secuencia de fases, el receptor obtendrá la secuencia de bits: 110101.

1.6.1. ASK (Amplitude Shift Keying)

La modulación ASK (Amplitude Shift Keying) es una forma de modulación digital en la que se representa la información binaria (0 y 1) mediante cambios en la amplitud de una señal portadora, mientras que la frecuencia y la fase permanecen constantes. Por ejemplo, un "1" puede representarse con una onda de cierta amplitud y un "0" con una onda de menor amplitud o incluso sin señal. Es sencilla de implementar, pero sensible al ruido, ya que cualquier interferencia que afecte la amplitud puede provocar errores. Se utiliza en aplicaciones como controles remotos, RFID y sistemas de comunicación de baja velocidad.



Ejercicio de Aplicación: Modulación por Desplazamiento de Amplitud (ASK)

Vamos a diseñar un sistema de comunicación digital que utiliza Modulación por Desplazamiento de Amplitud (ASK) para transmitir datos binarios. Queremos enviar la siguiente secuencia de bits: 101100.

Paso 1: Definición de Amplitudes

Definimos dos niveles de amplitud para la modulación:

- Amplitud alta (A1) representa el bit 1.
- Amplitud baja (A0) representa el bit 0.

Suponiendo que:

- A1 = 5V (para el bit 1)
- A0 = 0V (para el bit 0)

Paso 2: Transmisión de la Secuencia

La secuencia por enviar es 101100. A continuación, se muestra cómo se modifica la amplitud de la señal portadora para cada bit:

- Bit 1: Amplitud 5V (A1)
- Bit 0: Amplitud 0V (A0)
- Bit 1: Amplitud 5V (A1)
- Bit 1: Amplitud 5V (A1)
- Bit 0: Amplitud 0V (A0)
- Bit 0: Amplitud 0V (A0)

Paso 3: Representación de la Señal

La señal resultante alternará entre las amplitudes definidas de acuerdo con la secuencia de bits, como sigue:

Inicio:

- 0V (sin señal)
- 1: Cambia a 5V
- 0: Cambia a 0V
- 1: Cambia a 5V
- 1: Mantiene en 5V
- 0: Cambia a 0V
- 0: Mantiene en 0V

Paso 4: Demodulación

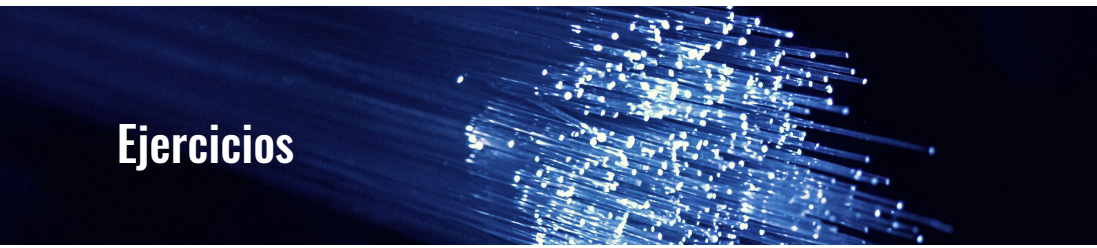
El receptor debe demodular la señal para recuperar la secuencia de bits original. Al detectar los niveles de amplitud, el receptor interpretará:

- 5V como 1
- 0V como 0

Al seguir la secuencia de amplitudes, el receptor obtendrá la secuencia de bits: 101100.

1.6.2. PSK (Phase Shift Keying)

La modulación PSK (Phase Shift Keying) es un tipo de modulación digital en la que la fase de la señal portadora se cambia para representar los datos binarios, mientras que su amplitud y frecuencia se mantienen constantes. Por ejemplo, en la forma más simple, llamada BPSK (Binary PSK), se usa una fase para el bit "0" y otra fase (generalmente opuesta) para el bit "1". Existen variantes más avanzadas como QPSK o 8-PSK, que usan más fases para transmitir varios bits por símbolo, aumentando la velocidad de transmisión. PSK es más resistente al ruido que ASK y se usa ampliamente en comunicaciones inalámbricas, Wi-Fi, GPS y redes móviles.



Ejercicios

Ejercicio de Aplicación: Modulación por Desplazamiento de Fase (PSK)

Vamos a diseñar un sistema de comunicación digital que utiliza Modulación por Desplazamiento de Fase (PSK) para transmitir datos binarios. Queremos enviar la siguiente secuencia de bits: 011010.

Paso 1: Definición de Fases

Definimos dos fases para la modulación:

- 0° representa el bit 0.
- 180° representa el bit 1.

Paso 2: Transmisión de la Secuencia

La secuencia por enviar es 011010. A continuación, se muestra cómo se modifica la fase de la señal portadora para cada bit:

- Bit 0: Fase 0°
- Bit 1: Fase 180°
- Bit 1: Fase 180° (se mantiene)
- Bit 0: Fase 0°
- Bit 1: Fase 180°
- Bit 0: Fase 0°

Paso 3: Representación de la Señal

La señal resultante alternará entre 0° y 180° de acuerdo con la secuencia de bits, como sigue:

- Inicio: 0° (sin señal)
- 0: Cambia a 0°
- 1: Cambia a 180°
- 1: Mantiene en 180°
- 0: Cambia a 0°
- 1: Cambia a 180°
- 0: Cambia a 0°

Paso 4: Demodulación

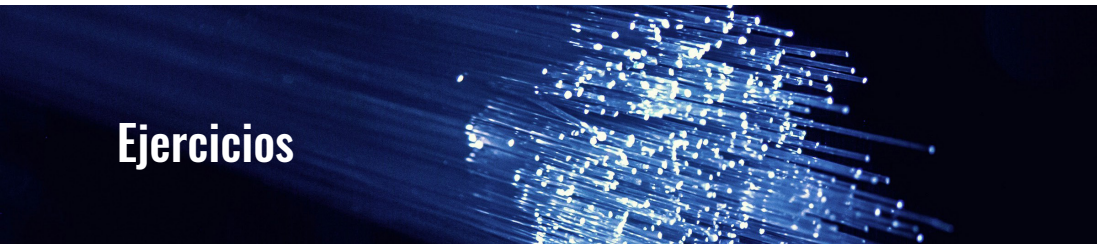
El receptor debe demodular la señal para recuperar la secuencia de bits original. Al detectar los cambios de fase, el receptor interpretará:

- 0° como 0
- 180° como 1

Al seguir la secuencia de fases, el receptor obtendrá la secuencia de bits: 011010.

1.6.3. QAM (Quadrature Amplitude Modulation)

La modulación QAM (Quadrature Amplitude Modulation) combina variaciones en la amplitud y la fase de una señal portadora para transmitir datos digitales, permitiendo enviar múltiples bits por cada símbolo. Por ejemplo, en 16-QAM, se usan 16 combinaciones distintas de amplitud y fase para representar 4 bits por símbolo. Esta técnica es muy eficiente en términos de velocidad de transmisión, por lo que se utiliza ampliamente en sistemas como Wi-Fi, televisión digital, 4G/5G y módems de internet. Aunque QAM ofrece alta capacidad de datos, es más sensible al ruido y a la distorsión que otras modulaciones más simples.



Ejercicios

Ejercicio de Aplicación: Modulación por Amplitud en Cuadratura (QAM)

Vamos a diseñar un sistema de comunicación digital que utiliza Modulación por Amplitud en Cuadratura (QAM) para transmitir datos binarios. En este caso, utilizaremos 16-QAM, que permite transmitir 4 bits por símbolo.

Paso 1: Definición de Niveles de Amplitud y Fases

En 16-QAM, combinamos 4 niveles de amplitud y 4 fases. Definimos los niveles de amplitud y las fases como sigue:

Niveles de Amplitud:

- A1 = 1 (nivel bajo)
- A2 = 3 (nivel medio)
- A3 = 5 (nivel alto)
- A4 = 7 (nivel muy alto)

Fases:

- 0° (0)
- 90° (1)
- 180° (2)
- 270° (3)

Paso 2: Mapeo de Bits a Símbolos

Para 16-QAM, cada símbolo representa 4 bits. A continuación, mapeamos los bits a símbolos:

Bits	*Símbolo*	*Amplitud*	*Fase*
0000	S1	A1	0°
0001	S2	A1	90°
0010	S3	A1	180°
0011	S4	A1	270°
0100	S5	A2	0°

Bits	Símbolo	Amplitud	Fase
0101	S6	A2	90°
0110	S7	A2	180°
0111	S8	A2	270°
1000	S9	A3	0°
1001	S10	A3	90°
1010	S11	A3	180°
1011	S12	A3	270°
1100	S13	A4	0°
1101	S14	A4	90°
1110	S15	A4	180°
1111	S16	A4	270°

Paso 3: Secuencia de Bits a Transmitir

Suponiendo que queremos enviar la secuencia de bits: 11010111. Dividimos esta secuencia en grupos de 4 bits:

- 1101 →Símbolo S14 (A4, 90°)
- 0111 → Símbolo S8 (A2, 270°)

Paso 4: Transmisión de la Señal

La transmisión de la señal se realiza en dos componentes:

- Componente en fase (I) para la amplitud y fase.
- Componente en cuadratura (Q) para la amplitud y fase.
- Símbolo S14: Amplitud A4 (7) y fase 90° → (0, 7)
- Símbolo S8: Amplitud A2 (3) y fase 270° → (-3, 0)

Paso 5: Demodulación

El receptor debe demodular la señal para recuperar la secuencia de bits original. Al detectar los niveles de amplitud y las fases, el receptor interpretará los símbolos y recuperará la secuencia de bits:

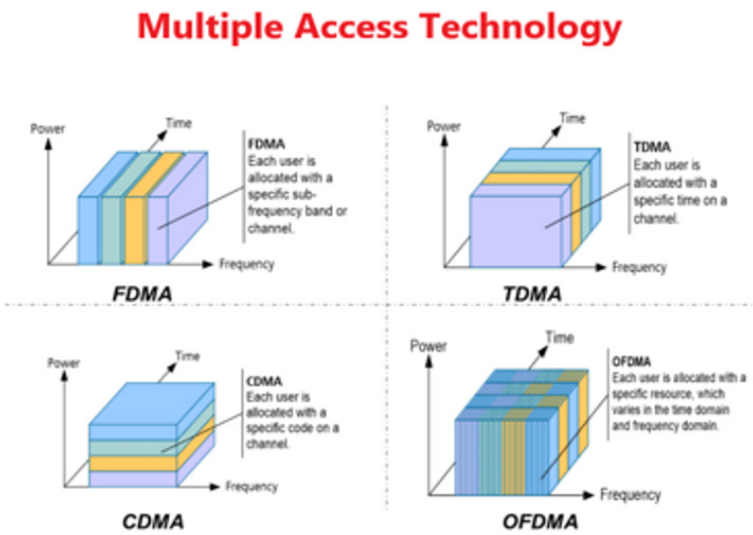
- S14 →1101
- S8 →0111

Por lo tanto, la secuencia de bits recuperada será 11010111.

1.7. Técnicas de acceso múltiples

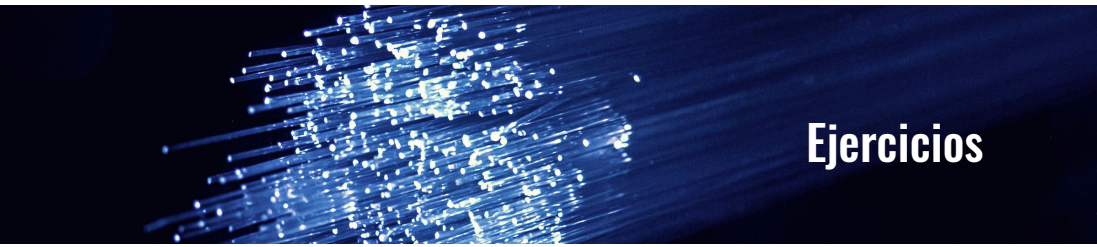
Las técnicas de acceso múltiple son métodos utilizados en sistemas de telecomunicaciones para permitir que múltiples usuarios compartan de manera eficiente los recursos de un canal de comunicación, como el espectro de frecuencias, el tiempo o el espacio. Estas técnicas son esenciales en redes inalámbricas, satelitales y sistemas de comunicación modernos, donde varios dispositivos necesitan transmitir datos simultáneamente.

Figura 16. Modulación digital múltiples accesos



FDMA (Frequency Division Multiple Access)

FDMA (Frequency Division Multiple Access) es una técnica de acceso múltiple que permite que varios usuarios compartan un canal de comunicación dividiendo el ancho de banda total disponible en canales de frecuencia separados. A cada usuario se le asigna una frecuencia específica de manera continua durante toda la comunicación, lo que evita interferencias entre usuarios. Este método se utilizó ampliamente en las primeras generaciones de redes celulares (como 1G) y también se aplica en sistemas de radio, televisión y satélites. Aunque es simple y confiable, no aprovecha eficientemente el canal si un usuario no está transmitiendo constantemente.



Ejercicios

Ejercicio de Aplicación: Acceso Múltiple por División de Frecuencia (FDMA)

Vamos a diseñar un sistema de comunicación que utiliza Acceso Múltiple por División de Frecuencia (FDMA) para permitir que múltiples usuarios compartan el mismo medio de comunicación. En este caso, consideraremos un canal de comunicación que se divide en varias frecuencias para diferentes usuarios.

Paso 1: Definición del Canal

Supongamos que tenemos un canal de comunicación con un ancho de banda total de 20 MHz. Vamos a dividir este canal en 4 frecuencias para diferentes usuarios.

Paso 2: Asignación de Frecuencias

Dividimos el ancho de banda total en 4 partes iguales:

- Frecuencia 1: 0 MHz a 5 MHz (Usuario A)
- Frecuencia 2: 5 MHz a 10 MHz (Usuario B)
- Frecuencia 3: 10 MHz a 15 MHz (Usuario C)
- Frecuencia 4: 15 MHz a 20 MHz (Usuario D)

Paso 3: Transmisión de Datos

Cada usuario puede transmitir datos en su frecuencia asignada sin interferir con los demás. Supongamos que cada usuario envía la siguiente cantidad de datos en un período de tiempo determinado:

- Usuario A: 1000 bits
- Usuario B: 1200 bits
- Usuario C: 800 bits
- Usuario D: 1500 bits

Paso 4: Modulación y Transmisión

Cada usuario modula sus datos utilizando una técnica de modulación adecuada (por ejemplo, QAM, PSK, etc.) en su frecuencia asignada.

- Usuario A (0-5 MHz): Envía 1000 bits.
- Usuario B (5-10 MHz): Envía 1200 bits.
- Usuario C (10-15 MHz): Envía 800 bits.
- Usuario D (15-20 MHz): Envía 1500 bits.

Paso 5: Recepción de Datos

El receptor está diseñado para recibir señales en cada una de las frecuencias asignadas. Utiliza filtros para separar las señales de cada usuario:

- Frecuencia 1: Recibe datos del Usuario A.
- Frecuencia 2: Recibe datos del Usuario B.
- Frecuencia 3: Recibe datos del Usuario C.
- Frecuencia 4: Recibe datos del Usuario D.

Paso 6: Demodulación

Cada usuario demodula su señal en el receptor para recuperar los datos originales:

- Usuario A: Recupera 1000 bits.
- Usuario B: Recupera 1200 bits.
- Usuario C: Recupera 800 bits.
- Usuario D: Recupera 1500 bits.

CDMA (Code Division Multiple Access)

El CDMA (Code Division Multiple Access) es una técnica de acceso múltiple utilizada en comunicaciones inalámbricas que permite que múltiples usuarios transmitan simultáneamente sobre la misma frecuencia. Cada usuario se identifica mediante un código único, lo que permite que las señales se separen y se decodifiquen en el receptor, incluso si se superponen en el tiempo y la frecuencia. Esta tecnología mejora la eficiencia del espectro y la capacidad de la red, siendo fundamental en sistemas como la telefonía móvil y la transmisión de datos.

TDMA (Time Division Multiple Access)

El TDMA (Time Division Multiple Access) es una técnica de acceso múltiple que divide el tiempo en intervalos o ranuras, permitiendo que múltiples usuarios compartan el mismo canal de comunicación. En este sistema, cada usuario tiene asignada una ranura de tiempo específica durante la cual puede transmitir su información, evitando así interferencias y colisiones. Esta metodología es eficiente en la gestión del espectro y se utiliza comúnmente en redes de telefonía móvil y sistemas de comunicación digital, donde se requiere una organización clara del tiempo para maximizar la capacidad y calidad de la transmisión.

1.7.1. Ventajas de la modulación digital

La modulación digital ofrece varias ventajas en comparación con la modulación analógica. Algunas de las principales ventajas pueden ser:

- ***Mayor resistencia al ruido:*** Las señales digitales son menos susceptibles a interferencias y ruido, lo que mejora la calidad de la transmisión.

- ***Eficiencia en el uso del espectro:*** Permite una mejor utilización del espectro de frecuencia, lo que puede aumentar la capacidad de la red.
- ***Facilidad de procesamiento:*** Las señales digitales son más fáciles de procesar y manipular mediante técnicas de codificación y compresión.
- ***Seguridad:*** La modulación digital puede incluir técnicas de encriptación, lo que hace más difícil la interceptación y el acceso no autorizado a la información.
- ***Compatibilidad con sistemas digitales:*** Se integra fácilmente con otros sistemas digitales, como computadoras y redes, facilitando la transmisión de datos.
- ***Mejor calidad de audio y video:*** Permite la transmisión de señales de alta calidad, como audio y video, sin degradación significativa.
- ***Facilidad de implementación de técnicas de corrección de errores:*** Se pueden aplicar algoritmos de corrección de errores para mejorar la fiabilidad de la comunicación.

Estas ventajas hacen que la modulación digital sea la opción preferida en muchas aplicaciones modernas de telecomunicaciones.

Robustez a ruidos e interferencias

La robustez a ruidos e interferencias en sistemas de comunicación se refiere a la capacidad de las señales digitales para mantener su integridad a pesar de perturbaciones externas. Gracias a su representación en forma de bits, las señales digitales son menos susceptibles a variaciones menores. Además, técnicas de modulación como PSK y QAM, junto con algoritmos de corrección de errores, mejoran la fiabilidad de la transmisión. El uso de filtros digitales y estrategias de repetición y diversificación también contribuyen a asegurar que, incluso en entornos ruidosos, la información se reciba correctamente, lo que hace que la modulación digital sea altamente eficaz en aplicaciones modernas.

Posibilidad de encriptación

La posibilidad de encriptación en sistemas de comunicación digital permite codificar información para que solo los destinatarios autorizados puedan acceder a ella, garantizando así la confidencialidad de los datos sensibles. Además, la encriptación contribuye a la integridad de la información al verificar que no ha sido alterada durante la transmisión y facilita la autenticación de usuarios y dispositivos. Las técnicas modernas de encriptación son difíciles de romper, proporcionando una sólida resistencia contra ataques cibernéticos, y su implementación es fundamental para cumplir con regulaciones y normativas de seguridad. En conjunto, la encriptación es esencial para proteger la seguridad y privacidad de la información en un entorno interconectado.

Capacidad de comprimir dados

La capacidad de comprimir datos en sistemas de comunicación digital permite reducir el tamaño de la información transmitida, lo que optimiza el uso del ancho de banda y permite almacenar más datos en menos espacio, beneficiando a dispositivos con recursos limitados. Esta compresión no solo reduce costos de transmisión y almacenamiento, sino que también mejora la velocidad de transferencia al enviar menos bits a través de la red. Además, los archivos más pequeños son más fáciles de manejar y compartir, lo que mejora la experiencia del usuario en aplicaciones de comunicación y almacenamiento. En conjunto, la compresión de datos es esencial para mejorar la eficiencia y optimizar el manejo de la información en un entorno interconectado.

1.7.2. Principios de la transmisión

La transmisión se refiere al proceso mediante el cual se envía información, señales o datos de un lugar a otro, ya sea a través de medios físicos como cables o de forma inalámbrica mediante ondas electromagnéticas. Para que este proceso sea eficiente y confiable, existen ciertos principios fundamentales que lo rigen.

Un principio clave es la modulación, que consiste en adaptar la señal de información para que pueda ser transmitida a través de un medio específico. Esto se logra combinando la señal original con una portadora, lo que facilita su propagación a largas distancias y su separación de otras señales en el mismo medio.

Otro principio importante es el uso eficiente del espectro, especialmente en sistemas inalámbricos. Dado que el espectro de frecuencias es un recurso limitado, es esencial gestionar su uso de manera adecuada para evitar interferencias y permitir que múltiples usuarios puedan transmitir simultáneamente.

La integridad de la señal también es fundamental. Durante la transmisión, las señales pueden degradarse debido a factores como el ruido, la atenuación o las interferencias. Por ello, se emplean técnicas como la amplificación, la corrección de errores y la codificación para garantizar que los datos lleguen al receptor de manera precisa y sin alteraciones.

Además, la sincronización entre el transmisor y el receptor es esencial para que la comunicación sea efectiva. Esto implica coordinar aspectos como el tiempo y las frecuencias utilizadas, asegurando que el receptor pueda interpretar correctamente la información recibida.

En resumen, los principios de la transmisión incluyen la modulación, el uso eficiente del espectro, la preservación de la integridad de la señal y la sincronización. Estos elementos son esenciales para garantizar que la información se transmita de forma confiable y eficiente en cualquier sistema de comunicación.

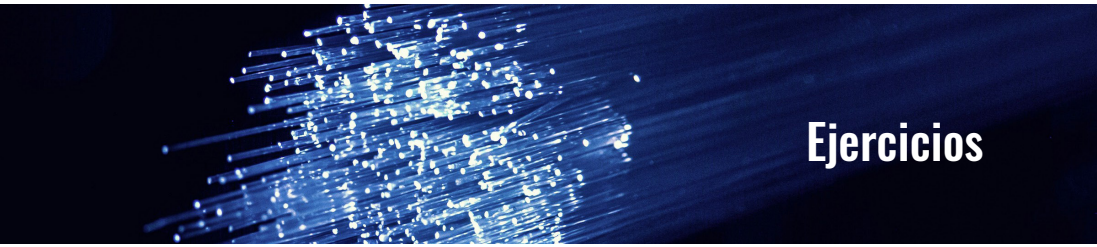
1.8. Propagación de señales

La propagación de señales se refiere al proceso mediante el cual las ondas electromagnéticas se transmiten a través de diferentes medios, y se clasifica en medios guiados y no guiados. En los medios guiados, como cables coaxiales y fibra óptica, las señales se transmiten de manera controlada con menor pérdida de señal, mientras que, en los medios no guiados, como ondas de radio, microondas e infrarrojos, las señales viajan a través del aire, lo que permite la comunicación inalámbrica, pero las hace más susceptibles a interferencias y obstáculos. Factores como la frecuencia, la presencia de obstáculos físicos y las condiciones atmosféricas afectan la calidad de la propagación, lo que es crucial para diseñar sistemas de comunicación eficientes y optimizar la cobertura en diversas aplicaciones.

1.8.1. Atenuación

La atenuación se refiere a la disminución de la intensidad de una señal a medida que se propaga a través de un medio, ya sea guiado o no guiado, y es un factor crítico en las comunicaciones. Este fenómeno puede ser causado por diversas razones, como la absorción de energía por el medio, la dis-

persión de la señal y las reflexiones en superficies. En medios guiados, como cables y fibras ópticas, la atenuación puede resultar de la resistencia eléctrica y las imperfecciones en el material, mientras que, en medios no guiados, factores como la distancia, la frecuencia de la señal y las condiciones atmosféricas juegan un papel importante. La atenuación impacta la calidad de la comunicación, ya que puede llevar a la pérdida de datos y la necesidad de amplificación o repetición de la señal para mantener la integridad de la información transmitida.



Ejercicios

Ejercicio sobre Atenuación en Comunicaciones

En este ejercicio, exploraremos el concepto de atenuación en diferentes medios de comunicación y cómo afecta la calidad de la señal. Utilizaremos ejemplos prácticos tanto en medios guiados como no guiados.

Parte 1: Atenuación en Medios Guiados

Ejemplo: Supongamos que tenemos un cable de par trenzado que se utiliza para transmitir datos en una red local. La longitud del cable es de ***150 metros*** y la atenuación del cable es de ***0.5 dB/m***.

Calcular la atenuación total:

Fórmula:

- Atenuación Total (dB)=Longitud del Cable (m)×Atenuación (dB/m)
- Sustituyendo los valores
- Atenuación Total=150 m×0.5 dB/m=75 dB

Interpretar el resultado:

La señal pierde ***75 dB*** a lo largo de los ***150 metros*** del cable. Esto significa que la intensidad de la señal se ha reducido significativamente, lo que podría afectar la calidad de la comunicación.

Parte 2: Atenuación en Medios No Guiados

Ejemplo: Consideremos una señal de microondas que se transmite a través del aire. La frecuencia de la señal es de ***2.4 GHz***, y la distancia entre el transmisor y el receptor es de ***100 metros.*** La atenuación en el aire a esta frecuencia es de aproximadamente ***0.2 dB/m.***

Calcular la atenuación total:

- Fórmula: Atenuación Total (dB)=Distancia (m)×Atenuación (dB/m)
- Sustituyendo los valores:
- Atenuación Total=100 m×0.2 dB/m=20 dB

Interpretar el resultado:

La señal pierde ***20 dB*** a lo largo de los ***100 metros*** en el espacio. Aunque la pérdida es menor que en el cable de par trenzado, todavía puede afectar la calidad de la comunicación, especialmente si hay obstáculos o interferencias.

Parte 3: Comparación y Conclusiones

Comparar la atenuación en ambos medios:

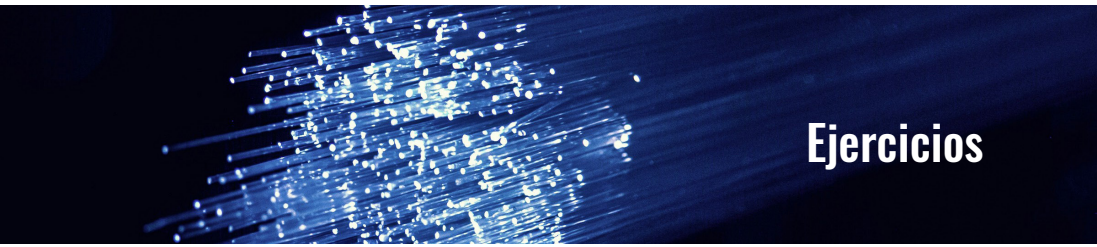
- ***Par Trenzado:*** 75 dB en 150 m.
- ***Microondas:*** 20 dB en 100 m.

Discusión:

- La atenuación en el par trenzado es considerablemente mayor que en la transmisión de microondas, lo que resalta cómo los medios guiados pueden ser más susceptibles a la pérdida de señal debido a la resistencia y las imperfecciones del material.
- En medios no guiados, aunque la atenuación es menor, factores externos como la interferencia atmosférica y obstáculos pueden tener un impacto significativo en la calidad de la señal.

1.8.2. Interferencia

La interferencia se refiere a la distorsión o degradación de una señal de comunicación causada por la superposición de múltiples señales, ya sean deseadas o no deseadas. Este fenómeno puede ocurrir en medios guiados y no guiados, y puede ser de varios tipos, como interferencia constructiva, donde las señales se suman y aumentan la amplitud, o interferencia destructiva, donde se cancelan entre sí, reduciendo la calidad de la señal. Factores como la proximidad a otras fuentes de señal, el tipo de modulación utilizada y el entorno físico pueden influir en la cantidad y tipo de interferencia experimentada. La interferencia puede resultar en la pérdida de datos, errores en la transmisión y una disminución general en la calidad de la comunicación, lo que hace esencial implementar técnicas de mitigación, como el uso de filtros, técnicas de modulación robustas y la planificación cuidadosa de la red.



Ejercicios

Ejercicio Breve sobre Interferencia en Comunicaciones

Imagina que estás configurando una red Wi-Fi que opera en la banda de ***2.4 GHz.*** La potencia de transmisión de la señal de Wi-Fi es de ***20 dBm***, y hay interferencia de un dispositivo que tiene una potencia de ***-70 dBm***.

Parte 1: Calcular la Relación Señal a Interferencia (SIR)

Calcular la SIR:

- Fórmula: SIR (dB)=Pseñal-Pinterferencia
- Sustituyendo los valores: SIR=20 dBm-(-70 dBm) =20+70=90 dB

Interpretar el resultado:

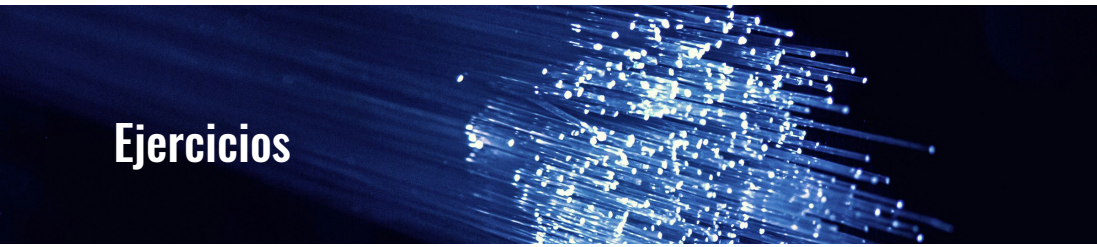
- Una SIR de ***90 dB*** indica que la señal de Wi-Fi es mucho más fuerte que la interferencia, lo que sugiere una buena calidad de conexión.

1.8.3. Ancho de banda y capacidad de transmisión

El ancho de banda y la capacidad de transmisión son conceptos fundamentales en las comunicaciones que se refieren a la cantidad de datos que pueden ser transmitidos a través de un canal en un período de tiempo determinado.

Ancho de banda

El ancho de banda se refiere a la diferencia entre las frecuencias más bajas y más altas que un canal puede transmitir, generalmente medido en hertzios (Hz). Un mayor ancho de banda permite la transmisión de más datos simultáneamente, lo que se traduce en velocidades de conexión más rápidas y una mejor calidad de servicio.



Ejercicios

Ejercicio sobre Ancho de Banda en Comunicaciones

Imagine que estás configurando una red de datos para una pequeña oficina. La conexión a Internet tiene un ancho de banda de ***100 Mbps*** (megabits por segundo).

Parte 1: Calcular la Capacidad de Transferencia de Datos

Calcular la cantidad de datos que se pueden transferir en 1 minuto:

$$Fórmula: Datos\ transferidos\ (MB) = \frac{Ancho\ de\ banda\ (Mbps) x 60}{8}$$

$$Sustituyendo\ los\ valores: (MB) = \frac{100 Mbps x 60}{8} = 750 MB$$

Parte 2: Interpretar el Resultado

Interpretación: En 1 minuto, se pueden transferir ***750 MB*** de datos a través de la conexión de ***100 Mbps.***

Capacidad de transmisión

La capacidad de transmisión, por otro lado, es la cantidad máxima de datos que puede ser transmitida a través de un canal en un segundo, comúnmente expresada en bits por segundo (bps). Esta capacidad está influenciada no solo por el ancho de banda, sino también por factores como la modulación utilizada, la calidad del medio de transmisión y la presencia de interferencias.

Ejercicio sobre capacidad de transmisión en comunicaciones

Supongamos que tienes una conexión de red que tiene un ancho de banda de 50 Mbps. Sin embargo, debido a factores como interferencias y la calidad del medio de transmisión, la capacidad de transmisión efectiva es solo el 70% del ancho de banda total.

Parte 1: Calcular la capacidad de transmisión

1. Calcular la capacidad de transmisión efectiva:

Fórmula:Capacidad de transmisión (bps)=Ancho de banda (bps)x Eficiencia

Dónde:

- Ancho de banda: 50mbps=50x10^{6}bps
- Eficiencia=70%

Capacidad de transmisión=50x10^6 bps x 0,7= 35x10^6 bps=35mbps

Parte 2: Interpretar el Resultado

- ***Interpretación:*** La capacidad de transmisión efectiva de la conexión es de 35 Mbps, lo que significa que, a pesar de tener un ancho de banda de 50 Mbps, solo se pueden transmitir 35 Mbps de datos de manera efectiva debido a factores como interferencias y la calidad del medio.

1.9. Multiplexado

El multiplexado es una técnica esencial en las telecomunicaciones modernas que permite transmitir varias señales independientes a través de un solo canal físico. Por ejemplo, en las redes de telefonía fija digital, el sistema E1 utilizado en Europa y América Latina puede transportar hasta 30 llamadas simultáneas por un mismo cable utilizando multiplexado por división de tiempo (TDM). Esto optimiza la infraestructura, ya que no es necesario instalar una línea para cada llamada, lo que reduce costos y facilita la expansión de la red. Además, el TDM es ampliamente utilizado en redes de datos como Ethernet, donde distintos paquetes viajan por el mismo canal en diferentes intervalos de tiempo.

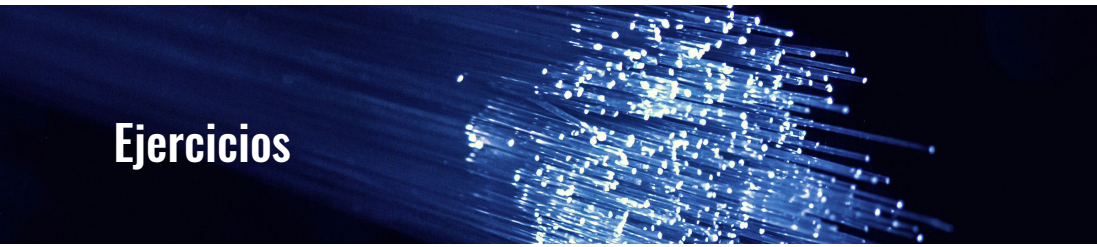
1.9.1. FDM (Frequency Division Multiplexing)

Asigna diferentes bandas de frecuencia a cada señal. Cada señal se modula en una frecuencia diferente, permitiendo que múltiples señales se transmitan simultáneamente a través del mismo medio.

Es una técnica que permite transmitir múltiples señales simultáneamente a través de un único medio de comunicación, asignando a cada señal un rango de frecuencia distinto dentro del ancho de banda disponible. Cada señal se modula en una portadora de frecuencia única, lo que evita interferencias entre ellas, y en el receptor se utilizan filtros para separar y de modular cada canal. Esta técnica es fundamental en sistemas como la radiodifusión AM/FM, la televisión analógica y las primeras redes telefónicas, donde su simplicidad y eficiencia en el uso del espectro fueron clave, aunque su desventaja es el desperdicio de ancho de banda cuando los canales no están activos.

FDM tiene variedad de aplicaciones, entre las siguientes:

- ***Radiodifusión AM/FM:*** Cada emisora opera en una frecuencia específica dentro del espectro radioeléctrico, permitiendo que múltiples estaciones transmitan simultáneamente sin interferencias.
- ***Televisión analógica:*** Los canales de TV tradicionales asignaban diferentes frecuencias para video, audio y sub-canales, usando FDM para su distribución.
- ***Telefonía fija (antiguos sistemas):*** En las primeras redes telefónicas, FDM permitía multiplexar hasta 24 llamadas sobre un mismo cable coaxial mediante portadoras de frecuencia distinta (ej: sistemas carrier).
- ***Comunicaciones por satélite:*** Los transpondedores satelitales dividen el ancho de banda en sub-canales de frecuencia para transmitir múltiples señales (TV, voz, datos).
- ***Redes de cable (HFC - Hibrid Fiber Coaxial):*** Combina FDM con fibra óptica para distribuir señales de internet, TV y telefonía por cable.



Ejercicios

Ejercicio sobre Multiplexado por División de Frecuencia (FDM)

Contexto: Se está diseñando un sistema de comunicaciones utilizando Multiplexado por División de Frecuencia (FDM) para optimizar la transmisión de múltiples señales a través de un único medio.

Parte 1: Cálculo de Frecuencias Asignadas

1. Calcular el número de canales:

Se admite que se tiene un ancho de banda total de 300 MHz disponible para transmisión.Si cada canal necesita un ancho de banda de 10 MHz, ¿cuántos canales se pueden transmitir simultáneamente?

Cálculo:

$$Número\ de\ canales = \frac{300MHz}{10MHz} = 30\ canales$$

Parte 2: Comparación de Uso de Frecuencia

2. Uso en Radiodifusión:

- Si una emisora de radio opera en una frecuencia de 101.5 MHz y necesita un ancho de banda de 200 kHz, ¿qué rango de frecuencias ocupa?
- ***Cálculo:***

Rango Ocupado=101.5MHz-0.1MHz (inferior) a 101.5MHz+0.1MHz (superior)=[101.4MHz,101.6MHz]

Parte 3: Aplicaciones Prácticas

Pregunta: Identifica dos aplicaciones de FDM en las que se utilicen estas capacidades de transmisión.

Respuestas:

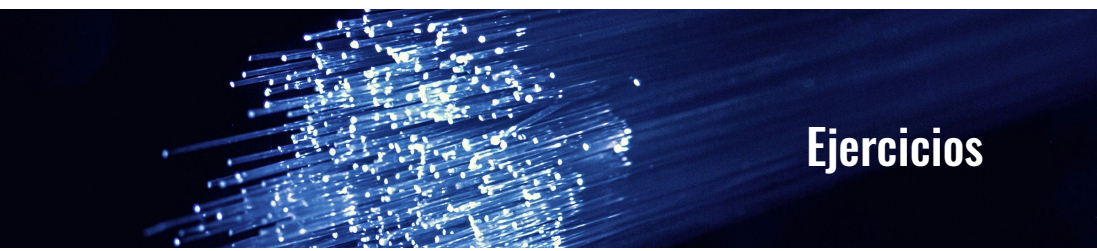
- Radiodifusión AM/FM donde múltiples emisoras transmiten simultáneamente.
- Comunicaciones por satélite que utilizan sub-canales de frecuencia para transmitir diferentes tipos de señales.

1.9.2. TDM (Time Division Multiplexing)

Asigna intervalos de tiempo específicos a cada señal en el canal. Cada señal se transmite en su propio "slot" de tiempo, permitiendo que múltiples señales compartan el mismo medio sin interferirse.

Es una técnica de transmisión que permite compartir un mismo canal de comunicación entre múltiples señales asignando a cada una un intervalo de tiempo específico (time slot) dentro de un ciclo repetitivo. A diferencia de FDM, que divide el ancho de banda en frecuencias, TDM organiza las señales en ráfagas secuenciales que se transmiten en rápida sucesión, aprovechando al máximo la capacidad del medio. Esta técnica es especialmente eficiente para señales digitales, ya que cada señal ocupa todo el ancho de banda durante su slot asignado, evitando interferencias mediante sincronización precisa. TDM es fundamental en tecnologías como redes telefónicas (ej: sistemas E1/T1), comunicaciones móviles GSM y redes de fibra óptica (SONET/SDH), donde su capacidad para manejar múltiples flujos de datos con baja latencia lo hace ideal para aplicaciones que requieren alta eficiencia y escalabilidad. Su principal ventaja es la optimización del ancho de banda, aunque requiere una estricta sincronización entre emisor y receptor para evitar solapamientos. Dentro de las aplicaciones que tiene TDM se puede ver las siguientes:

- ***Telefonía tradicional (POTS):*** Sistemas E1 (Europa) y T1 (EE.UU.) que multiplexan 30/24 llamadas telefónicas respectivamente sobre un único enlace físico mediante slots de tiempo predefinidos.
- ***Redes ópticas (SONET/SDH):*** Transporte jerárquico de datos a alta velocidad (hasta 40 Gbps) mediante estructuras TDM síncronas, utilizadas en redes troncales de operadores.
- ***Redes digitales de acceso (PON):*** Tecnologías como GPON usan TDM para compartir fibra óptica entre múltiples usuarios en redes FTTH (Fiber to the Home).
- ***Comunicaciones satelitales:*** Asignación eficiente de ancho de banda entre estaciones terrenas mediante slots temporales en enlaces TDMA.



Ejercicio sobre Multiplexado por División de Tiempo (TDM)

Estás diseñando un sistema de comunicaciones utilizando ***Multiplexado por División de Tiempo (TDM)*** para optimizar el uso del ancho de banda en un enlace de comunicación.

Parte 1: Cálculo de Slots de Tiempo

Calcular el número de llamadas:

Suponiendo que un sistema E1 puede multiplexar 30 llamadas telefónicas utilizando slots de tiempo. Si cada llamada ocupa un slot de 125 ms en un ciclo de 3 segundos, ¿cuántas llamadas se pueden realizar en un ciclo completo?

Cálculo: Ciclo Total=3000 ms125 ms=24 slots

- Por lo tanto, el sistema puede manejar 30 llamadas simultáneas en un ciclo.

Parte 2: Comparación de Capacidad

Capacidad en redes móviles GSM:

- En una red GSM, si un canal puede manejar hasta 8 conversaciones simultáneas y se utilizan 4 canales, ¿cuál es la capacidad total de conversaciones simultáneas?
- Cálculo: Capacidad Total=4×8=32 conversaciones

Parte 3: Aplicaciones Prácticas

Pregunta: Identifica dos aplicaciones de TDM en las que se utilicen estas capacidades de transmisión.

Respuestas:

- Telefonía tradicional (sistemas E1 y T1).
- Redes ópticas (SONET/SDH).

1.9.3. WDM (Wavelength Division Multiplexing)

Utilizado en fibras ópticas, este método permite que múltiples longitudes de onda de luz se transmitan a través de la misma fibra, aumentando significativamente la capacidad de transmisión.

Es una tecnología óptica que permite transmitir múltiples señales de datos simultáneamente a través de una sola fibra óptica, utilizando diferentes longitudes de onda (colores) de luz láser. Cada señal viaja en su propia longitud de onda sin interferir con las demás, multiplicando exponencialmente la capacidad de transmisión. Existen dos variantes principales: CWDM (hasta 18 canales con separación de 20 nm, ideal para distancias cortas) y DWDM (hasta 160 canales con separación de 0.8 nm, para enlaces transoceánicos). Dentro de las aplicaciones se tiene las siguientes:

- Redes troncales de Internet: Conexiones de alta capacidad entre continentes (ej: cables submarinos).
- Centros de datos: Interconexión de servidores con terabits/s de ancho de banda.
- Telecomunicaciones 5G: Transporte de gran volumen de datos en redes metropolitanas.
- Televisión por cable (HFC): Distribución de señales de video sobre fibra.

1.9.4. SDM (Space Division Multiplexing)

Es una tecnología avanzada que incrementa la capacidad de transmisión en redes de comunicaciones al utilizar múltiples canales espaciales independientes dentro de un mismo medio físico. A diferen-

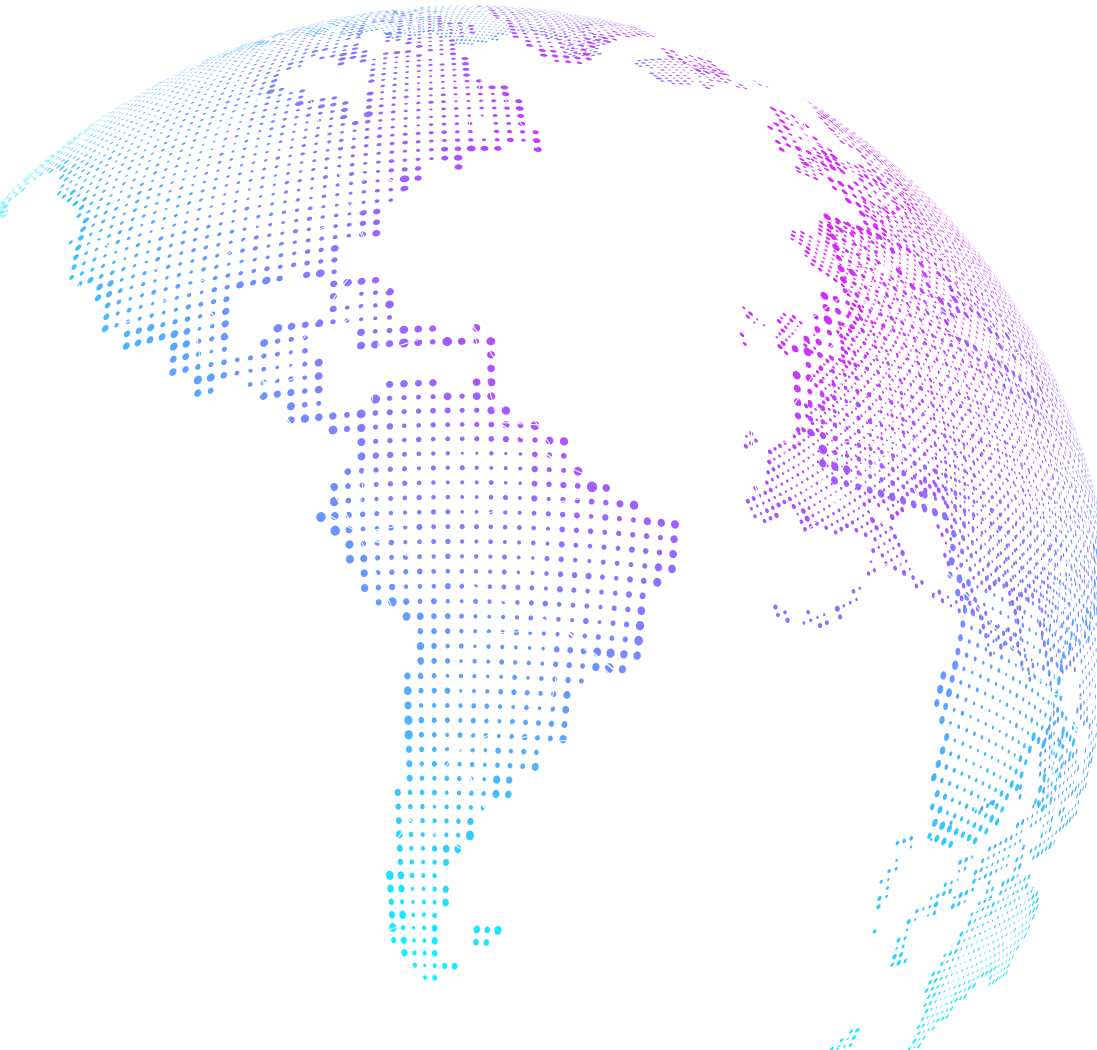
cia de técnicas como WDM (que usa longitudes de onda) o TDM (que divide el tiempo), SDM aprovecha la dimensión física del espacio. Dentro de las aplicaciones que tiene SDM están las siguientes:

- Redes 5G/6G: Aumenta la capacidad mediante MIMO masivo (ej: antenas con 64 o 128 elementos)
- Centros de datos: Fibras multi núcleo para interconexiones de alta densidad (hasta 1 Petabit/s por cable).
- Comunicaciones submarinas: Amplía la capacidad de cables transoceánicos sin tender nuevas fibras.
- LiFi: Usa modos espaciales de luz para transmisiones paralelas en comunicaciones por luz visible.

El multiplexado es una técnica que permite la transmisión simultánea de múltiples señales a través de un solo canal de comunicación, lo que ofrece varias ventajas significativas. En primer lugar, maximiza el uso del ancho de banda disponible, reduciendo la necesidad de múltiples canales físicos y, por ende, los costos de instalación y mantenimiento. Además, incrementa la capacidad de transmisión de datos al permitir que diferentes señales se envíen al mismo tiempo, facilitando la integración de diversos servicios como voz, video y datos en una única infraestructura. Esta flexibilidad también permite una gestión dinámica de recursos, mejorando la calidad del servicio al priorizar ciertas señales y aumentando la seguridad al dificultar la interceptación de datos individuales. En conjunto, estas ventajas hacen del multiplexado una técnica esencial en las telecomunicaciones y en el diseño de redes modernas.

La optimización del uso del canal implica implementar estrategias como el multiplexado, la compresión de datos, la modulación eficiente y el control de errores para maximizar la eficiencia en la transmisión de información. Estas técnicas permiten que múltiples señales compartan el mismo canal, aumentan la capacidad de transmisión y mejoran la calidad del servicio al reducir la latencia y priorizar el tráfico. Como resultado, se logra una mayor capacidad de transmisión, se reducen costos operativos y se mejora la experiencia del usuario en un entorno digital en constante crecimiento.

CAPÍTULO II
FUNDAMENTOS DE REDES



CAPÍTULO II

FUNDAMENTOS DE REDES

2.1. Introducción

Actualmente en la era digital, las redes de computadoras se han convertido en la columna vertebral de la comunicación y el intercambio de información. Desde pequeñas redes locales en oficinas hasta vastas redes globales que conectan millones de dispositivos, la infraestructura de red es esencial para el funcionamiento de empresas, instituciones educativas y servicios públicos. Comprender los fundamentos de las redes es crucial para diseñar, implementar y gestionar sistemas que no solo sean eficientes, sino también seguros y escalables. Este libro se propone ofrecer una visión integral de los principios que rigen las redes y telecomunicaciones, abordando tanto los aspectos teóricos como las aplicaciones prácticas.

Los fundamentos de redes abarcan una amplia variedad de temas, desde la arquitectura y los protocolos de comunicación hasta la seguridad y la gestión del rendimiento. A medida que las tecnologías evolucionan, surgen nuevas tendencias y desafíos, como el Internet de las Cosas (IoT), la computación en la nube y la creciente demanda de conectividad. Este libro explorará cómo estas tendencias afectan el diseño y la implementación de redes, así como las mejores prácticas para su gestión efectiva. Al comprender estos conceptos, los profesionales y estudiantes estarán mejor equipados para enfrentar los retos del entorno tecnológico actual.

Además, la seguridad en las redes se ha convertido en una prioridad absoluta, dado el aumento de las amenazas cibernéticas y la necesidad de proteger datos sensibles. Este texto no solo proporcionará una base sólida en los aspectos técnicos de las redes, sino que también enfatizará la importancia de la gestión de riesgos y la implementación de políticas de seguridad robustas. A lo largo de los capítulos, se presentarán casos de estudio y ejemplos prácticos que ilustrarán cómo aplicar estos fundamentos en situaciones del mundo real, preparando a los lectores para contribuir de manera efectiva en el campo de las redes y telecomunicaciones.

A continuación, se presenta la terminología base de redes:

- ***Red de Computadoras:*** Conjunto de dispositivos interconectados que pueden comunicarse entre sí para compartir recursos e información.
- ***LAN (Red de Área Local):*** Red que conecta dispositivos en un área geográfica limitada, como una oficina o un edificio.
- ***WAN (Red de Área Amplia):*** Red que abarca un área geográfica extensa, conectando múltiples LANs a través de grandes distancias.
- ***MAN (Red de Área Metropolitana):*** Red que conecta varias LANs dentro de una ciudad o área metropolitana.
- ***Topología de Red:*** Disposición física o lógica de los dispositivos en una red, que puede ser en forma de estrella, bus, anillo o malla.
- ***Protocolo:*** Conjunto de reglas y estándares que permiten la comunicación entre dispositivos en una red.

- ***Dirección IP:*** Identificador único asignado a cada dispositivo en una red, que permite su localización y comunicación.
- ***Subnetting:*** Proceso de dividir una red IP en subredes más pequeñas para mejorar la gestión y la eficiencia del tráfico.
- ***Firewall:*** Dispositivo o software que controla el acceso a una red, permitiendo o bloqueando el tráfico según políticas de seguridad predefinidas.
- ***VPN (Red Privada Virtual):*** Tecnología que crea una conexión segura y cifrada a través de una red pública, permitiendo el acceso remoto a recursos de la red.
- ***QoS (Calidad de Servicio):*** Conjunto de tecnologías que garantizan un rendimiento adecuado de la red al priorizar ciertos tipos de tráfico.
- ***Ciberseguridad:*** Prácticas y tecnologías diseñadas para proteger sistemas, redes y datos de ataques, daños o accesos no autorizados.
- ***IoT (Internet de las Cosas):*** Concepto que se refiere a la interconexión de dispositivos físicos a Internet, permitiendo la recopilación y el intercambio de datos.
- ***SDN (Redes Definidas por Software):*** Enfoque de diseño de red que separa el plano de control del plano de datos, permitiendo una gestión más flexible y dinámica de la red.
- ***Ancho de Banda:*** Capacidad máxima de una conexión de red para transmitir datos, generalmente medida en bits por segundo (bps).
- ***NAT (Traducción de Direcciones de Red):*** Técnica que permite a múltiples dispositivos en una red local compartir una única dirección IP pública.
- ***DNS (Sistema de Nombres de Dominio):*** Servicio que traduce nombres de dominio legibles por humanos en direcciones IP que las computadoras pueden entender.

Esta terminología proporcionará un marco claro y accesible para los estudiantes, ayudándoles a familiarizarse con los conceptos clave en el campo de las redes y telecomunicaciones.

2.2. Modelos OSI

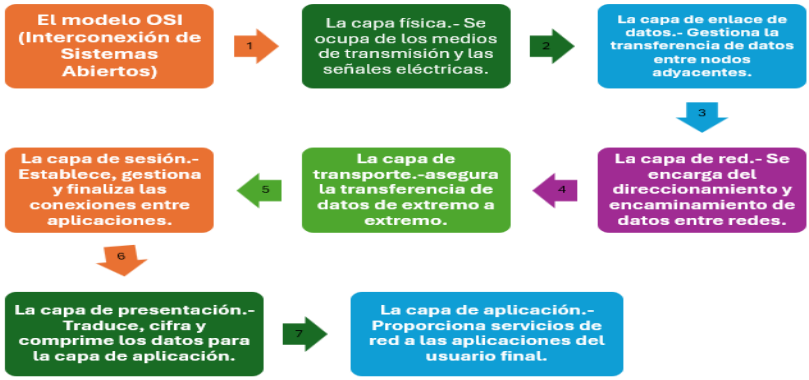
Los modelos OSI (Interconexión de Sistemas Abiertos) y TCP/IP (Protocolo de Control de Transmisión/Protocolo de Internet) son marcos de referencia que estructuran la comunicación en redes de computadoras.

Se compone de siete capas: física, enlace de datos, red, transporte, sesión, presentación y aplicación, cada una de las cuales desempeña un papel específico en el proceso de transmisión de datos.

2.2.1. Capas del modelo OSI

El modelo OSI (Interconexión de Sistemas Abiertos) es un marco conceptual que estandariza las funciones de un sistema de telecomunicaciones o de computación en siete capas distintas. Cada capa tiene un propósito específico y se encarga de una parte del proceso de comunicación.

Figura 17. Capas del Modelo OSI



La ***capa física*** es como los cimientos de una casa en el modelo OSI. Se ocupa de que los datos, en forma de bits (ceros y unos), puedan viajar realmente por el medio físico, ya sea a través de cables, fibra óptica o señales inalámbricas. Lo importante aquí es cómo se transmiten esas señales: se manejan detalles eléctricos y mecánicos para que la información llegue de un dispositivo a otro. Algunos ejemplos de tecnologías que trabajan en esta capa son Ethernet, USB y Wi-Fi.

La ***capa de enlace de datos*** es la encargada de poner orden a esos bits, agrupándolos en tramas y asegurándose de que la información llegue correctamente entre dos dispositivos que están conectados uno al otro. Además, aquí se detectan y corrigen errores básicos para evitar problemas en la comunicación. Esta capa utiliza direcciones físicas, como las famosas direcciones MAC, y emplea protocolos como Ethernet, Wi-Fi y PPP.

En la ***capa de red***, el trabajo principal es decidir por dónde deben ir los datos para llegar a su destino, aunque tengan que pasar por varias redes y dispositivos. Es como el GPS de la información: aquí se usan direcciones IP y protocolos como IP, ICMP y ARP para elegir la mejor ruta y lograr que los datos lleguen de forma eficiente.

La ***capa de transporte*** se asegura de que los datos sean divididos en partes más pequeñas y lleguen completos, en el orden correcto y sin repeticiones. Si algo falla, esta capa lo detecta y lo corrige. Hay dos formas principales de enviar los datos: una confiable, como TCP, que verifica que todo llegue bien, y otra más rápida pero menos segura, como UDP. Así, las aplicaciones reciben la información tal como fue enviada.

La ***capa de sesión*** es como el encargado de abrir y cerrar la puerta para que dos dispositivos puedan comunicarse. Administra el inicio, el mantenimiento y el cierre de las conversaciones entre aplicaciones, permitiendo que la comunicación siga activa y se cierre correctamente cuando ya no se necesita. Protocolos como NetBIOS y RPC ayudan a que estas sesiones funcionen sin interrupciones.

La ***capa de presentación*** se ocupa de que los datos sean entendibles y seguros para quien los recibe. Aquí se traduce la información, se cifra para protegerla y se comprime para que ocupe menos espacio y llegue más rápido. Por ejemplo, se usan protocolos como SSL/TLS para proteger la información y formatos como JPEG o MPEG para imágenes y videos.

Por último, la ***capa de aplicación*** es la que está más cerca de nosotros, los usuarios. Es donde funcionan los programas que usamos todos los días, como el correo electrónico, los navegadores web o los chats. Los protocolos que encontramos aquí, como HTTP, FTP, SMTP y DNS, hacen posible que podamos navegar por internet, enviar archivos o comunicarnos con otras personas.

Este modelo ayuda a los desarrolladores y profesionales de redes a entender y diseñar sistemas de comunicación complejos al dividirlos en partes manejables. Se debe tomar en cuenta que cada capa depende de la anterior y es base para la siguiente, es decir trabajan solo en conjunto y no de forma individual.

Tabla. Características de las capas del Modelo OSI

Capa	*Características*	*Funcionamiento*	*Ejemplos de Protocolos*
Física	Transmisión de bits	Señales eléctricas/ópticas	Ethernet, USB, Wi-Fi
Enlace de datos	Tramas, control de errores	Comunicación directa	Ethernet, Wi-Fi, PPP
Red	Direccionamiento, rutas	Envío entre redes	IP, ICMP, ARP
Red	Direccionamiento, rutas	Envío entre redes	IP, ICMP, ARP
Transporte	Entrega confiable/rápida	Segmentación y verificación	TCP, UDP
Sesión	Manejo de conversaciones	Inicio y cierre de sesiones	NetBIOS, RPC
Presentación	Traducción, cifrado, compresión	Adaptación de datos	SSL/TLS, JPEG, MPEG
Aplicación	Servicios al usuario	Interacción directa	HTTP, FTP, SMTP, DNS

2.2.2. Capas del modelo TCP/IP

El modelo TCP/IP, es más práctico y utilizado en Internet, se basa en el modelo OSI, algunas capas se fusionan en una sola. Se divide en cuatro capas: enlace, Internet, transporte y aplicación, integrando funciones similares a las del modelo OSI, pero de manera más simplificada. Ambos modelos permiten estandarizar las comunicaciones, facilitando la interoperabilidad entre diferentes sistemas y dispositivos, aunque el modelo TCP/IP es más prevalente en la implementación real de redes modernas.

Figura 18. Capas del Modelo TCP/IP

Capa de Aplicación

Esta capa es el punto de contacto entre los usuarios y la red. Aquí residen todos los programas y servicios que utilizamos directamente: navegadores web, clientes de correo, transferencia de archivos y aplicaciones de mensajería. La capa define cómo las aplicaciones formatean, presentan y acceden a los datos. No se preocupa por cómo viajan los datos, solo por qué información enviar y cómo interpretarla al recibirla. Los protocolos más comunes incluyen HTTP para páginas web, SMTP para correo electrónico y FTP para transferencia de archivos.

Capa de Transporte

La capa de transporte garantiza que los datos lleguen completos y en orden correcto desde el origen hasta el destino. Funciona como un servicio de paquetería que puede ofrecer dos tipos de entrega: TCP proporciona entrega confiable con confirmación de recepción (como correo certificado), mientras que UDP ofrece entrega rápida sin garantías (como correo ordinario). Esta capa también maneja la multiplexación, permitiendo que múltiples aplicaciones compartan la misma conexión de red mediante el uso de puertos.

Capa de Internet

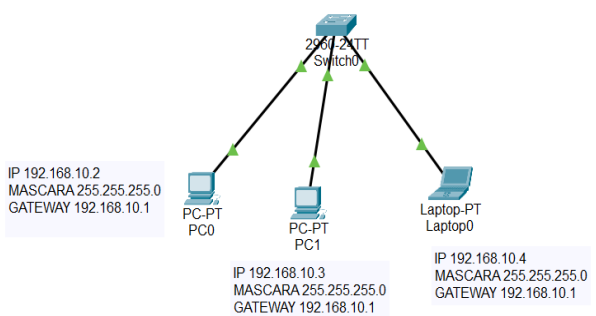
La capa de Internet es responsable del direccionamiento y enrutamiento de paquetes a través de redes interconectadas. Su protocolo principal, IP, asigna direcciones únicas a cada dispositivo y determina la mejor ruta para que los paquetes alcancen su destino, funcionando como el sistema postal global. No garantiza la entrega ni el orden de los paquetes; simplemente hace su mejor esfuerzo para moverlos de un punto a otro. También maneja la fragmentación de paquetes grandes y proporciona servicios de diagnóstico mediante ICMP.

Capa de Acceso a la Red

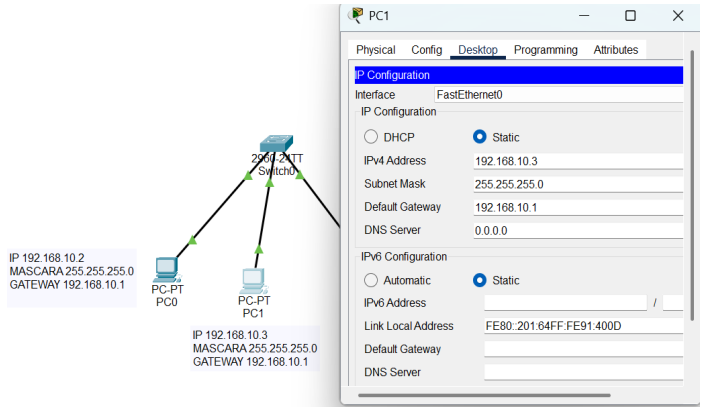
Esta capa maneja la transmisión física de datos entre dispositivos en la misma red local. Define cómo los bits se convierten en señales eléctricas, ópticas o de radio, y cómo los dispositivos acceden al medio compartido. Incluye tecnologías como Ethernet para redes cableadas y WiFi para inalámbricas. La capa se encarga del direccionamiento físico (MAC), detección de errores en la transmisión y control de acceso al medio para evitar colisiones cuando múltiples dispositivos intentan transmitir simultáneamente.

Ejemplo. Simular en CISCO Packet Tracer una red básica para revisar las capas del modelo OSI y TCP/IP

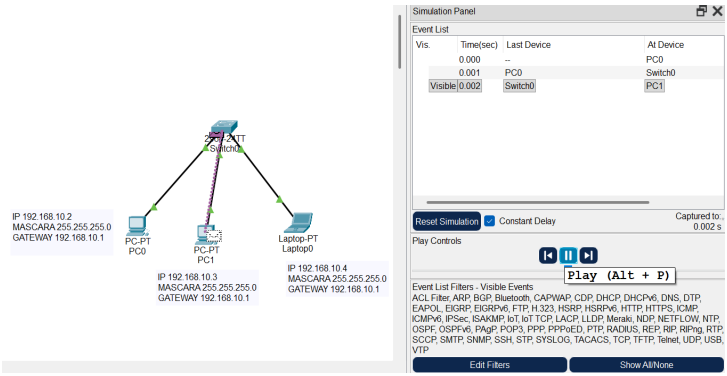
Figura 19. Topología Red Básica



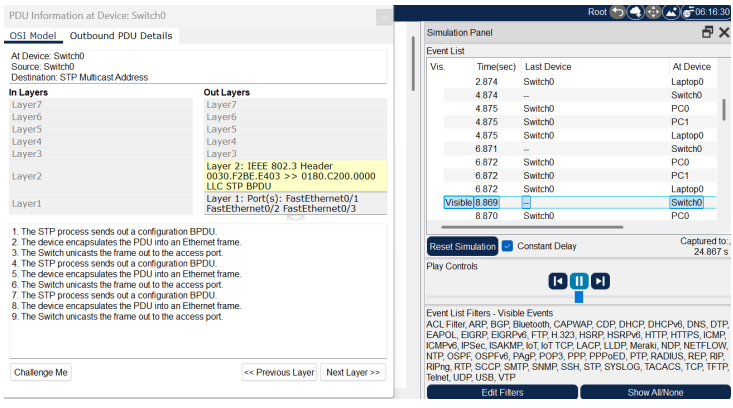
En las diferentes computadoras, dando un clic en la PC, colocar la IP, Máscara y Gateway.



Mandar un paquete para ver la conexión



Luego doble chic en el dispositivo de capa 2 para visualizar las capas que está utilizando.



2.2.3. Arquitecturas de red

Las arquitecturas de red son diseños estructurales que definen cómo se organizan y operan las redes de comunicación. Estas arquitecturas especifican la disposición de los componentes de la red, cómo se conectan entre sí y cómo se gestionan los flujos de datos.

Entre las arquitecturas de red más comunes se pueden encontrar:

Arquitectura Cliente-Servidor

En esta arquitectura, los servidores proporcionan recursos y servicios, mientras que los clientes solicitan y utilizan estos servicios. Es común en redes empresariales donde los servidores manejan aplicaciones, almacenamiento y bases de datos.

Arquitectura Peer-to-Peer (P2P)

Todos los nodos en la red actúan como iguales, compartiendo recursos directamente sin necesidad de un servidor central. Esta arquitectura es popular en aplicaciones de intercambio de archivos y redes descentralizadas.

Arquitectura de Red de Área Local (LAN)

Se utiliza para conectar dispositivos en un área geográfica limitada, como una oficina o un edificio. Las LANs suelen utilizar topologías de estrella o bus y permiten altas velocidades de transferencia de datos.

Arquitectura de Red de Área Amplia (WAN)

Conecta redes LAN a través de grandes distancias geográficas. Utiliza tecnologías como MPLS, VPNs y enlaces de fibra óptica para garantizar la conectividad entre diferentes ubicaciones.

Arquitectura de Red Definida por Software (SDN)

Separa el plano de control del plano de datos, permitiendo una gestión más flexible y dinámica de la red. Los administradores pueden programar y controlar el comportamiento de la red centralmente.

Arquitectura de Red en la Nube

Permite a las organizaciones utilizar recursos de computación y almacenamiento a través de internet. Esta arquitectura es escalable y flexible, y es esencial para servicios como IaaS, PaaS y SaaS.

Arquitectura de Red de Sensores Inalámbricos

Consiste en pequeños dispositivos distribuidos que monitorean y transmiten datos sobre condiciones ambientales. Son comunes en aplicaciones de IoT y monitoreo ambiental.

Cada arquitectura tiene sus propias ventajas y desventajas, y la elección de una u otra depende de las necesidades específicas de la organización, incluyendo factores como el costo, la escala, la seguridad y la flexibilidad.

2.2.4. Importancia de las Arquitecturas de Red

Son fundamentales para el diseño y funcionamiento eficiente de las redes de comunicación, ya que proporcionan un marco estructural que guía la disposición y conexión de los componentes de la red. Estas arquitecturas determinan cómo se gestionan los flujos de datos, garantizan la seguridad y escalabilidad, y facilitan la integración de nuevas tecnologías y servicios. Entre las que se pueden destacar tenemos:

- Eficiencia.- Facilitan la optimización del rendimiento de la red al definir cómo se deben gestionar los recursos.
- Escalabilidad.- Permiten la expansión de la red a medida que crecen las necesidades de los usuarios y dispositivos.
- Seguridad.- Proporcionan marcos para implementar medidas de seguridad que protegen la información y los dispositivos conectados.
- Interoperabilidad.- Aseguran que diferentes sistemas y tecnologías puedan comunicarse entre sí, promoviendo la integración.

2.2.5. Hardware y componentes

El hardware de red se refiere a los dispositivos físicos que permiten la interconexión y comunicación entre computadoras y otros dispositivos en una red. A continuación, se presentan los principales componentes de las redes:

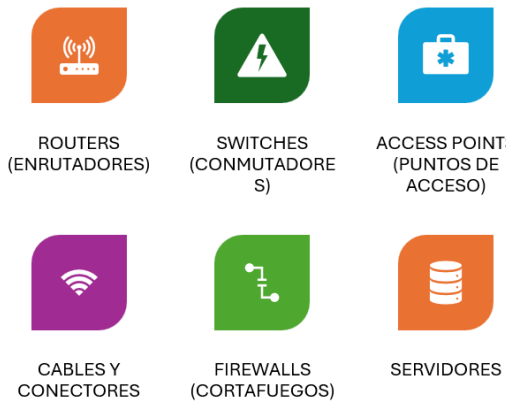


Tabla. Descripción de los componentes de una red básica

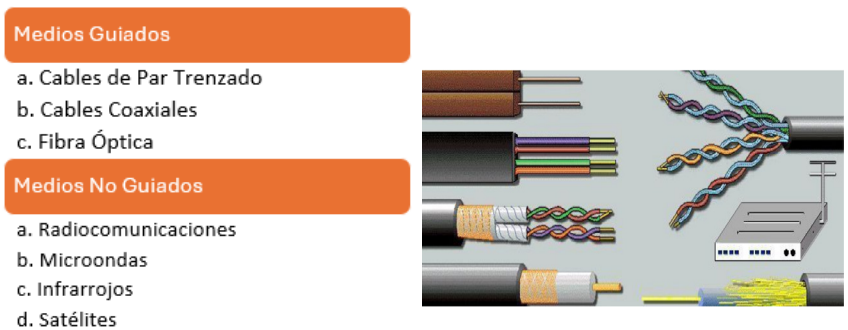
Componentes de redes	***Descripción***	***Funciones***
Routers (Enrutadores)	Los routers son dispositivos que dirigen el tráfico de datos entre diferentes redes. Su función principal es determinar la mejor ruta para enviar los datos desde el origen hasta el destino.	Conecta diferentes redes. Gestiona el tráfico de datos. Proporciona funciones de seguridad, como firewalls.
Switches (Conmutadores)	Los switches son dispositivos que conectan múltiples dispositivos dentro de una misma red local (LAN). A diferencia de los routers, que operan a nivel de red, los switches funcionan a nivel de enlace de datos.	Filtrar y reenviar datos entre dispositivos en la misma red. Mejorar la eficiencia del tráfico de red.
Access Points (Puntos de Acceso)	Los puntos de acceso permiten la conexión de dispositivos inalámbricos a una red cableada. Son esenciales para la creación de redes Wi-Fi.	Proporcionar conectividad inalámbrica. Ampliar la cobertura de la red.
Modems (Módems)	Los módems son dispositivos que modulan y demodulan señales para permitir la comunicación entre redes digitales y analógicas. Se utilizan comúnmente para conectar a Internet.	Convertir señales digitales en analógicas y viceversa. Facilitar la conexión a proveedores de servicios de Internet (ISP).
Cables y Conectores	Los cables son esenciales para la transmisión de datos en redes cableadas. Los tipos pueden ser: Cables Ethernet. - Utilizados para conexiones LAN. Cables de fibra óptica. - Ofrecen alta velocidad y capacidad a largas distancias.	Conectores: RJ45: Utilizado para cables Ethernet. SC, LC: Conectores comunes en fibra óptica.
Firewalls (Cortafuegos)	Los firewalls son dispositivos de seguridad que controlan el tráfico de red, permitiendo o bloqueando datos según reglas predefinidas.	Proteger la red de accesos no autorizados. Monitorear y registrar el tráfico de datos.
Servidores	Los servidores son computadoras que proporcionan recursos, datos y servicios a otros dispositivos en la red.	Tipos: Servidores de archivos: Almacenan y gestionan archivos. Servidores de aplicaciones: Ejecutan aplicaciones y servicios.

El hardware y los componentes de redes son esenciales para el funcionamiento eficiente y seguro de las comunicaciones en red. Comprender cada uno de estos elementos ayuda a diseñar, implementar y mantener redes efectivas.

2.3. Medios de transmisión

En el vasto mundo de las telecomunicaciones y las redes de datos, la transmisión de información es el pilar fundamental. Para que los datos viajen de un emisor a un receptor, necesitan un medio o canal a través del cual propagarse. Estos canales se conocen como medios de transmisión y se clasifican principalmente en dos grandes categorías, dependiendo de si las señales se confinan dentro una ruta física o si se propagan libremente por el espacio: medios de transmisión guiados y medios de transmisión no guiados.

Figura 20. Tipos de medios guiados y no guiados

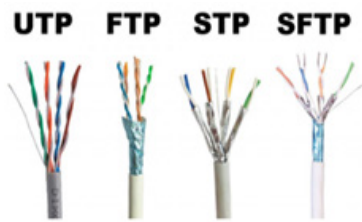


Los medios de transmisión guiados, también conocidos como medios cableados o confinados, son aquellos que utilizan un camino físico sólido para dirigir las señales electromagnéticas. La señal viaja a lo largo de este conductor, lo que proporciona una ruta definida y, a menudo, mayor seguridad y menor susceptibilidad a interferencias externas.

Por otro lado, los medios de transmisión no guiados, también llamados medios inalámbricos o no confinados, transmiten las señales electromagnéticas a través del espacio libre, sin necesidad de un conductor físico. Estas señales se propagan en todas direcciones (o en direcciones específicas si se usan antenas direccionales) y son la base de la comunicación móvil y muchas otras tecnologías inalámbricas.

El ***cable de par trenzado*** es como el clásico de las conexiones en casa y la oficina. Se divide en dos tipos principales: el UTP, que es el más común porque es barato y fácil de instalar, y el STP, que tiene una capa extra de protección para evitar interferencias, ideal si trabajas en lugares con muchos aparatos eléctricos o en ambientes industriales. Dentro del UTP hay categorías como Cat 5e, Cat 6 y Cat 7, cada una pensada para diferentes velocidades y necesidades. Además, existen otras variantes como el FTP y el SFTP, que ofrecen distintos niveles de protección según lo que necesites.

Figura 21. Tipos de cables par trenzado



El ***cable coaxial*** también tiene sus propias versiones, dependiendo de para qué lo uses. Por ejemplo, el RG-6 es el típico que ves en la televisión por cable y en el internet de banda ancha. El RG-58 era muy usado en las redes Ethernet más antiguas, y el RG-59 se encuentra sobre todo en cámaras de seguridad y sistemas de video. Cada uno tiene su propio grosor, capacidad y resistencia a las interferencias, así que se elige según el trabajo que va a realizar.

La ***fibra óptica*** es el Ferrari de la transmisión de datos. Se divide en dos grandes tipos: la fibra monomodo, que tiene un núcleo muy delgado y puede enviar información a largas distancias y a velocidades altísimas (perfecta para conectar ciudades o países), y la fibra multimodo, que tiene un núcleo más ancho y se usa en distancias más cortas, como dentro de edificios o campus. También hay diferencias en el material (puede ser de vidrio o plástico) y en cómo se agrupan los cables, lo que permite adaptarse a distintas formas de instalación.

Las ***ondas de radio*** son las que nos permiten conectarnos sin cables, y aquí hay varias opciones según la frecuencia y el uso. Por ejemplo, el Wi-Fi funciona en las bandas de 2.4 GHz y 5 GHz, mientras que el Bluetooth usa la de 2.4 GHz pero con menos alcance. Los celulares se comunican usando bandas como 3G, 4G y 5G, cada una con diferentes velocidades y cobertura. Además, existen tecnologías como ZigBee para dispositivos que no necesitan mucha energía ni alcance, y los enlaces de microondas que conectan puntos distantes directamente.

La ***transmisión por infrarrojos*** también tiene sus clases, según la potencia y el alcance. Los controles remotos son el ejemplo más común: funcionan a pocos metros y necesitan estar "apuntando" al dispositivo. Otros sistemas, como los que permitían transferir archivos entre celulares antiguos, son más rápidos, pero siguen necesitando esa alineación directa. Hoy en día, los infrarrojos se usan en casos muy específicos porque otras tecnologías inalámbricas han superado sus limitaciones.

Cada tipo de medio de transmisión y sus variantes se elige según lo que realmente necesitas: qué tan rápido quieres que viaje la información, qué distancia debe cubrir, cuánta protección necesitas contra interferencias y el lugar donde vas a instalar la red. Así, puedes tener una comunicación eficiente y adaptada a cada situación.

Comprender las características, ventajas y desventajas de cada tipo de medio es crucial para diseñar redes eficientes, fiables y adecuadas a las necesidades específicas de comunicación, ya sea para conectar dispositivos en una pequeña oficina o para establecer enlaces de comunicación a escala global.

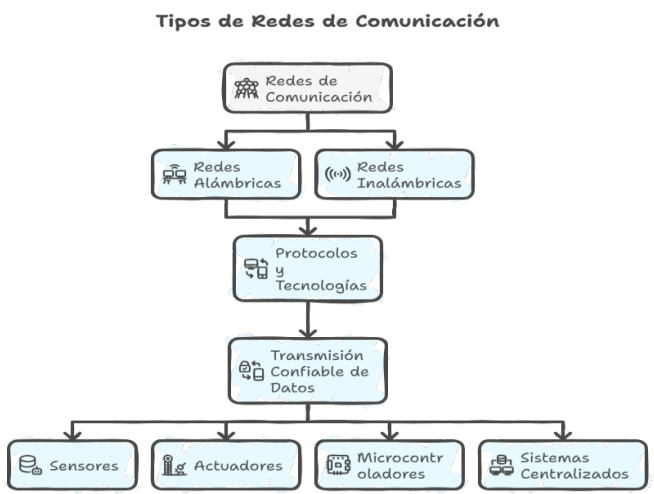
Comparación de tipos de cable

Característica	Cable de par trenzado	Cable coaxial	Fibra óptica	Ondas de radio	Transmisión por infrarrojos
Descripción	Conexión clásica para hogar y oficina	Versiones según el uso	Ferrari de la transmisión de datos	Conexión sin cables	Potencia y alcance según la clase
Tipos	UTP, STP, FTP, SFTP	RG-6, RG-58, RG-59	Monomodo, multimodo	Wi-Fi, Bluetooth, 3G, 4G, 5G, ZigBee, microondas	Controles remotos, transferencia de archivos
Aplicaciones	Redes domésticas y de oficina	Televisión por cable, internet, redes antiguas, cámaras de seguridad	Conectar ciudades, campus, edificios	Wi-Fi, Bluetooth, celulares, dispositivos de bajo consumo	Controles remotos, transferencia de archivos entre celulares antiguos
Ventajas	Barato, fácil de instalar	Versátil	Alta velocidad, larga distancia	Sin cables	Simple
Desventajas	Susceptible a interferencias	Grosor, capacidad, resistencia a interferencias	Costoso, instalación compleja	Alcance limitado, interferencias	Corto alcance, requiere alineación

2.4. Tipos de redes

En la actualidad, la comunicación eficiente entre dispositivos electrónicos es fundamental para el desarrollo de sistemas modernos en áreas como la automatización, la informática, la industria y el Internet de las cosas (IoT). Las redes de comunicación en electrónica permiten el intercambio de información, la coordinación de procesos y la integración de tecnologías diversas, facilitando soluciones innovadoras y mejorando la funcionalidad de los dispositivos.

Existen diferentes tipos de redes de comunicación, cada una diseñada para satisfacer necesidades específicas en cuanto a velocidad, alcance, consumo energético y robustez. Estas redes pueden ser alámbricas o inalámbricas, y emplean diversos protocolos y tecnologías para garantizar la transmisión confiable de datos entre sensores, actuadores, microcontroladores y sistemas centralizados.

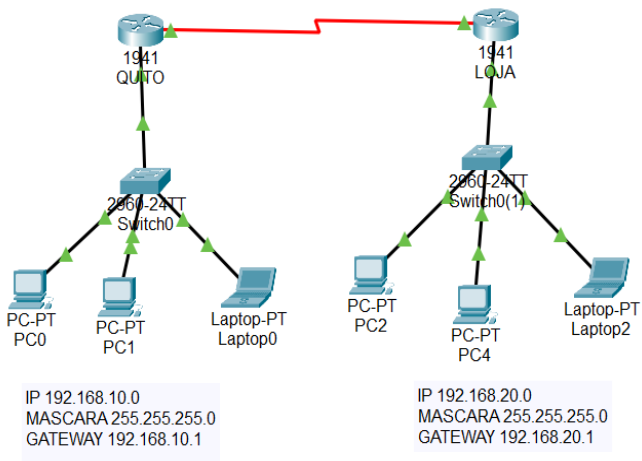


2.4.1. Redes de Comunicación Alámbricas

Redes Seriales

Las redes seriales se refieren a la transferencia de datos bit a bit a través de un único canal o cable, siendo una tecnología de comunicación alámbrica fundamental para conectar dispositivos y redes. Aunque más lentas que las redes paralelas en términos de volumen de bits simultáneos, las redes seriales ofrecen mayor alcance, menor complejidad de cableado y alta fiabilidad, lo que las hace adecuadas para una amplia gama de aplicaciones, desde la conexión de periféricos como ratones e impresoras hasta enlaces de alta velocidad en centros de datos.

Figura 22. Red Serial



RS-232, RS-485, UART: Utilizadas para la transmisión punto a punto o multipunto entre dispositivos electrónicos como microcontroladores, computadoras y módulos de comunicación industrial.

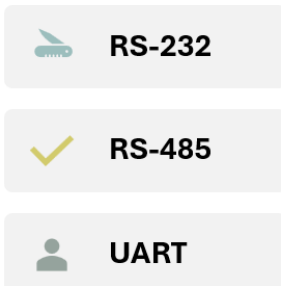
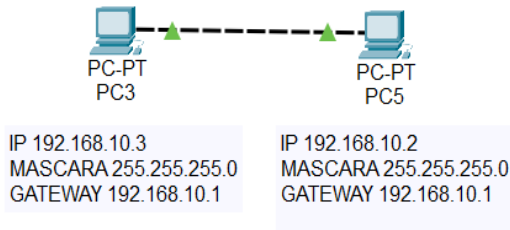


Figura 23. RS-232



Son estándares de comunicación serial que difieren en su modo de transmisión, distancia y capacidad de conexión: RS-232 es punto a punto para distancias cortas, RS-485 es multipunto para distancias largas y usa señalización diferencial, y UART es un controlador de hardware que implementa la lógica de la comunicación serial.

Tabla. Estándares de comunicación utilizados con estos estándares de comunicación

RS-232	***Tipo de conexión:*** Punto a punto, para conectar dos dispositivos. ***Modo de transmisión:*** *Un solo extremo, donde la señal se compara con tierra.* ***Distancia:*** Corta distancia, limitada a unos 15 metros. ***Velocidad:*** Relativamente baja. ***Aplicaciones:*** Comunicación de corto alcance, a menudo con dispositivos informáticos más antiguos.
RS-485	***Tipo de conexión:*** Multipunto, permitiendo una red de hasta 32 dispositivos. ***Modo de transmisión:*** Diferencial, usando dos señales eléctricas complementarias para mayor inmunidad al ruido. ***Distancia:*** Larga distancia, superando los 1000 metros. ***Velocidad:*** Puede alcanzar altas velocidades, aunque la distancia afecta la velocidad. ***Aplicaciones:*** Muy común en la industria, para redes de control de larga distancia.
UART (Universal Asynchronous Receiver / Transmitter)	***Rol:*** Es un circuito integrado (hardware) que implementa la lógica de la comunicación serial. ***Función:*** Se encarga de convertir los datos paralelos del microprocesador en datos seriales para transmitirlos un bit a la vez y viceversa, para la recepción. ***Uso:*** A menudo se encuentra dentro de los microcontroladores para la comunicación interna o de corta distancia.

UART es el "reloj" que genera la señal serial, mientras que RS-232 y RS-485 son los estándares que definen cómo se transmiten esas señales a nivel eléctrico en el cable.

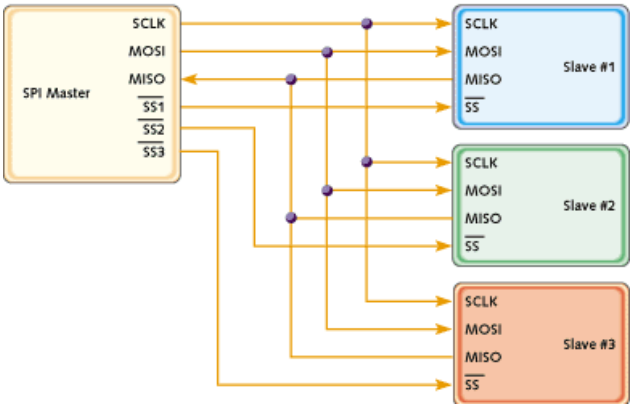
Tabla. Características, ventajas, aplicaciones y ejemplos de RS-232, RS-485, UART

Características principales	***Bus de dos hilos:*** ***SDA (Serial Data):*** Línea de datos. SCL (Serial Clock): Línea de reloj. Comunicación maestro-esclavo: Un dispositivo maestro controla la comunicación y puede dirigir mensajes a uno o varios dispositivos esclavos. Direcciones únicas: Cada dispositivo esclavo tiene una dirección única en el bus, lo que permite identificarlo y comunicarse con él de manera específica. ***Velocidades estándar:*** ***Estándar:*** 100 kHz ***Rápido:*** 400 kHz ***Alta velocidad:*** 3.4 MHz
Ventajas	Solo requiere dos cables para conectar varios dispositivos. Permite agregar múltiples dispositivos sin complicaciones de cableado. Ideal para aplicaciones donde el espacio y el costo son limitados.
Aplicaciones comunes	Comunicación entre microcontroladores y sensores. Control de pantallas LCD y memorias EEPROM. Interconexión de periféricos en sistemas embebidos.
Ejemplo de conexión I2C	Un microcontrolador puede estar conectado a varios sensores y una pantalla, todos compartiendo las líneas SDA y SCL. El microcontrolador actúa como maestro y selecciona el dispositivo con el que desea comunicarse mediante la dirección I2C.

SPI (Interfaz periférica en serie): Es un protocolo de comunicación serial síncrono y dúplex completo para la transferencia de datos a corta distancia entre un controlador (maestro) y uno o más dispositivos periféricos (subnodos) en sistemas integrados Utiliza un reloj serial (SCLK) y líneas de datos independientes (MOSI para controlador a periférico y MISO para periférico a controlador), junto con una línea de selección de chip (CS) para seleccionar un periférico específico. SPI es conocido por su alta velocidad y sencilla implementación, lo que lo hace ideal para aplicaciones como la conexión de microcontroladores a sensores, convertidores analógico-digitales (ADC), convertidores digital-analógicos (DAC) y registros de desplazamiento.

Si existen varios dispositivos esclavos, el maestro genera una señal de selección de esclavo independiente para cada uno. Estas relaciones se ilustran en la siguiente figura.

Figura 24. Implementación de SPI de un solo maestro y múltiples esclavos



En su popular configuración de 4 cables, SPI utiliza estas señales principales:

SCLK (Reloj Serial):	El controlador genera esta señal de reloj para sincronizar la transferencia de datos.
MOSI (Master Out Slave In)	Los datos viajan desde el controlador al dispositivo periférico.
MISO (Master In Slave Out)	Los datos viajan desde el dispositivo periférico al controlador.
CS (selección de chip o selección de esclavo)	El controlador activa esta línea para seleccionar un dispositivo periférico específico para la comunicación.

Aunque SPI no describe una forma específica de implementar sistemas multimaestro, algunos dispositivos SPI admiten señales adicionales que posibilitan dichas implementaciones. Sin embargo, es complicado y suele ser innecesario, por lo que no se suele implementar.

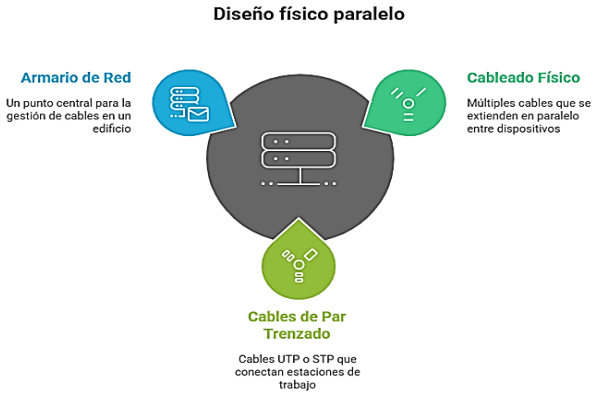
2.4.2. Redes Paralelas

El término Redes Paralelas no es un concepto estándar, pero se puede interpretar de dos maneras: conexiones físicas que corren en paralelo, como los cables de un mismo cableado estructurado que van del centro de cómputo a diferentes áreas, o la transmisión de datos en paralelo a través de medios físicos, aunque la comunicación en redes alámbricas generalmente se realiza por medios secuenciales.

Diseño físico paralelo:

- ***Cableado físico:*** Se refiere a múltiples cables que se extienden de forma paralela entre dispositivos o puntos de una red alámbrica.
- ***Ejemplos:*** En un edificio, un armario de red puede tener múltiples cables de par trenzado (UTP o STP) que se extienden en paralelo para conectar las estaciones de trabajo de los pisos superiores.
- ***Ventaja:*** Permite una infraestructura de red organizada y eficiente para la transferencia de datos.

Figura 25. Diseño de redes paralelas



Transmisión paralela de datos:

- ***Concepto de transmisión:*** Las redes alámbricas, principalmente las basadas en Ethernet operan enviando datos de forma secuencial en las líneas de comunicación.
- ***Manejo paralelo:*** Sin embargo, el concepto de comunicación paralela puede aplicarse a nivel de cómo los protocolos gestionan y dirigen el tráfico de datos en la red, o a la tecnología subyacente de los medios físicos.
- ***Tecnologías que usan "paralelismo":*** Algunas tecnologías, como la fibra óptica o ciertos tipos de cables coaxiales, pueden procesar múltiples señales o flujos de datos simultáneamente a través de diferentes canales.

Si bien las redes alámbricas utilizan cables para la transmisión, la comunicación de los datos en sí mismo es mayormente secuencial, mientras que los "paralelos" se refieren más a la organización física del cableado para soportar múltiples conexiones en paralelo o a la forma en que algunos protocolos manejan el tráfico

2.4.3. Redes Ethernet

Las redes de comunicación alámbricas Ethernet son el estándar para conectar dispositivos en una red de área local (LAN) mediante cables, como los de par trenzado (RJ45), ofreciendo alta velocidad, fiabilidad, mayor seguridad y menor latencia que las redes inalámbricas (Wi-Fi). Se utilizan en hogares, oficinas, y grandes redes empresariales para la transmisión de datos entre computadoras, impresoras y otros dispositivos, siendo vitales para la infraestructura de comunicaciones cableadas a nivel mundial.

Figura 26. Redes Ethernet

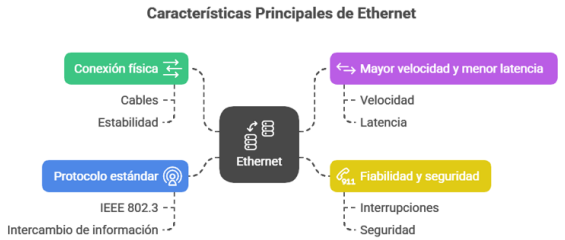
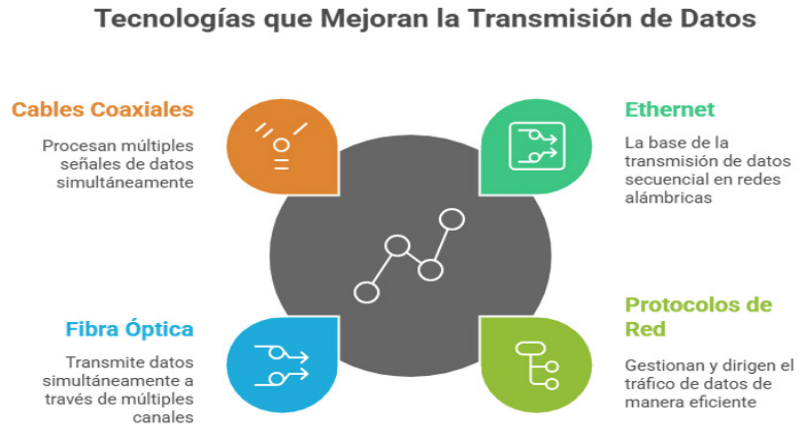


Tabla. Características principales de Red Ethernet

Conexión física	La transmisión de datos se realiza a través de cables, lo que proporciona una conexión directa y estable.
Mayor velocidad y menor latencia	Ethernet ofrece velocidades de transferencia de datos más altas y una latencia reducida en comparación con las redes inalámbricas.
Fiabilidad y seguridad	Al ser una conexión física, las redes Ethernet son menos vulnerables a interrupciones y ofrecen un mayor grado de seguridad al no transmitir la señal por el aire.
Protocolo estándar	Se basa en el estándar IEEE 802.3, que define el protocolo de comunicación para que los dispositivos puedan intercambiar información

Figura 27. Tecnologías que mejoran la transmisión de datos



Usos comunes:

Redes locales (LAN)	Conexión de computadoras, impresoras y otros dispositivos en oficinas y hogares
Redes de área amplia (WAN)	Utilizadas en empresas para conectar redes en distintas ubicaciones.
Redes de área metropolitana (MAN)	Redes a mayor escala que cubren áreas urbanas.

2.5. Clasificación de las redes según el número de dispositivos

La clasificación de las redes de acuerdo con el número de dispositivos conectados es una forma práctica de entender su alcance, tamaño y propósito. Esta clasificación permite identificar el tipo de red que mejor se adapta a las necesidades de comunicación y transmisión de datos en diferentes entornos, desde redes personales hasta grandes redes empresariales o globales.

Figura 28. Tipos de Redes según el número de dispositivos

Redes de Área Personal (PAN - Personal Area Network)

Las PAN son redes diseñadas para conectar un número reducido de dispositivos en un entorno personal, generalmente en un rango de pocos metros. Este tipo de red se utiliza para la comunicación entre dispositivos personales, como teléfonos móviles, tablets, computadoras portátiles, entre otros. Se recomienda que el número de dispositivos sea de 2 a 10 dispositivos.

Características:

- Rango limitado (generalmente hasta 10 metros).
- Uso de tecnologías inalámbricas como Bluetooth, Zigbee o infrarrojo.
- Baja velocidad de transmisión, suficiente para sincronización y transferencia de datos pequeños.

Un ejemplo de esta red es la conexión entre un teléfono móvil y unos audífonos Bluetooth.

Redes de Área Local (LAN - Local Area Network)

Las LAN son redes que conectan dispositivos dentro de un área geográfica pequeña, como una oficina, hogar o edificio. Son las más comunes en entornos domésticos y empresariales.

La cantidad de dispositivos que abarca va de 10 a varios cientos de dispositivos, dependiendo del tamaño de la red.

Características:

- Alta velocidad de transmisión (generalmente entre 100 Mbps y varios Gbps).
- Uso de tecnologías como Ethernet y Wi-Fi.
- Fácil de instalar y mantener.

Como ejemplo puede ser una red en una oficina que conecta computadoras, impresoras y servidores.

Redes de Área Metropolitana (MAN - Metropolitan Area Network)

Las MAN son redes diseñadas para conectar múltiples LAN dentro de una ciudad o área metropolitana. Estas redes son utilizadas por empresas grandes, universidades o gobiernos para interconectar diferentes ubicaciones geográficas cercanas.

Número de dispositivos va desde cientos hasta miles de dispositivos.

Características

- Cobertura de hasta 50 kilómetros.
- Uso de tecnologías como fibra óptica, WiMAX o enlaces dedicados.
- Mayor capacidad de transmisión en comparación con las LAN.

La red que conecta las sucursales de un banco dentro de una ciudad.

Redes de Área Amplia (WAN - Wide Area Network)

Las WAN son redes que abarcan grandes áreas geográficas, como países o incluso continentes. Estas redes interconectan múltiples LAN y MAN utilizando infraestructura de telecomunicaciones, como satélites, cables submarinos y enlaces dedicados.

Número de dispositivos, desde miles hasta millones de dispositivos.

Características:

- Cobertura global.
- Uso de tecnologías como MPLS, VPN y enlaces satelitales.
- Baja velocidad de transmisión en comparación con las LAN y MAN, debido a la distancia.

Internet es el ejemplo más grande y conocido de una WAN.

Redes de Área de Almacenamiento (SAN - Storage Area Network)

Las SAN son redes especializadas diseñadas para conectar dispositivos de almacenamiento, como servidores y discos duros externos, con el objetivo de gestionar grandes volúmenes de datos.

La cantidad de dispositivos generalmente de decenas a cientos de dispositivos.

Características:

- Alta velocidad y baja latencia para la transferencia de datos.
- Uso de tecnologías como Fibre Channel y iSCSI.
- Diseñadas para entornos empresariales y centros de datos.

Como ejemplo puede ser una red que conecta servidores y sistemas de almacenamiento en un centro de datos.

Redes de Área Global (GAN - Global Area Network)

Las GAN son redes que conectan dispositivos y redes en múltiples países o continentes. Estas redes son utilizadas por empresas globales para garantizar la comunicación entre sus oficinas en diferentes partes del mundo.

Tiene miles hasta millones de dispositivos.

Características:

- Cobertura internacional.
- Uso de infraestructura global, como cables submarinos y satélites.
- Alta capacidad de transmisión, aunque con mayor latencia.

Ejemplo práctico:

Una empresa multinacional que conecta sus oficinas en diferentes continentes.

Tabla. Tipos de redes según el número de dispositivos

Tipo de Red	*Número de Dispositivos*	*Cobertura Geográfica*	*Ejemplo*
PAN	2 a 10	Pocos metros	Conexión entre un teléfono y audífonos
LAN	10 a cientos	Edificio u oficina	Red doméstica o empresarial
MAN	Cientos a miles	Ciudad o área metropolitana	Red de sucursales bancarias
WAN	Miles a millones	Países o continentes	Internet
SAN	Decenas a cientos	Centros de datos	Red de almacenamiento empresarial
GAN	Miles a millones	Global	Empresa multinacional

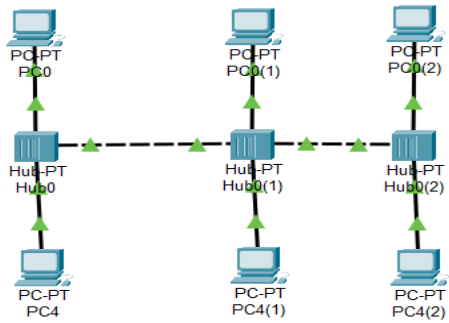
2.6. Tipos de topologías de redes

Las principales topologías de redes son la de bus, anillo, estrella, árbol, malla e híbrida. La elección de una topología depende de factores como el tamaño de la red, la escala, los objetivos y el presupuesto de la empresa, según Hispasat. Cada topología tiene diferentes configuraciones de nodos y enlaces, y una topología de malla ofrece la mayor tolerancia a fallos, mientras que la de bus es más económica.

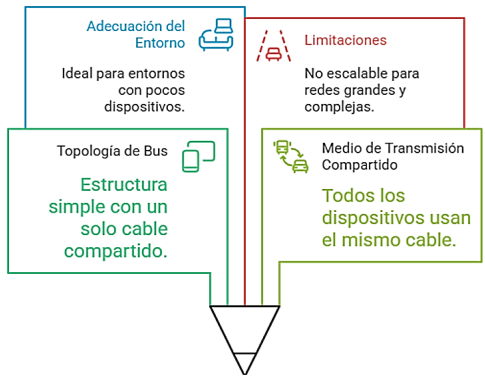
2.6.1. Topología de bus

Todos los dispositivos están conectados a un único cable, y las señales viajan a lo largo de todo el bus.

Figura 29. Topología bus en simulador Cisco Packet Tracer



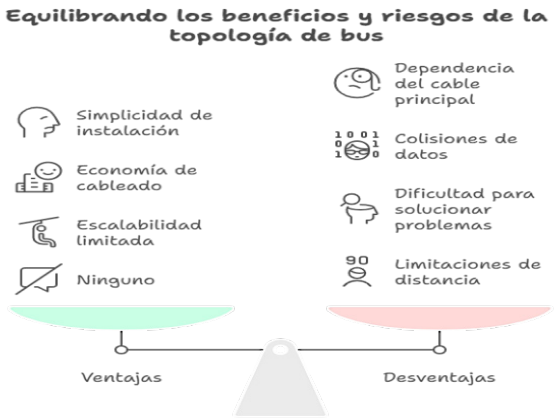
La topología de bus es una de las configuraciones más simples y utilizadas en redes de computadoras, especialmente en los primeros sistemas de redes. En esta estructura, todos los dispositivos de la red están conectados a un único cable principal denominado bus o troncales, que actúa como un medio de transmisión compartido. Esta topología tiene características específicas que la hacen adecuada para ciertos entornos, pero también presenta limitaciones importantes.



Características principales

- ***Estructura lineal.*** Todos los nodos (computadoras, impresoras, etc.) están conectados al mismo cable principal. El cable funciona como un canal de comunicación único para todos los dispositivos.
- ***Comunicación compartida.*** Los datos viajan en ambas direcciones a lo largo del bus.
- Solo un dispositivo puede transmitir datos en un momento dado; los demás deben esperar su turno.
- ***Terminadores.*** En los extremos del cable se colocan terminadores para evitar que las señales se reflejen y causen interferencias.

Figura 30. Ventajas y desventajas de la topología bus

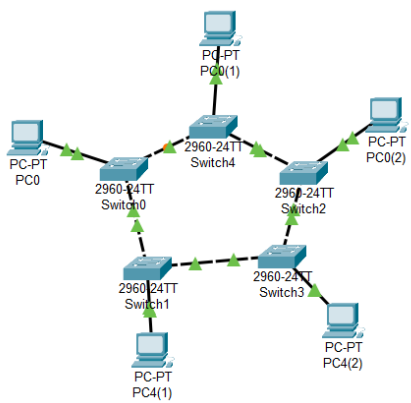


La topología de bus fue ampliamente utilizada en redes pequeñas y locales (LAN) durante los primeros años de desarrollo de las tecnologías de redes. Sin embargo, con el avance de las tecnologías modernas y la aparición de topologías más eficientes como la estrella y el anillo, su uso ha disminuido. Actualmente, se encuentra principalmente en aplicaciones específicas o en entornos donde la simplicidad y el bajo costo son factores clave.

2.6.2. Topología de anillo

Los dispositivos se conectan en un patrón circular, formando un anillo. Los datos viajan a través de cada dispositivo, y puede haber dos anillos para mayor redundancia. La topología de anillo es una configuración en la que los dispositivos de la red están conectados en un circuito cerrado, formando un anillo continuo. En esta estructura, cada dispositivo está conectado directamente al siguiente, y el último se conecta al primero, creando un flujo circular para la transmisión de datos. Es una topología que, aunque menos común en redes modernas, ha sido utilizada ampliamente en sistemas donde la transmisión ordenada y controlada es esencial.

Figura 31. Topología en anillo



Características	*Descripción*
Estructura circular	Los dispositivos están conectados en forma de anillo, lo que significa que cada nodo tiene exactamente dos conexiones: una hacia el nodo anterior y otra hacia el siguiente. No hay un nodo central; todos los dispositivos tienen la misma importancia en la red.
Dirección de transmisión	Los datos viajan en una única dirección (unidireccional) o en ambas direcciones (bidireccional), dependiendo del diseño de la red. Cada nodo actúa como un repetidor, amplificando y retransmitiendo la señal para que pueda llegar al siguiente dispositivo.
Método de acceso	Utiliza un esquema de control de acceso como el Token Passing, en el cual un "token" (señal de control) circula por el anillo para permitir que un dispositivo transmita datos. Esto reduce las colisiones, ya que solo el dispositivo que posee el token puede enviar información.

Ventajas y desventajas de la topología en anillo

VENTAJAS	*DESVENTAJAS*
• Orden en la transmisión: El uso del token asegura que no haya colisiones de datos, lo que mejora la eficiencia en redes con tráfico moderado. • Facilidad de diagnóstico: Es más fácil identificar fallas, ya que los problemas suelen estar relacionados con un nodo específico o una conexión. • Distancia: Los datos pueden viajar a mayores distancias gracias al uso de repetidores en cada nodo.	• Dependencia de los nodos: Si un nodo o conexión falla, toda la red puede quedar inoperativa, a menos que se implemente redundancia. • Tiempo de transmisión: En redes grandes, el tiempo que tarda el token en recorrer el anillo puede aumentar la latencia. • Escalabilidad limitada: Agregar nuevos dispositivos requiere interrumpir el funcionamiento de la red y puede ser complicado.

La topología de anillo fue ampliamente utilizada en redes locales (LAN), especialmente en sistemas como Token Ring desarrollados por IBM. Aunque su uso ha disminuido con el surgimiento de topologías más flexibles como la estrella, sigue siendo relevante en ciertas aplicaciones industriales y en sistemas de redes de fibra óptica, como SONET/SDH, donde la redundancia del anillo es clave para garantizar la confiabilidad.

2.6.3. Topología de estrella

Los dispositivos se conectan a un dispositivo central, como un hub o switch. En la actualidad es una de las más utilizadas por la forma sencilla de conectar todos sus dispositivos, ya que solo necesitan un cable par trenzado directo, computadoras y el dispositivo central, en cuanto a HW y las IP y máscara en SW.

La topología de estrella es ampliamente utilizada en redes locales (LAN) modernas, especialmente en entornos corporativos, educativos y domésticos. Es ideal para redes Ethernet, donde los switches y routers actúan como nodos centrales para gestionar la comunicación entre dispositivos como computadoras, impresoras, cámaras IP y otros periféricos.

Figura 32. Componentes de la red Topología en Estrella

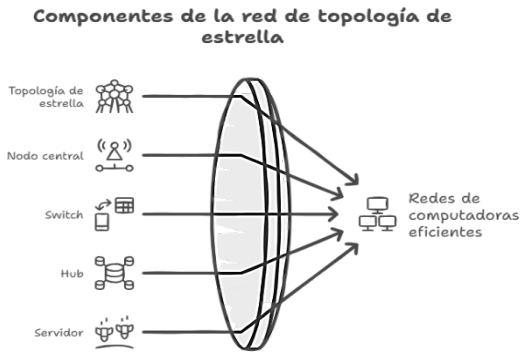


Tabla. Características principales de la topología en estrella

Características	*Descripción*
Estructura centralizada	Todos los dispositivos están conectados directamente al nodo central mediante cables individuales. El nodo central es responsable de gestionar la comunicación entre los dispositivos conectados.
Comunicación	Los datos enviados por un dispositivo pasan primero por el nodo central, que los dirige hacia el destinatario correspondiente. La comunicación puede ser unidireccional o bidireccional, dependiendo del tipo de nodo central utilizado (hub o switch).
Dependencia del nodo central	El nodo central es crítico para el funcionamiento de la red; si falla, toda la red queda inoperativa.

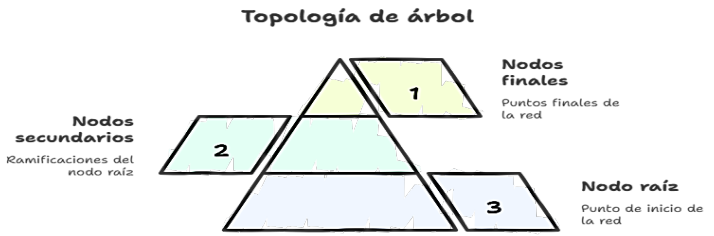
Tabla. Ventajas y desventajas principales de la topología en estrella

VENTAJAS	*DESVENTAJAS*
Facilidad de instalación y configuración: Es intuitiva y sencilla de implementar, ya que cada dispositivo tiene una conexión directa al nodo central. ***Mantenimiento y diagnóstico:*** Es fácil identificar fallos, ya que los problemas suelen estar relacionados con un cable o dispositivo específico. ***Escalabilidad:*** Permite agregar nuevos dispositivos sin afectar el funcionamiento de la red existente. ***Control eficiente:*** El nodo central puede gestionar el tráfico de datos, reduciendo colisiones y mejorando el rendimiento.	***Dependencia del nodo central:*** El funcionamiento de toda la red depende del nodo central; si éste falla, la red completa se ve afectada. ***Costo:*** Requiere más cableado que otras topologías, ya que cada dispositivo necesita una conexión directa al nodo central. ***Limitaciones físicas:*** La longitud de los cables está limitada por las especificaciones del medio de transmisión, lo que puede restringir el tamaño de la red.

2.6.4. Topología de árbol:

La topología de árbol es una estructura jerárquica de red que combina topologías de bus y estrella, con un nodo raíz central que se ramifica en múltiples subnodos de manera similar a un árbol. Se caracteriza por su facilidad para la expansión y la gestión organizada de redes grandes, como las de campus universitarios o corporativos, pero requiere un enlace troncal robusto y es vulnerable a fallos en el nodo central.

Figura 33. Partes de la topología en árbol



La topología de árbol es una estructura jerárquica que combina características de la topología de estrella y la topología de bus, siendo ideal para redes grandes y organizadas. En esta configuración, los nodos están conectados formando una estructura similar a un árbol, con un nodo principal (raíz) que

actúa como el punto de inicio de la red y varios niveles de nodos secundarios que se ramifican desde él. Es ampliamente utilizada en redes empresariales, educativas y sistemas distribuidos.

Figura 34. Conexión de una topología en árbol

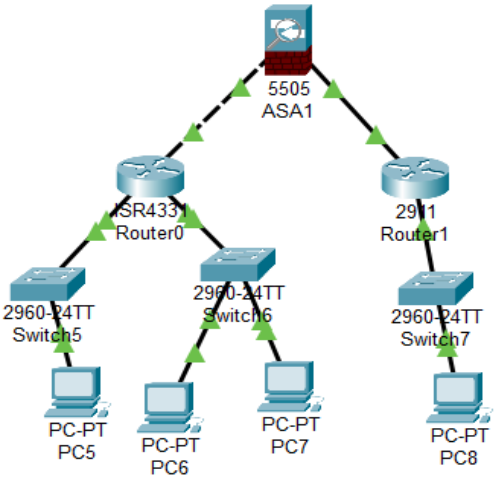


Tabla. Características principales de la topología en árbol

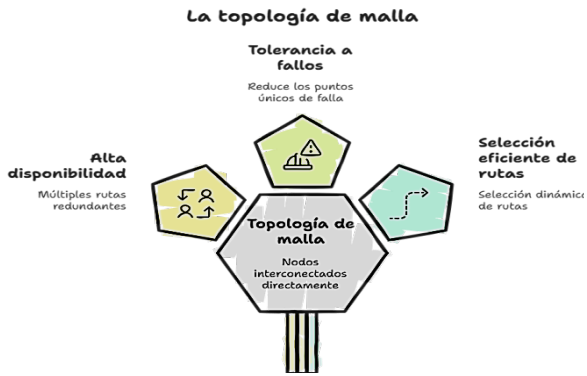
Características	*Descripción*
Estructura jerárquica	La red se organiza en niveles, comenzando con un nodo raíz central que se conecta a otros nodos secundarios. Los nodos secundarios pueden actuar como puntos de conexión para otros nodos, formando una estructura de ramas.
Combinación de topologías	Cada rama de la red puede adoptar una configuración de estrella o bus, dependiendo de las necesidades del diseño. La topología general mantiene la forma de un árbol, con múltiples niveles interconectados.
Segmentación	La red puede dividirse en subredes más pequeñas, lo que facilita la gestión y el mantenimiento. Cada subred puede operar de manera independiente, pero sigue conectada a la red principal.

VENTAJAS	DESVENTAJAS
Escalabilidad: • Es fácil expandir la red añadiendo nuevos nodos en los niveles inferiores sin afectar significativamente el funcionamiento de la red. • Ideal para redes grandes que requieren una organización estructurada. ***Facilidad de gestión:*** • La estructura jerárquica facilita la administración y el control de la red, ya que cada nivel puede ser gestionado de forma independiente. ***Segmentación eficiente:*** • Las fallas en una rama de la red no afectan directamente a las demás ramas, lo que mejora la confiabilidad. ***Soporte para redes grandes:*** • Permite conectar un gran número de dispositivos manteniendo una organización clara y ordenada.	***Dependencia de los nodos principales:*** • Si el nodo raíz o un nodo intermedio falla, las ramas conectadas a él también quedan inoperativas. ***Complejidad en el cableado:*** • Requiere una cantidad significativa de cableado para conectar los diferentes niveles de nodos, lo que puede aumentar los costos. ***Dificultad para solucionar problemas:*** • Identificar fallas puede ser complicado en redes grandes debido a la estructura jerárquica.

2.6.5. Topología de malla

La topología de malla es un modelo de interconexión en el que algunos o todos los nodos de la red están conectados directamente entre sí mediante múltiples enlaces redundantes. Su objetivo principal es maximizar la disponibilidad, la tolerancia a fallos y la eficiencia en la selección dinámica de rutas. A diferencia de estructuras jerárquicas (árbol) o segmentadas (estrella, bus), la malla distribuye la inteligencia y reduce los puntos únicos de falla, favoreciendo la continuidad operativa en entornos críticos.

Figura 35. Topología en malla



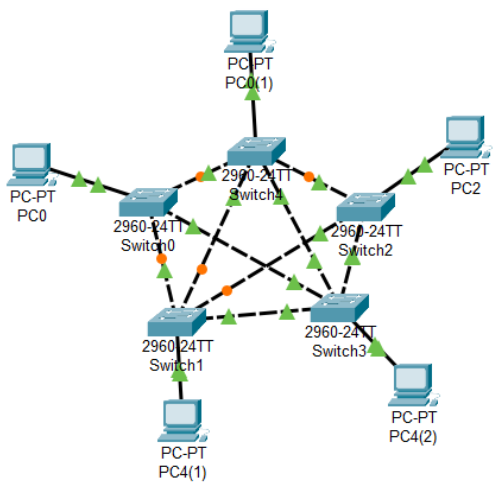
Tipos de topología en malla

- Malla completa (Full Mesh)
- Malla parcial (Partial Mesh)
- Malla lógica sobre infraestructura física no mallada
- Malla inalámbrica (Wireless Mesh Network, WMN)

Malla completa (Full Mesh): Cada nodo dispone de un enlace físico o lógico directo con todos los demás.

- Número de enlaces: n(n-1)/2 (enlace no dirigido) o n(n-1) si son canales dirigidos.
- Ventaja: Máxima redundancia y mínima latencia promedio.
- Desventaja: Crecimiento cuadrático de coste y complejidad.

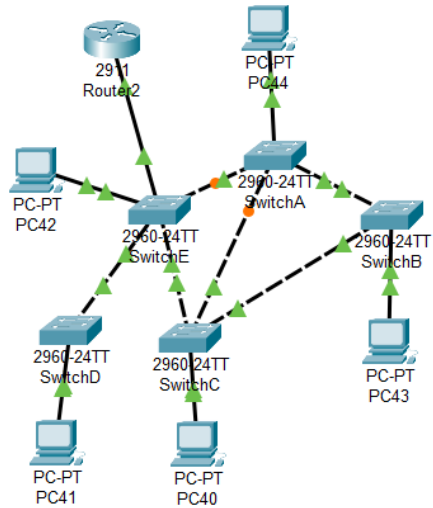
Figura 36. Topología de red tipo malla realizado en simulador CISCO Packet Tracer



Malla parcial (Partial Mesh): Solo los nodos clave (core, agregación, críticos) tienen múltiples enlaces; otros mantienen conexiones limitadas.

- Ventaja: Balance entre resiliencia y coste.
- Uso típico: WAN corporativas, redes ISP, entornos híbridos SD-WAN.

Figura 37. Topología de red tipo malla parcial realizado en simulador CISCO Packet Tracer



Malla lógica sobre infraestructura física no mallada: Se construye mediante túneles (MPLS, VXLAN, GRE, IPSec) o superposición (overlay) sobre una capa subyacente más simple.

Malla inalámbrica (Wireless Mesh Network, WMN): Nodos radio que actúan simultáneamente como clientes y routers, utilizando protocolos de encaminamiento adaptativo (ej. HWMP, OLSR, BATMAN, 802.11s).

Componentes y roles

- Nodos terminales: ***Equipos finales, sensores, servidores.***
- Nodos de reenvío (forwarders): ***Conmutadores, routers, access points mesh.***
- Nodos de puerta de enlace (gateways): ***Interfaz hacia Internet, WAN o nube.***
- Controladores/Orquestadores (en arquitecturas SDN): ***Gestionan políticas, caminos y segmentación.***
- Planos funcionales: Datos (data plane), control (routing, señalización), gestión (telemetría, configuración), seguridad (ACL, cifrado, AAA).

Características claves

- Redundancia intrínseca: ***Múltiples rutas alternativas.***
- Rutas dinámicas: ***Protocolos adaptan el forwarding ante fallos o congestión.***
- Escalabilidad condicionada: ***Complejidad de mantenimiento de tablas crece con los nodos.***
- Distribución de carga: ***Posibilidad de balanceo multipath (ECMP, multipath TCP).***
- Autocuración (self-healing): Reconfiguración rápida tras pérdida de enlaces.

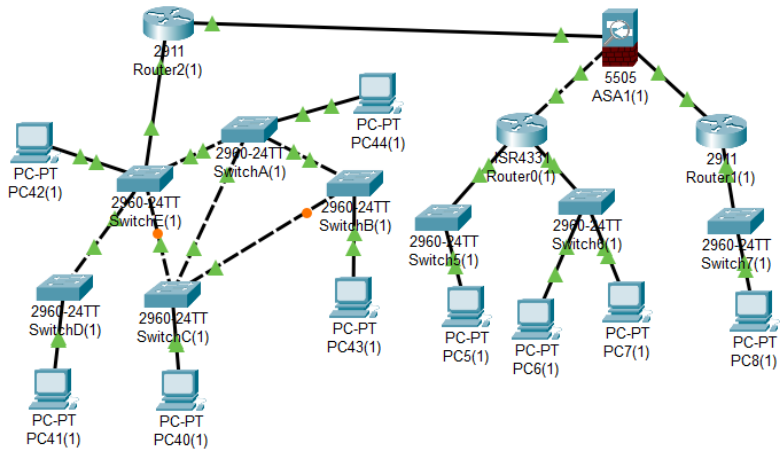
VENTAJAS	*DESVENTAJAS*
Alta disponibilidad y tolerancia a fallos. Reducción de latencias en trayectos críticos (caminos más cortos múltiples). Eliminación de puntos únicos de falla (si se diseña adecuadamente). Uso eficiente de ancho de banda mediante paths paralelos. Mejor soporte para tráfico este-oeste (data centers, microservicios). Facilidad de crecimiento incremental en malla parcial o lógica.	Coste elevado en malla completa (cables, puertos, óptica, energía). Mayor complejidad de gestión y de políticas de seguridad. Sobrecarga de señalización de protocolos de enrutamiento si no se optimiza. Mayor superficie de ataque (más enlaces, más puntos de acceso potencial). Dificultad en troubleshooting sin herramientas de visibilidad avanzadas.

La topología de malla es un pilar en diseños que requieren alta disponibilidad, baja latencia y flexibilidad en la ingeniería de tráfico. Su adopción debe balancear redundancia y coste mediante estrategias parciales y el apoyo de tecnologías de automatización, segmentación y telemetría avanzada. Bien implementada, soporta de forma robusta aplicaciones modernas distribuidas, servicios en tiempo real, IoT industrial y arquitecturas multicloud, sirviendo como base resiliente para la evolución futura de redes convergentes y definidas por software.

2.6.6. Topología híbrida

Una topología híbrida en redes combina dos o más topologías de red estándar, como estrella, bus, anillo o malla, en una única configuración para crear una estructura de red más flexible, escalable y eficiente. Este enfoque permite a las organizaciones aprovechar las ventajas de cada topología individual, adaptando la red a necesidades específicas de rendimiento, ubicación de los dispositivos y cantidad de usuarios, resultando en una solución compleja, pero a menudo más robusta y tolerante a fallos.

Figura 38. Topología de red tipo híbrida en simulador CISCO Packet Tracer



Es una solución flexible y eficiente que se adapta a las necesidades específicas de redes complejas y grandes, donde las topologías tradicionales no son suficientes para garantizar un rendimiento óptimo.

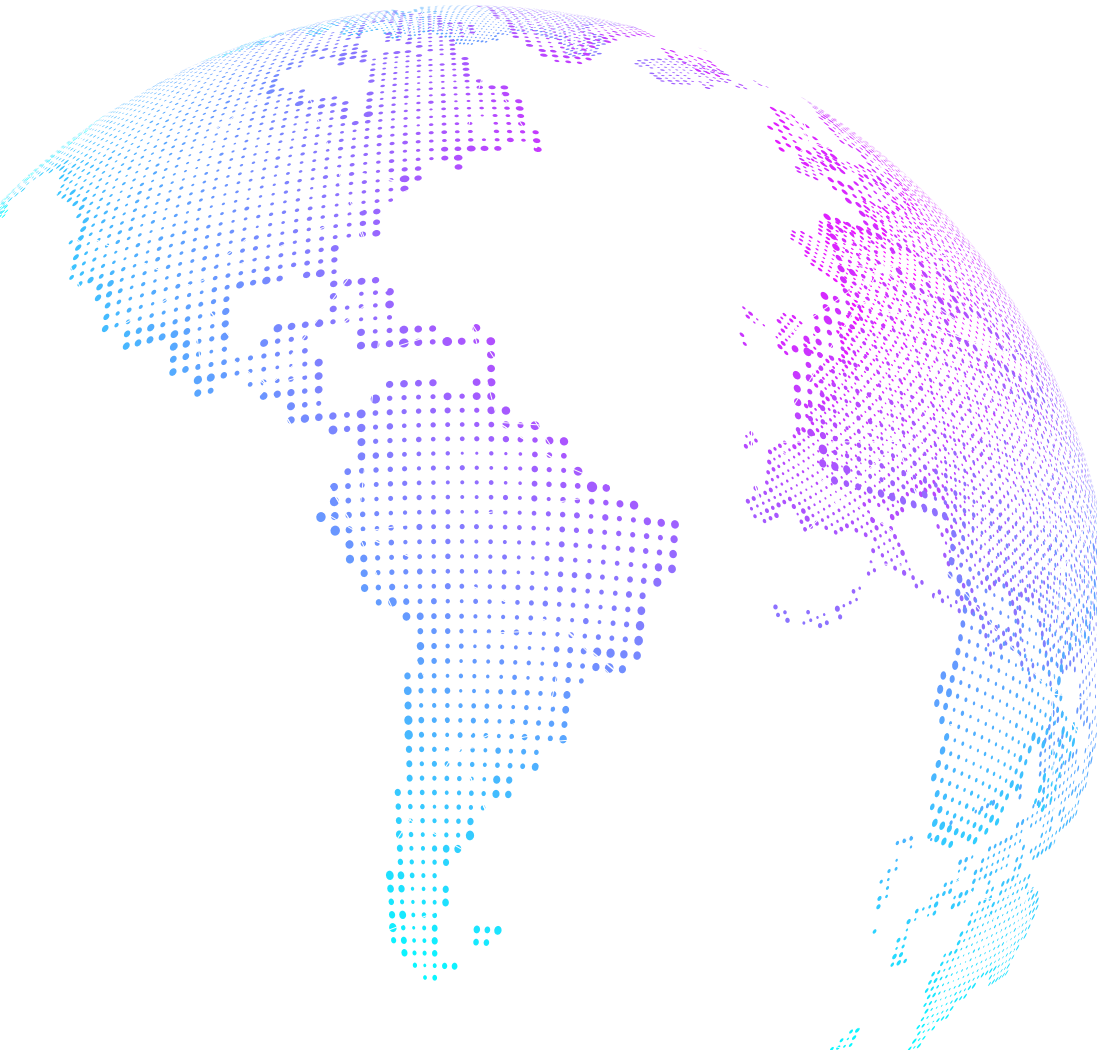
Tabla. Características principales de la topología híbrida

Características	*Descripción*
Combinación de topologías	Integra diferentes topologías (estrella, bus, anillo, árbol, entre otras) en una única red. La estructura puede variar dependiendo de los requisitos funcionales, físicos y de rendimiento de la red.
Flexibilidad	Permite diseñar redes adaptadas a los entornos específicos, como oficinas, fábricas, universidades o centros de datos. Ofrece la posibilidad de modificar o ampliar la red sin necesidad de rediseñarla completamente.
Dependencia de nodos principales	Aunque es una combinación de topologías, la red puede depender de nodos centrales o puntos críticos, dependiendo de la estructura utilizada.

Tabla. Ventajas y desventajas de la topología híbrida

VENTAJAS	*DESVENTAJAS*
Adaptabilidad Se puede personalizar según las necesidades específicas de la organización, combinando las mejores características de cada topología. ***Escalabilidad*** Es fácil añadir nuevos nodos o subredes sin comprometer el rendimiento general de la red. ***Eficiencia*** Al combinar topologías, se optimiza la comunicación y el uso de recursos, reduciendo problemas como colisiones o congestión. ***Resiliencia:*** Al integrar redundancia en el diseño, se puede garantizar que una falla en una parte de la red no afecte al resto.	***Complejidad*** El diseño, implementación y mantenimiento de una topología híbrida requiere un alto nivel de conocimiento técnico. ***Costo elevado*** La combinación de diferentes topologías puede incrementar los costos de hardware, cableado y configuración. ***Diagnóstico de fallas*** Identificar problemas en una red híbrida puede ser más complicado debido a la interacción entre las diferentes topologías.

CAPÍTULO III
PROTOCOLOS Y COMUNICACIONES



CAPÍTULO III

PROTOCOLOS Y COMUNICACIONES

3.1. Protocolos de red

Los protocolos de red son un conjunto de reglas y estándares que permiten la comunicación entre dispositivos en una red. Estos protocolos definen cómo se envían y reciben los datos, asegurando que la información se transfiera de manera efectiva y sin errores. Dentro de los más utilizados se tiene los siguientes protocolos:

- ***Internet Protocol (IP):*** Protocolo fundamental que se encarga del direccionamiento y enrutamiento de paquetes de datos en una red. Existen dos versiones principales: IPv4 e IPv6.
- ***Transmission Control Protocol (TCP):*** Protocolo que asegura la entrega confiable de datos entre dispositivos. Establece una conexión antes de enviar datos y garantiza que los paquetes lleguen en orden y sin errores.
- ***User Datagram Protocol (UDP):*** Protocolo que permite el envío de datagramas sin establecer una conexión previa. Es más rápido que TCP, pero no garantiza la entrega ni el orden de los paquetes, lo que lo hace adecuado para aplicaciones como streaming de video o juegos en línea.
- ***Hypertext Transfer Protocol (HTTP);*** Protocolo utilizado para la transferencia de información en la web. Permite la comunicación entre navegadores y servidores web. Su versión segura es HTTPS, que utiliza cifrado para proteger los datos.
- ***File Transfer Protocol (FTP):*** Protocolo utilizado para la transferencia de archivos entre un cliente y un servidor. Permite subir y bajar archivos de manera eficiente. También tiene versiones seguras como FTPS y SFTP.
- ***Simple Mail Transfer Protocol (SMTP):*** Protocolo utilizado para el envío de correos electrónicos. Se encarga de la transmisión de mensajes desde el cliente de correo al servidor de correo.
- ***Post Office Protocol (POP3):*** Protocolo utilizado por los clientes de correo electrónico para recuperar correos desde un servidor. Descarga los correos y, generalmente, los elimina del servidor.
- ***Internet Message Access Protocol (IMAP):*** Protocolo que permite a los clientes de correo acceder a los mensajes en un servidor de correo. A diferencia de POP3, IMAP permite gestionar los correos directamente en el servidor, lo que facilita el acceso desde múltiples dispositivos.
- ***Dynamic Host Configuration Protocol (DHCP):*** Protocolo que asigna direcciones IP automáticamente a los dispositivos en una red. Facilita la gestión de direcciones IP sin necesidad de configurarlas manualmente.
- ***Domain Name System (DNS):*** Protocolo que traduce nombres de dominio en direcciones IP. Permite que los usuarios accedan a sitios web mediante nombres fáciles de recordar en lugar de tener que recordar direcciones IP numéricas.
- ***Secure Sockets Layer (SSL) / Transport Layer Security (TLS):*** Protocolos de seguridad que proporcionan cifrado para la transmisión de datos a través de Internet. Se utilizan comúnmente en conexiones HTTPS para proteger la información sensible.
- ***Address Resolution Protocol (ARP):*** Protocolo utilizado para mapear direcciones IP a direcciones MAC en una red local. Permite que los dispositivos se encuentren y se comuniquen dentro de la misma red.
- ***Network Time Protocol (NTP):*** Protocolo que sincroniza los relojes de los dispositivos en una

red. Asegura que todos los dispositivos tengan la misma hora, lo cual es crucial para muchas aplicaciones.

- ***Point-to-Point Protocol (PPP):*** Protocolo utilizado para establecer una conexión directa entre dos nodos de red. Se utiliza comúnmente en conexiones de acceso telefónico y en redes de área amplia (WAN).
- ***Layer 2 Tunneling Protocol (L2TP):*** Protocolo de túnel que permite la creación de conexiones VPN. Combina características de PPP y L2F (Layer 2 Forwarding) para proporcionar una comunicación segura.

3.1.1. Internet Protocol (IP)

El Internet Protocol (IP) es uno de los protocolos más importantes en el conjunto de protocolos de Internet. Su función principal es permitir la comunicación entre dispositivos a través de una red. IP se encarga de la dirección y el enrutamiento de los paquetes de datos desde el origen hasta el destino. Dirección IP: Identifica un dispositivo en una red. Está compuesta por 32 bits (en IPv4) y se representa en formato decimal (ej: 192.168.1.1).

Existen dos versiones principales de IP:

a) IPv4 (Internet Protocol version 4):

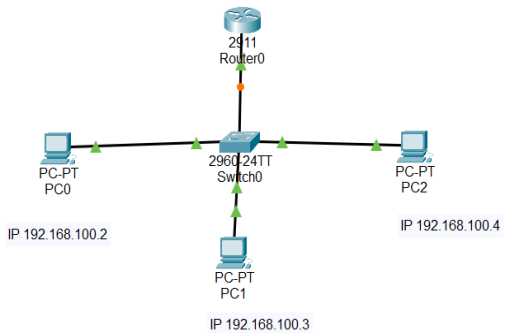
- Utiliza direcciones de 32 bits.
- Permite aproximadamente 4.3 mil millones de direcciones únicas.
- Se representa en formato decimal, dividido en cuatro octetos (por ejemplo, 192.168.1.1).

b) IPv6 (Internet Protocol version 6):

- Utiliza direcciones de 128 bits.
- Permite un número prácticamente ilimitado de direcciones únicas (340 undecillones).
- Se representa en formato hexadecimal, dividido en ocho grupos de cuatro dígitos (por ejemplo, 2001:0db8:85a3:0000:0000:8a2e:0370:7334).

Funciones del IP

- ***Direccionamiento:*** Cada dispositivo en una red debe tener una dirección IP única para poder enviar y recibir datos.
- ***Encaminamiento:*** IP determina la mejor ruta para que los datos lleguen a su destino. Esto se realiza a través de routers que analizan la dirección IP de destino y deciden cómo enviar los datos.



Clases de direcciones IP

• *Clase A*

La IP está conformada de 4 octetos. Cada octeto tiene 8 número binarios (0 y 1). Los primeros 3 octetos son de red y el último octeto es de host.

R	*H*	*H*	*H*
01100101	11010001	10010101	00000000

El rango va desde 0.0.0.0 hasta 127.255.255.255. Utiliza el primer octeto para identificar la red y los otros tres octetos para los hosts, por ello permite un gran número de hosts por red (hasta 16.777.214).

Generalmente es usado por grandes organizaciones, proveedores de servicios de Internet (ISP) y empresas que requieren una gran cantidad de direcciones IP.

Ejemplo:

Dirección IP 125.100.0.0

• *Clase B*

Dos octetos son de red y dos de host.

R	*R*	*H*	*H*
10101011	11010001	10010101	00000000

El rango de direcciones es de 128.0.0.0 a 191.255.255.255. Permite un número moderado de hosts por red (hasta 65.534).

Es utilizado por empresas medianas y grandes que requieren un número considerable de direcciones IP.

Ejemplo:

Dirección IP: 172.16.0.0

• *Clase C*

Tres octetos son de red y uno de host.

R	*H*	*H*	*H*
11001011	11010000	10000000	00000000

El rango de direcciones es de: 192.0.0.0 a 223.255.255.255

Utiliza los tres primeros octetos para identificar la red y el último para los hosts. Permite un número limitado de hosts por red (hasta 254). La primera dirección (por ejemplo, 192.0.0.0) es la dirección de red, y la última (por ejemplo: 223.255.255.255) es la dirección de broadcast.

Comúnmente es utilizado por pequeñas empresas y redes domésticas debido a su capacidad limitada de hosts.

Ejemplo:

Dirección IP: 192.168.1.0

Tipo C porque el primer octeto es 192

3.1.2. Máscara de subred

Una máscara de subred es un número que se utiliza junto con una dirección IP para dividir una red en subredes más pequeñas. Esto permite una mejor organización y gestión de las direcciones IP dentro de una red.

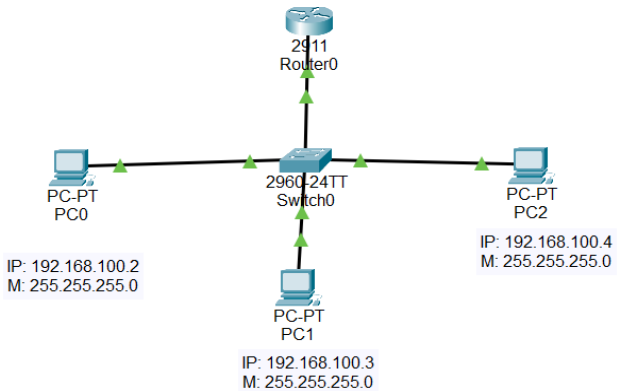
La máscara de subred también se representa en formato decimal, similar a una dirección IP. Por ejemplo, una máscara de subred común es 255.255.255.0. Esta máscara indica que los primeros tres octetos (24 bits) de la dirección IP se utilizan para identificar la red, mientras que el último octeto (8 bits) se utiliza para identificar los dispositivos dentro de esa red.

Además, define qué parte de la dirección IP identifica la red y qué parte identifica el host. Se representa en formato decimal (ejemplo: 255.255.255.0) o en formato CIDR (ejemplo: /24).

Ejemplo de máscara de subred

Consideremos una red con la dirección IP 192.168.1.0 y la máscara de subred 255.255.255.0. Esto significa que:

- ***Red:*** 192.168.1.0
- ***Máscara de subred:*** 255.255.255.0
- ***Rango de direcciones IP disponibles:*** 192.168.1.1 a 192.168.1.254
- ***IP*** 192.168.1.255 se reserva como dirección de broadcast



Importancia de la máscara de subred

La máscara de subred es crucial para:

- ***Segmentación de redes:*** Permite dividir una red grande en subredes más pequeñas, lo que mejora la eficiencia y la seguridad.
- ***Reducción de tráfico:*** Al segmentar redes, se reduce el tráfico innecesario, ya que los dispositivos solo reciben datos destinados a su subred.
- ***Mejor administración:*** Facilita la gestión de direcciones IP y la implementación de políticas de seguridad.

Clase	*Rango de Direcciones*	*Máscara de Subred*	*Hosts por Red*	*Ejemplo de IP*
A	0.0.0.0 a 127.255.255.255	255.0.0.0 (/8)	16,777,214	10.0.0.1
B	128.0.0.0 a 191.255.255.255	255.255.0.0 (/16)	65,534	172.16.0.1
C	192.0.0.0 a 223.255.255.255	255.255.255.0 (/24)	254	192.168.1.1

3.1.3. Gateway

Un gateway (puerta de enlace) es un dispositivo de red que actúa como un punto de acceso entre diferentes redes, permitiendo la comunicación y el intercambio de datos entre ellas. Se utiliza para conectar redes que utilizan diferentes protocolos, lo que facilita la interoperabilidad entre sistemas diversos. Además, un Gateway se refiere a un punto de acceso que permite la comunicación entre diferentes redes o sistemas. En el ámbito tecnológico, puede tener diversas aplicaciones, incluyendo:

a) Redes Informáticas:

- Actúa como un nodo que conecta dos redes con diferentes protocolos (distintas IP), facilitando la transferencia de datos entre ellas.
- Ejemplos incluyen routers y firewalls que gestionan el tráfico de datos.

b) Internet de las Cosas (IoT):

- En IoT, un gateway conecta dispositivos inteligentes a internet, permitiendo la recopilación y transmisión de datos.
- Puede realizar funciones de procesamiento de datos, asegurando que solo la información relevante sea enviada a la nube.

c) Servicios en la Nube:

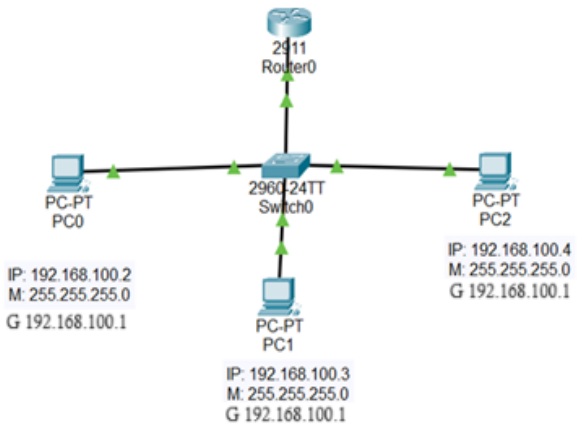
- Los gateways en la nube permiten la integración de servicios locales con aplicaciones basadas en la nube.
- Facilitan la gestión de datos y la comunicación entre sistemas locales y plataformas de nube.

Existen varios tipos de Gateway:

- ***Gateway de Aplicación:*** Facilita la comunicación entre diferentes aplicaciones, transformando los datos según sea necesario.
- ***Gateway de Protocolo:*** Permite la interconexión de redes que utilizan diferentes protocolos de comunicación.
- ***Gateway de Seguridad:*** Actúa como un filtro para proteger redes de amenazas externas, gestionando el tráfico y asegurando la integridad de los datos.

Funciones Clave:

- ***Interoperabilidad:*** Permite que diferentes sistemas y redes se comuniquen eficazmente.
- ***Transformación de Datos:*** Puede modificar el formato de los datos para que sean comprensibles en diferentes sistemas.
- ***Seguridad:*** Proporciona capas adicionales de seguridad al controlar el acceso y filtrar el tráfico.



Su capacidad para facilitar la comunicación, asegurar datos y transformar información convierte a la puerta de enlace en un componente esencial en diversas aplicaciones tecnológicas. Es indispensable conocer que cada dispositivo de la misma red tiene un solo Gateway, el mismo que debe estar dentro de la misma IP que se está utilizando.

Ejemplo:

Se tiene la IP 192.168.100.0. Como es una IP clase C (el primer octeto es 192), los primeros 3 octetos son de Red (esos números no se mueven) y el último octeto es de Host (único que cambia acorde a la red que se tiene), entonces solo ese octeto puede cambiar acorde a nuestras necesidades.

IP madre	Máscara	Prefijo	IP utilizables	Puerta de enlace	Broadcast
192.168.100.0	255.255.255.0	/24	192.168.100.1 192.168.100.254	192.168.100.1	192.168.100.255

Cuando se tiene una IP clase C, si no está subneteado (dividido en subredes pequeñas) la máscara de es 255.255.255.0, lo mismo que en binario sería: 11111111.11111111.11111111.00000000. Se puede colocar la máscara completa en decimales o simplemente el prefijo que sería el conteo de los "1", es decir "/24"

Ejercicios

Se tiene la IP 145.200.10.0. ¿Determine qué clase de IP es y cuál es su máscara?

Resolución:

Lo primero que se determina es a qué Clase de IP pertenece.

Los rangos de los tipos de IP son:

- Clase A: 0-127
- Clase B: 128-191
- Clase C: 192-223

Entonces la IP 145.200.10.0 está dentro del rango de la clase B. Se debe recordar cuando es clase B se tiene 2 octetos de red y 2 de host (R.R.H.H.). Entonces la máscara será 255.255.0.0.

Se tiene la IP 195.20.10.0. ¿Determine qué clase de IP es y cuál es su máscara?

Resolución:

Lo primero que se determina es a qué Clase de IP pertenece.

Los rangos de los tipos de IP son:

- Clase A: 0-127
- Clase B: 128-191
- Clase C: 192-223

Entonces la IP 195.20.10.0 está dentro del rango de la clase C. Se debe recordar cuando es clase C se tiene 3 octetos de red y 1 de host (R.R.R.H.). Entonces la máscara será 255.255.255.0.

3.2. Subneteo

El subneteo (o subnetting) es una técnica utilizada en redes de computadoras para dividir una red IP en varias subredes más pequeñas, conocidas como subredes. Esto se hace para mejorar la eficiencia en el uso de direcciones IP, facilitar la administración de la red, mejorar la seguridad y optimizar el rendimiento al reducir el tráfico en cada segmento de la red.

La subred es una división lógica de una red IP. Cada subred tiene su propio rango de direcciones IP. El CIDR (Classless Inter-Domain Routing) es una notación que indica cuántos bits de la dirección IP pertenecen a la red (ej: /24 significa que los primeros 24 bits son la red).

Los objetivos del Subneteo pueden ser:

- ***Optimizar el uso de direcciones IP:*** Evitar el desperdicio de direcciones en redes grandes.

- ***Mejorar el rendimiento:*** Reducir la congestión al dividir la red en segmentos más pequeños.
- ***Aumentar la seguridad:*** Aislar tráfico entre subredes.
- ***Facilitar la administración:*** Organizar dispositivos en grupos lógicos.

El subneteo implica "tomar prestados" bits de la parte del host de una dirección IP para crear subredes adicionales. Esto afecta la máscara de subred y el número de hosts disponibles en cada subred.

Pasos para realizar subneteo:

a) ***Identificar la dirección IP y la máscara de subred original:***
Ejemplo: Red 192.168.1.0 con máscara 255.255.255.0 (/24).
b) ***Determinar el número de subredes necesarias:***
Depende de cuántas subredes se requieran.
c) ***Calcular los bits necesarios para las subredes:***
Usar la fórmula: $2^n \geq$ Número de subredes $2^n \geq$ Número de subredes, donde n es el número de bits a «tomar prestados».
d) ***Calcular la nueva máscara de subred:***
Sumar los bits prestados a la máscara original.
Ejemplo: Si se toman 2 bits prestados en una red /24, la nueva máscara será /26 (24 + 2).
e) ***Determinar el número de hosts por subred:***
Usar la fórmula: 2^m-2, donde m es el número de bits restantes para hosts.
f) ***Calcular los rangos de direcciones IP para cada subred:***
Dividir la red original en bloques según los bits prestados.

Ejercicio de subneteo

Supongamos que se tiene la red ***192.168.1.0/24*** y se necesita crear 4 subredes.

a) ***Bits necesarios para subredes:***
$2n \geq 4 \rightarrow n=2$ (porque $22 = 4$).
b) ***Nueva máscara de subred:***
Original: /24 → Nueva: /26 (24 + 2).
11111111.11111111.11111111.11000000→255.255.255.192
c) ***Número de hosts por subred:***
Bits para hosts: 32-26=6
Hosts por subred: 26-2=62.
d) ***Rangos de subredes:***
Subred 1: 192.168.1.0/26 (Hosts: 192.168.1.1 - 192.168.1.62).
Subred 2: 192.168.1.64/26 (Hosts: 192.168.1.65 - 192.168.1.126).
Subred 3: 192.168.1.128/26 (Hosts: 192.168.1.129 - 192.168.1.190).
Subred 4: 192.168.1.192/26 No es utilizable.

Otra forma de resolver:

Supongamos que se tiene la red ***192.168.1.0/24*** y se necesita crear 4 subredes.

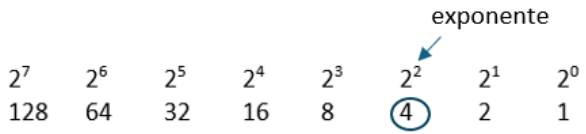
a) El /24 significa que, de los 32 bit, 24 están prendidos y el resto apagados (11111111.11111111. 11111111.00000000).

b)

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1

El octeto está dividido en 8 elementos, los bits son 0 y 1, base 2.

c) Para resolver de esta forma lo primero que se debe conocer es que cuando se habla de host eso equivale a "0" y cuando se habla de subredes es "1". Entonces si nos piden para 4 subredes se debe mirar en la tabla que número le contiene o es igual a 4 y en la fila superior al exponente que esta elevado la base 2.



Como el exponente es 2 y se está calculando para subredes significaría que son 2 "1", entonces el octeto de donde vamos a trabajar tendrá 2 "1" y 6 "0". Queda así: 11000000 en binario, lo que corresponde en decimal a 192. Por lo que la máscara quedaría: 255.255.255.192

d) Ahora podemos también calcular los saltos para las nuevas subredes. Hay que tomar en cuenta que los saltos dan la base 2 elevado a la cantidad de ceros. En nuestro ejemplo se tiene 6 ceros, eso equivale a 26 = 64, entonces los saltos son de 64 en 64.

IP: 192.168.1.0 (IP madre no se utiliza)
192.168.1.1 - 192.168.1.32 (IP utilizables)
192.168.1.33 (IP de broadcast no se utiliza)

Primer salto:
192.168.1.64 (IP madre no se utiliza)
192.168.1.65 - 192.168.1.126 (IP utilizables)
192.168.1.127 (IP de broadcast no se utiliza)

Segundo salto:
192.168.1.128 (IP madre no se utiliza)
192.168.1.129 - 192.168.1.190 (IP utilizables)
192.168.1.191 (IP de broadcast no se utiliza)

Siguiente salto:
192.168.1.192 (IP madre no se utiliza)
Los saltos se harán hasta que el número del salto sea menor a la máscara:
192.168.1.192 255.255.255.192
192.168.1.128 Último salto válido

Consideraciones Importantes

- ***Dirección de red:*** La primera dirección en cada subred identifica la subred (no se puede asignar a un host).
- ***Dirección de broadcast:*** La última dirección en cada subred se usa para broadcast (no se puede asignar a un host).

- ***Subneteo VLSM (Variable Length Subnet Mask):*** Permite crear subredes de diferentes tamaños dentro de la misma red principal.
- ***Calculadoras de subredes:*** Herramientas en línea o software que automatizan los cálculos.
- ***Comandos de red:*** En sistemas operativos como Windows (ipconfig) o Linux (ifconfig).

El subneteo es una habilidad esencial para los administradores de redes, ya que permite diseñar redes eficientes y escalables.

Ejercicios de subneteo

1. ***Se tiene una IP clase B. Al inicio de la red se necesita solo 10 subredes. Cada año aumentará 5 subredes. ¿Qué máscara se debe utilizar al cabo de 4 años?***

Resolución: Inicio 10 subredes + 20 subredes = 30 subredes

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1

2^5=32

R. R. H. H

11111111.11111111.11111000.00000000

128+64+32+16+8=***248***

Respuesta:

255.255.248.0

2. ***Usted tiene la siguiente dirección IP 192.233.10.56/28 ¿Cuántos IP para host y cuantas subredes como máximo son posibles?***

Resolución:

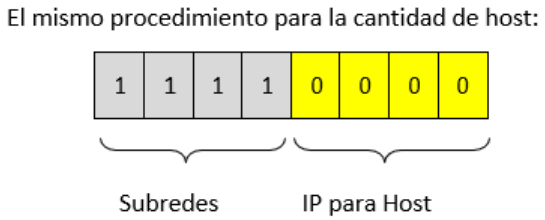
Primero identificamos a que clase pertenece y vemos el primer octeto del lado izquierdo de la dirección IP que es 192 y podemos determinar que es una dirección de Clase C por lo tanto su máscara es de:

Mascara por defecto	255.255.255.0	=>	24 bits.
Mascara de la IP	255.255.255.240	=>	28 bits.

Podemos concluir lo siguiente:

$2^n = 2^4 = 16$ subredes como máximo.

El mismo procedimiento para la cantidad de host:



Como se aplica la misma fórmula tenemos lo siguientes:

$2^n = 2^4 = 16$ IP por subred como máximo.

Respuesta:

16 subredes como máximo

16 host por subred como máximo

---

3. *Se tiene una IP 150.10.95.0/20*

Encontrar:

- Max. Subredes utilizables: ***$2^4 - 2 = 14$***
- Max. Hosts utilizables: ***$2^{12} - 2 = 4094$***
- Máscara: ***255.255.240.0***
- Saltos que tiene el tercer octeto: ***de 16 en 16***
- IP a la que pertenece la subred dada (IP madre):
  150.10.0.0
  150.10.16.0
  150.10.32.0
  150.10.48.0
  150.10.64.0
  150.10.80.0
  150.10.96.0
- IP utilizables en este salto y el broadcast
  150.10.81.0.....150.10.94.0
  Broadcast: ***150.10.95.0***

---

4. *Se tiene una IP clase C. La red empieza con 4 subredes, cada año aumenta 3 subredes. Encontrar la máscara al cabo de 5 años.*

4 subredes

3 subredes c/a, después de 5 =15 +4 =19

Al 19 le contiene el 32, para tener este número se eleva el 2 a la 5, entonces el 5 son "1" porque estamos calculando subredes. Queda de la siguiente forma el último octeto: 11111000 en binario. Para tener la respuesta se le pasa a decimal.

Respuesta:

255.255.255.248

---

5. *Se tiene las siguientes subredes;*

195.10.0.0/28

192.16.0.0/29

198.32.0.0/30

¿Cuál de las 3 subredes puede tener más host utilizables?

Tomando en cuenta que para calcular los hosts se lo hace mediante la cantidad de "0", la subred que más host tiene es la 195.10.0.0/28 porque en el último octeto tendríamos 4 "0" (11110000). Entonces la cantidad de host sería: 2^4=16

---

6. *¿Qué máscara puedo utilizar para tener 1200 host, tomando en cuenta que la IP es clase B?*

2^{12}	2^{11}	2^{10}	2^9	2^8	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
2048	1024	512	256	128	64	32	16	8	4	2	1	

El número que le contiene a 1200 es el 2048, entonces el exponente es 11. Por lo tanto, la respuesta serán 11 "0" y los octetos quedarán de la siguiente forma:

11111111.11111111.11111000.00000000 (en binario)

Lo pasamos a decimal: 255.255.248.0

Respuesta:

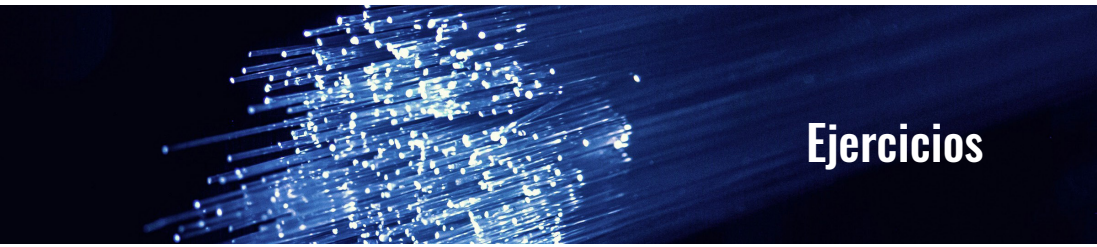
255.255.248.0

3.3. VLSM (Variable Length Subnet Mask)

VLSM es una técnica utilizada en redes para asignar diferentes longitudes de máscara de subred a diferentes subredes. Esto permite un uso más eficiente de las direcciones IP, ya que se puede asignar solo la cantidad necesaria de direcciones a cada subred. Se utiliza esta técnica para evitar el desperdicio de IP.

Características:

- VLSM permite una gestión eficiente de las direcciones IP adecuándola a las necesidades de la red o cantidad de host disponibles por cada subred.
- Puede crear subredes de diferentes tamaños según las necesidades, de ésta forma se da mayor seguridad a la misma.
- Asignar direcciones y máscaras adecuadas es clave para el funcionamiento óptimo de la red.



Ejercicios

EJEMPLO PRÁCTICO 1

Se tiene una IP 192.168.1.0. Utilizar VLSM para el cálculo de las siguientes subredes:

1. ***Subred B:*** 30 hosts
2. ***Subred C:*** 10 hosts
3. ***Subred A:*** 50 hosts

Paso 1: Ordenar las subredes que se tiene de mayor a menor de acuerdo a la cantidad de host.

1. ***Subred A:*** 50 hosts
2. ***Subred B:*** 30 hosts
3. ***Subred C:*** 10 hosts

Paso 2: Calcular las máscaras necesarias

- ***Subred A:*** Necesitamos al menos 50 direcciones. La siguiente potencia de 2 que cubre esto es 64 (2^6). Por lo tanto, la máscara será /26 (255.255.255.192).
- ***Subred B:*** Necesitamos al menos 30 direcciones. La siguiente potencia es 32 (2^5). Así que la máscara será /27 (255.255.255.224).
- ***Subred C:*** Necesitamos al menos 10 direcciones. La siguiente potencia es 16 (2^4). La máscara será /28 (255.255.255.240).

Paso 3: Asignar las subredes

- ***Subred A:*** 192.168.1.0/26
  - Rango de hosts: 192.168.1.1 - 192.168.1.62
  - Dirección de broadcast: 192.168.1.63
- ***Subred B:*** 192.168.1.64/27
  - Rango de hosts: 192.168.1.65 - 192.168.1.94
  - Dirección de broadcast: 192.168.1.95
- ***Subred C:*** 192.168.1.96/28
  - Rango de hosts: 192.168.1.97 - 192.168.1.110
  - Dirección de broadcast: 192.168.1.111

Subred	*IP madre*	*Máscara*	*IP utilizable*	*Broadcast*
Subred A	192.168.1.0	255.255.255.192	192.168.1.0 - 192.168.1.62	192.168.1.63
Subred B	192.168.1.64	255.255.255.224	192.168.1.65 - 192.168.1.94	192.168.1.95
Subred C	192.168.1.96	255.255.255.240	192.168.1.97 - 192.168.1.110	192.168.1.111

EJEMPLO PRÁCTICO 2

Red inicial: 172.16.0.0/24

Requerimientos de subredes:

Subred 1: 100 hosts

Subred 2: 50 hosts

Subred 3: 25 hosts

Subred 4: 10 hosts

Subred 5: 5 hosts

Paso 1: Calcular las máscaras necesarias

- ***Subred 1:*** Necesitamos al menos 100 direcciones. La siguiente potencia de 2 es 128 (2^7). Por lo tanto, la máscara será /25 (255.255.255.128).
- ***Subred 2:*** Necesitamos al menos 50 direcciones. La siguiente potencia es 64 (2^6). Así que la máscara será /26 (255.255.255.192).
- ***Subred 3:*** Necesitamos al menos 25 direcciones. La siguiente potencia es 32 (2^5). La máscara será /27 (255.255.255.224).
- ***Subred 4:*** Necesitamos al menos 10 direcciones. La siguiente potencia es 16 (2^4). La máscara será /28 (255.255.255.240).
- ***Subred 5:*** Necesitamos al menos 5 direcciones. La siguiente potencia es 8 (2^3). La máscara será /29 (255.255.255.248).

Paso 2: Asignar las subredes

a) ***Subred 1:*** 172.16.0.0/25
- ***Rango de hosts:*** 172.16.0.1 - 172.16.0.126
- ***Dirección de broadcast:*** 172.16.0.127

b) ***Subred 2:*** 172.16.0.128/26
- ***Rango de hosts:*** 172.16.0.129 - 172.16.0.190
- ***Dirección de broadcast:*** 172.16.0.191

c) ***Subred 3:*** 172.16.0.192/27
- ***Rango de hosts:*** 172.16.0.193 - 172.16.0.222
- ***Dirección de broadcast:*** 172.16.0.223

d) ***Subred 4:*** 172.16.0.224/28
- ***Rango de hosts:*** 172.16.0.225 - 172.16.0.238
- ***Dirección de broadcast:*** 172.16.0.239

e) ***Subred 5:*** 172.16.0.240/29
- ***Rango de hosts:*** 172.16.0.241 - 172.16.0.246
- ***Dirección de broadcast:*** 172.16.0.247

Resumen de la Asignación de Subredes con VLSM

Subred	*Dirección de Red*	*Máscara*	*Rango de Hosts*	*Dirección de Broadcast*
Subred 1	172.16.0.0	/25 (255.255.255.128)	172.16.0.1 - 172.16.0.126	172.16.0.127
Subred 2	172.16.0.128	/26 (255.255.255.192)	172.16.0.129 - 172.16.0.190	172.16.0.191
Subred 3	172.16.0.192	/27 (255.255.255.224)	172.16.0.193 - 172.16.0.222	172.16.0.223
Subred 4	172.16.0.224	/28 (255.255.255.240)	172.16.0.225 - 172.16.0.238	172.16.0.239
Subred 5	172.16.0.240	/29 (255.255.255.248)	172.16.0.241 - 172.16.0.246	172.16.0.247

EJEMPLO PRÁCTICO 3

Se tiene las siguientes subredes:

Subred 1: 30 host

Subred 2: 10 host

Subred 3: 4 host

Subred 4: 50 host

Subred 5: 14 host

3 enlaces de 2 host cada uno

Realizar un VLSM vs Subneteo con una sola mascara y determinar ¿cuántas posibles IP pérdidas tengo de diferencia al utilizar estos dos métodos?

La IP a utilizar es 198.100.0.0

Se calcula los saltos y estos son de 64 en 64

Subneteo con una sola máscara

El momento que se realiza un Subneteo con una sola máscara significa que los saltos van a ser iguales para todas las redes sin importar la cantidad de dispositivos finales que tengan cada una de ellas.

Subred	*IP madre*	*Máscara*	*IP utilizables*	*Broadcast*	*Posible IP pérdidas*
Subred 1: 30 host	198.100.0.0	255.255.255.192	198.100.0.1 – 198.100.0.62	198.100.0.63	32
Subred 2: 10 host	198.100.0.64	255.255.255.192	198.100.0.65 – 198.100.0.126	198.100.0.127	52
Subred 3: 4 host	198.100.0.128	255.255.255.192	198.100.0.129 – 198.100.0.190	198.100.0.191	58
Subred 4: 50 host	198.100.1.0	255.255.255.192	198.100.1.1 – 198.100.1.62	198.100.1.63	12
Subred 5: 14 host	198.100.1.64	255.255.255.192	198.100.1.65 – 198.100.1.126	198.100.1.127	48
Enlace 1	198.100.1.128	255.255.255.192	198.100.1.129 – 198.100.1.190	198.100.1.191	60
Enlace 2	198.100.2.0	255.255.255.192	198.100.2.1 – 198.100.2.62	198.100.2.63	60
Enlace 3	198.100.2.64	255.255.255.192	198.100.2.65 – 198.100.2.126	198.100.2.127	60
Total posibles IP perdidas					382

Subneteo con VLSM.

Al momento de realizar el Subneteo con VLSM hay que recordar que se va a utilizar las máscaras de acuerdo con la cantidad de dispositivos finales.

Subred	*IP madre*	*Máscara*	*IP utilizables*	*Broadcast*	*Posible IP pérdidas*
Subred 4: 50 host	198.100.0.0	255.255.255.192	198.100.0.1 - 198.100.0.62	198.100.0.63	12
Subred 1: 30 host	198.100.0.64	255.255.255.224	198.100.0.65 - 198.100.0.94	198.100.0.95	0

Subred	*IP madre*	*Máscara*	*IP utilizables*	*Broadcast*	*Posible IP pérdidas*
Subred 5: 14 host	198.100.0.96	255.255.255.240	198.100.0.97 - 198.100.0.110	198.100.0.111	0
Subred 2: 10 host	198.100.0.112	255.255.255.240	198.100.0.113 - 198.100.0.126	198.100.0.127	4
Subred 3: 4 host	198.100.0.128	255.255.255.248	198.100.0.129 - 198.100.0.134	198.100.0.135	2
Enlace 1	198.100.0.136	255.255.255.252	198.100.0.137 - 198.100.0.138	198.100.0.139	0
Enlace 2	198.100.0.140	255.255.255.252	198.100.0.141 - 198.100.0.142	198.100.0.143	0
Enlace 3	198.100.0.144	255.255.255.252	198.100.0.145 - 198.100.0.146	198.100.0.147	0
Total posibles IP perdidas					18

EJEMPLO PRÁCTICO 4.

Calcular las posibles IP que se pueden perder después de realizar en subneteo con una sola máscara o con máscara variable. Utilice la IP 198.100.0.0.

MÉTODO DE VLSM

Subred/ VLAN	*IP*	*Mascara*	*IP Utilizables*	*Broadcast*	*IP Perdidas*
Subred 60 host	198.100.0.0	255.255.255.192	198.100.0.1 - 198.100.0.62	198.100.0.63	2
Subred 45 host	198.100.0.64	255.255.255.192	198.100.0.65 - 198.100.0.126	198.100.0.127	17

Subred/ VLAN	*IP*	*Mascara*	*IP Utilizables*	*Broadcast*	*IP Perdidas*
Subred 40 host	198.100.0.128	255.255.255.192	198.100.0.129 - 198.100.0.190	198.100.0.191	22
Vlan25 30 host	198.100.0.192	255.255.255.224	198.100.0.193 - 198.100.0.222	198.100.0.223	0
Vlan100 25 host	198.100.1.0	255.255.255.224	198.100.1.1 - 198.100.1.30	198.100.1.31	5
Vlan15 20 host	198.100.1.32	255.255.255.224	198.100.1.33 - 198.100.1.62	198.100.1.63	10
Vlan10 15 host	198.100.1.64	255.255.255.224	198.100.1.65 - 198.100.1.94	198.100.1.95	15
Vlan110 15 host	198.100.1.96	255.255.255.224	198.100.1.97 - 198.100.1.126	198.100.1.127	15
Vlan50 12 host	198.100.1.128	255.255.255.224	198.100.1.129- 198.100.1.142	198.100.1.143	2
Vlan5 10 host	198.100.1.144	255.255.255.240	198.100.1.145 -198.100.1.158	198.100.1.159	4
Vlan60 8 host	198.100.1.160	255.255.255.240	198.100.1.161- 198.100.1.174	198.100.1.175	6
Vlan20 5 host	198.100.1.176	255.255.255.248	198.100.1.177 -198.100.1.182	198.100.1.183	1
Vlan70 5 host	198.100.1.184	255.255.255.248	198.100.1.185- 198.100.1.190	198.100.1.191	1
Enlace A	198.100.1.192	255.255.255.252	198.100.1.193 -198.100.1.194	198.100.1.195	0
Enlace B	198.100.1.196	255.255.255.252	198.100.1.97 - 198.100.1.198	198.100.1.199	0

Subred/ VLAN	IP	Mascara	IP Utilizables	Broadcast	IP Perdidas
Enlace C	198.100.1.200	255.255.255.252	198.100.1.201 -198.100.1.202	198.100.1.203	0
Total de posibles IP que se pierden					100

SUBNETEO CON MÁSCARA FIJA

SUBRED/ VLAN	IP	MASCARA	IP utilizables	BROADCAST	IP perdidas
SUBRED 60 HOST	198.100.0.0	255.255.255.192	198.100.0.1 - 198.100.0.62	198.100.0.63	2
SUBRED 45 HOST	198.100.0.64	255.255.255.192	198.100.0.65 - 198.100.0.126	198.100.0.127	17
SUBRED 40 HOST	198.100.0.128	255.255.255.192	198.100.0.129 198.100.0.190	198.100.0.191	22
VLAN25 30 HOST	198.100.1.0	255.255.255.192	198.100.1.1 - 198.100.1.62	198.100.1.63	32
VLAN100 25 HOST	198.100.1.64	255.255.255.192	198.100.1.65 - 198.100.1.126	198.100.1.127	37
VLAN15 20 HOST	198.100.1.128	255.255.255.192	198.100.1.129 198.100.1.190	198.100.1.191	42
VLAN10 15 HOST	198.100.2.0	255.255.255.192	198.100.2.1 - 198.100.2.62	198.100.2.63	47
VLAN110 15 HOST A	198.100.2.64	255.255.255.192	198.100.2.65 - 198.100.2.126	198.100.2.127	47
VLAN50 12 HOST	198.100.2.128	255.255.255.192	198.100.2.129 198.100.2.190	198.100.2.191	50

SUBRED/ VLAN	IP	MASCARA	IP utilizables	BROADCAST	IP perdidas
VLAN5 10 HOST	198.100.3.0	255.255.255.192	198.100.3.1 - 198.100.3.62	198.100.3.63	52
VLAN60 8 HOST	198.100.3.64	255.255.255.192	198.100.3.65 - 198.100.3.126	198.100.3.127	54
VLAN20 5 HOST A	198.100.3.128	255.255.255.192	198.100.3.129 198.100.3.190	198.100.3.191	57
VLAN70 5 HOST	198.100.4.0	255.255.255.192	198.100.4.1 - 198.100.4.62	198.100.4.63	57
ENLACE A	198.100.4.64	255.255.255.192	198.100.4.65 - 198.100.4.126	198.100.4.127	60
ENLACE B	198.100.4.128	255.255.255.192	198.100.4.129 198.100.4.190	198.100.4.191	60
ENLACE C	198.100.5.0	255.255.255.192	198.100.5.1 - 198.100.5.62	198.100.5.203	60
Total de posibles IP que se pierden					696

Como se puede ver en los ejercicios anteriores las posibles pérdidas de IP utilizando método de subneteo con una solo máscara, es decir que los saltos son iguales, se pierde muchas IP, lo que puede afectar al correcto funcionamiento de la red. En cambio, al utilizar las VLSM se calcula la máscara acorde a la cantidad de dispositivos finales que se van a utilizar, eso evita la pérdida de IP.

3.4. Enrutamiento (estático – dinámico)

3.4.1. Enrutamiento estático

El enrutamiento estático es una forma de configurar manualmente las rutas en un router para que sepa cómo llegar a ciertas redes. A diferencia del enrutamiento dinámico, donde los routers intercambian información automáticamente para aprender las rutas, el enrutamiento estático requiere que un administrador configure manualmente cada ruta. Esto es útil en redes pequeñas o donde se necesita un control preciso sobre el tráfico.

Ventajas del Enrutamiento Estático:

1. ***Simplicidad:*** Es fácil de configurar en redes pequeñas.
2. ***Bajo uso de recursos:*** No consume ancho de banda ni recursos del router para intercambiar información de enrutamiento.
3. ***Control total:*** El administrador tiene control completo sobre las rutas que se utilizan.
4. ***Seguridad:*** Al no intercambiar información de enrutamiento, es menos vulnerable a ataques.

Desventajas del Enrutamiento Estático:

1. ***Escalabilidad:*** No es práctico en redes grandes debido a la cantidad de rutas que se deben configurar manualmente.
2. ***Mantenimiento:*** Cualquier cambio en la topología de la red requiere una actualización manual de las rutas.
3. ***Falta de redundancia:*** Si una ruta falla, no hay un mecanismo automático para redirigir el tráfico.

Configuración de Enrutamiento Estático en Cisco Packet Tracer

Para simular el enrutamiento estático en Cisco Packet Tracer, sigue los siguientes pasos:

1. ***Topología de Red:***

- Cree una topología simple con al menos dos routers y dos redes LAN.
- Conecte los routers mediante interfaces seriales o Ethernet.
- Asigna direcciones IP a las interfaces de los routers y a los dispositivos finales (PCs).

2. ***Configuración de Interfaces en los Routers***

- Accede a la CLI de cada router y configura las interfaces con las direcciones IP correspondientes.

```
Router> enable

Router# configure terminal

Router(config)# interface GigabitEthernet0/0

Router(config-if)# ip address 192.168.1.1 255.255.255.0

Router(config-if)# no shutdown

Router(config-if)# exit
```

Repite este proceso para todas las interfaces de los routers.

3. ***Configuración de Rutas Estáticas***

- Usa el comando ip route para configurar rutas estáticas en cada router.

```
Router(config)# ip route [Red de Destino] [Máscara de Subred] [Next-Hop o Interfaz de Salida]
```

Ejemplo:

- Si el router necesita llegar a la red 192.168.2.0/24 a través de la dirección IP 192.168.1.2 (otro router), la configuración sería:

```
Router(config)# ip route 192.168.2.0 255.255.255.0 192.168.1.2
```

- Si la ruta es a través de una interfaz directamente conectada:

```
Router(config)# ip route 192.168.2.0 255.255.255.0 GigabitEthernet0/1
```

4. Verificación de la Configuración

- Usa el comando show ip route para verificar que las rutas estáticas se han configurado correctamente.

```
Router# show ip route
```

Deberías ver las rutas estáticas en la tabla de enrutamiento.

5. Prueba de Conectividad

- Usa el comando ping desde una PC para verificar la conectividad entre redes.

```
PC> ping 192.168.2.10
```

Si la configuración es correcta, deberías recibir respuestas exitosas.

Ejemplo Completo en Simulador de Cisco Packet Tracer

Supongamos que tienes dos routers (Router0 y Router1) conectados entre sí, y cada router tiene una red LAN conectada.

- **Router0:**
  - Interfaz GigabitEthernet0/0: 192.168.1.1/24 (conectada a la LAN1).
  - Interfaz Serial0/0/0: 10.0.0.1/30 (conectada a Router1).
- **Router1**:
  - Interfaz GigabitEthernet0/0: 192.168.2.1/24 (conectada a la LAN2).
  - Interfaz Serial0/0/0: 10.0.0.2/30 (conectada a Router0).

Configuración en Router0:

```
Router> enable

Router# configure terminal

Router(config)# interface GigabitEthernet0/0

Router(config-if)# ip address 192.168.1.1 255.255.255.0

Router(config-if)# no shutdown

Router(config-if)# exit

Router(config)# interface Serial0/0/0

Router(config-if)# ip address 10.0.0.1 255.255.255.252

Router(config-if)# no shutdown

Router(config-if)# exit

Router(config)# ip route 192.168.2.0 255.255.255.0 10.0.0.2

Router(config)# exit

Router# write memory
```

Configuración en Router1:

Verificación:

- En Router0:

```
Router# show ip route
```

- En Router1:

```
Router# show ip route
```

Ambos routers deberían mostrar las rutas estáticas configuradas.

Prueba de Conectividad:

- Desde una PC en la LAN1 (192.168.1.10):

```
PC> ping 192.168.2.10
```

Si todo está configurado correctamente, el ping debería ser exitoso.

El enrutamiento estático es una técnica útil para redes pequeñas o donde se necesita un control preciso sobre el tráfico. Sin embargo, en redes más grandes o dinámicas, el enrutamiento dinámico (como OSPF o EIGRP) es más adecuado debido a su capacidad para adaptarse automáticamente a los cambios en la topología de la red.

3.4.2. Enrutamiento dinámico

El ***enrutamiento dinámico*** es un método en el que los routers intercambian automáticamente información sobre las redes que conocen y calculan las mejores rutas para enviar paquetes de datos. A diferencia del enrutamiento estático, donde las rutas se configuran manualmente, el enrutamiento dinámico utiliza protocolos de enrutamiento para aprender y actualizar las rutas de manera automática. Esto es especialmente útil en redes grandes y complejas donde los cambios en la topología son frecuentes.

Ventajas del Enrutamiento Dinámico

a) ***Escalabilidad:*** Ideal para redes grandes y complejas.
b) ***Adaptabilidad:*** Los routers se adaptan automáticamente a cambios en la topología de la red (por ejemplo, caída de un enlace).
c) ***Redundancia:*** Permite el uso de múltiples rutas para llegar a un destino, mejorando la tolerancia a fallos.
d) ***Menor mantenimiento:*** No es necesario configurar manualmente las rutas cuando hay cambios en la red.

Desventajas del Enrutamiento Dinámico

a) ***Consumo de recursos:*** Los protocolos de enrutamiento dinámico consumen ancho de banda, memoria y CPU.

b) ***Complejidad:*** La configuración y el diagnóstico pueden ser más complejos que en el enrutamiento estático.
c) ***Seguridad:*** Si no se configura correctamente, puede ser vulnerable a ataques o filtrado de información.

Protocolos de Enrutamiento Dinámico

Existen dos tipos principales de protocolos de enrutamiento dinámico:

a) ***Protocolos de Gateway Interior (IGP):***
- Usados dentro de un sistema autónomo (AS).
- Ejemplos: RIP, EIGRP, OSPF.

b) ***Protocolos de Gateway Exterior (EGP):***
- Usados para intercambiar información entre sistemas autónomos.
- Ejemplo: BGP.

Protocolos Comunes de Enrutamiento Dinámico

a) ***RIP (Routing Information Protocol):***
- Protocolo de vector de distancia.
- Usa el número de saltos como métrica.
- Límite de 15 saltos.

b) ***EIGRP (Enhanced Interior Gateway Routing Protocol):***
- Protocolo avanzado de vector de distancia.
- Usa métricas compuestas (ancho de banda, retraso, carga, etc.).
- Propietario de Cisco.

c) ***OSPF (Open Shortest Path First):***
- Protocolo de estado de enlace.
- Usa el algoritmo Dijkstra para calcular rutas.
- Escalable y adecuado para redes grandes.

Configuración de Enrutamiento Dinámico en Cisco Packet Tracer

A continuación, se muestra cómo configurar enrutamiento dinámico usando los protocolos ***RIP***, ***EIGRP*** y ***OSPF*** en Cisco Packet Tracer.

1. Topología de Red

- Crea una topología con al menos dos routers y dos redes LAN.
- Conecta los routers mediante interfaces seriales o Ethernet.
- Asigna direcciones IP a las interfaces de los routers y a los dispositivos finales (PCs).

2. Configuración de Interfaces en los Routers

Accede a la CLI de cada router y configura las interfaces con las direcciones IP correspondientes.

```
Router> enable
Router# configure terminal
Router(config)# interface GigabitEthernet0/0
Router(config-if)# ip address 192.168.1.1 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)# exit
```

Repite este proceso para todas las interfaces de los routers.

3. Configuración de Enrutamiento Dinámico

a. Configuración de RIP

RIP es un protocolo simple y fácil de configurar.

- *En Router0:*

```
Router(config)# router rip
Router(config-router)# version 2
Router(config-router)# network 192.168.1.0
Router(config-router)# network 10.0.0.0
Router(config-router)# no auto-summary
Router(config-router)# exit
```

- *En Router1:*

```
Router(config)# router rip
Router(config-router)# version 2
Router(config-router)# network 192.168.2.0
Router(config-router)# network 10.0.0.0
Router(config-router)# no auto-summary
Router(config-router)# exit
```

b. Configuración de EIGRP

EIGRP es un protocolo avanzado y eficiente.

- *En Router0:*

```
Router(config)# router eigrp 1
Router(config-router)# network 192.168.1.0
Router(config-router)# network 10.0.0.0
Router(config-router)# no auto-summary
Router(config-router)# exit
```

- *En Router1:*

```
Router(config)# router eigrp 1
Router(config-router)# network 192.168.2.0
Router(config-router)# network 10.0.0.0
Router(config-router)# no auto-summary
Router(config-router)# exit
```

c. Configuración de OSPF

OSPF es un protocolo de estado de enlace muy escalable.

- *En Router0:*

```
Router(config)# router ospf 1
Router(config-router)# network 192.168.1.0 0.0.0.255 area 0
Router(config-router)# network 10.0.0.0 0.0.0.3 area 0
Router(config-router)# exit
```

- *En Router1:*

```
Router(config)# router ospf 1
Router(config-router)# network 192.168.2.0 0.0.0.255 area 0
Router(config-router)# network 10.0.0.0 0.0.0.3 area 0
Router(config-router)# exit
```

4. Verificación de la Configuración

Usa los siguientes comandos para verificar la configuración:

- *Mostrar tabla de enrutamiento:*

```
Router# show ip route
```

- *Mostrar vecinos (para EIGRP y OSPF):*
  - *EIGRP:*

```
Router# show ip eigrp neighbors
```

  - *OSPF:*

```
Router# show ip ospf neighbor
```

- *Mostrar información de RIP:*

```
Router# show ip rip database
```

5. Prueba de Conectividad

Usa el comando ping desde una PC para verificar la conectividad entre redes.

```
PC> ping 192.168.2.10
```

Si la configuración es correcta, deberías recibir respuestas exitosas.

Ejemplo Completo en Packet Tracer

Supongamos que tienes dos routers (Router0 y Router1) conectados entre sí, y cada router tiene una red LAN conectada.

- *Router0:*
  - *Interfaz GigabitEthernet0/0: 192.168.1.1/24 (conectada a la LAN1).*
  - *Interfaz Serial0/0/0: 10.0.0.1/30 (conectada a Router1).*
- *Router1:*
  - *Interfaz GigabitEthernet0/0: 192.168.2.1/24 (conectada a la LAN2).*
  - *Interfaz Serial0/0/0: 10.0.0.2/30 (conectada a Router0).*

Configuración de OSPF en Router0:

```
Router> enable
Router# configure terminal
Router(config)# interface GigabitEthernet0/0
Router(config-if)# ip address 192.168.1.1 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# interface Serial0/0/0
Router(config-if)# ip address 10.0.0.1 255.255.255.252
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# router ospf 1
Router(config-router)# network 192.168.1.0 0.0.0.255 area 0
Router(config-router)# network 10.0.0.0 0.0.0.3 area 0
Router(config-router)# exit
Router(config)# exit
Router# write memory
```

Configuración de OSPF en Router1:

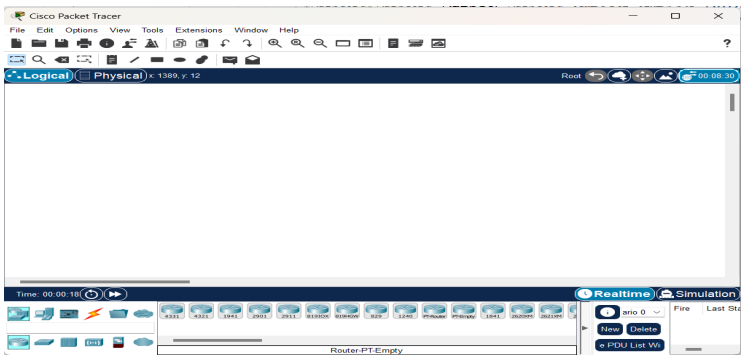
```
CopyRouter> enable
Router# configure terminal
Router(config)# interface GigabitEthernet0/0
Router(config-if)# ip address 192.168.2.1 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# interface Serial0/0/0
Router(config-if)# ip address 10.0.0.2 255.255.255.252
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# router ospf 1
Router(config-router)# network 192.168.2.0 0.0.0.255 area 0
Router(config-router)# network 10.0.0.0 0.0.0.3 area 0
Router(config-router)# exit
Router(config)# exit
Router# write memory
```

El enrutamiento dinámico es esencial para redes grandes y complejas, ya que permite a los routers adaptarse automáticamente a los cambios en la topología. Protocolos como RIP, EIGRP y OSPF ofrecen diferentes ventajas según el tamaño y los requisitos de la red. En Cisco Packet Tracer, puedes simular y probar estos protocolos para entender su funcionamiento y comportamiento.

3.4.3. Práctica en simulador: Uso básico del simulador Cisco Packet Tracer

Cisco Packet Tracer es un software propiedad de Cisco System Inc., diseñado para la simulación de redes basadas en los equipos de la citada compañía. Junto con los materiales didácticos diseñados con tal fin, es la principal herramienta de trabajo para pruebas y simulación de prácticas en los cursos de formación de Cisco System. Para su utilización se requiere la aceptación de la licencia de usuario y la autorización del propietario a través de las entidades denominadas "academias" que están autorizadas para la impartición de los citados cursos.

a. El entorno de trabajo



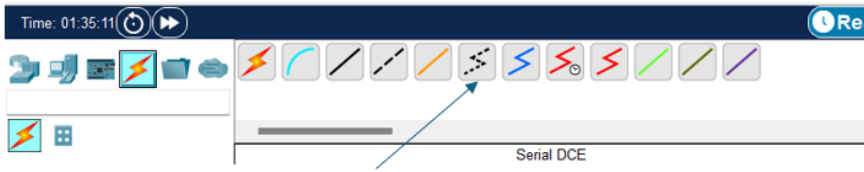
En el espacio de trabajo de Packet Tracer se encuentran diferentes zonas:

- Zona de menús. Es el área donde se encuentran las opciones típicas de todos los programas para la gestión y la configuración del software.
- Selector de presentación. Permite cambiar entre esquema lógico y esquema físico a la hora de presentar los dispositivos. Lo habitual es trabajar con el esquema lógico.
- Espacio de trabajo. Es la zona donde se situarán los dispositivos que conforman la red.
- Barra de herramientas. Proporciona herramientas para seleccionar dispositivos, mover el espacio de trabajo, analizar parámetros específicos de los dis positivos (la lupa), generar unidades de datos de protocolo (PDU) simples o complejas.
- Selector de modos de operación. Para cambiar entre el modo de Tiempo real o el modo Simulación.
- Selector de escenarios. Sirve para realizar distintos análisis sobre una misma red.
- Área de estado del escenario. Muestra las UDP que han intervenido en el análisis realizado, ya sea en tiempo real o en modo simulación.
- Área de dispositivos. Es la zona que permite seleccionar los dispositivos que van a ser incluidos en el espacio de trabajo, así como la conexión entre estos.

b. Creación de una topología de red

El modo de operación con Packet Tracer es muy sencillo ya que se trata de un programa muy intuitivo. La primera operación consistirá en seleccionar los dispositivos que forman la red, para ello se seleccionará el grupo correspondiente: de izquierda a derecha y de arriba hacia abajo: Ruteadores, Switches, Hubs. Dispositivos inalámbricos, Conexiones, Dispositivos finales, Emulación de WAN, Dispositivos personalizados y Conexión multiusuario.

El conexionado de los distintos equipos se puede realizar eligiendo personalmente el tipo de conexión o mediante la herramienta de conexionado automático. En cualquier caso, hay que señalar sobre los dispositivos a conexionar y, si el caso lo requiere, se ofrecerá la posibilidad de elegir el tipo de interface.



Diferentes tipos de cables para conectar los diferentes dispositivos de red

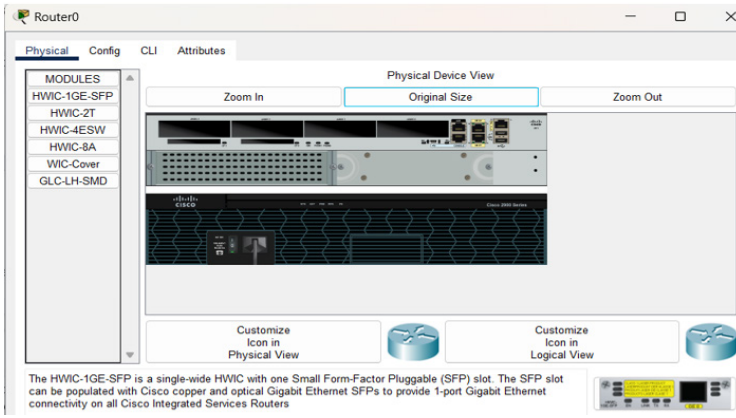
c. Configuración de los dispositivos

Cuando los dispositivos se encuentran sobre el escenario, al situar el cursor sobre ellos aparecerá un recuadro con la información acerca de su configuración a nivel de red.

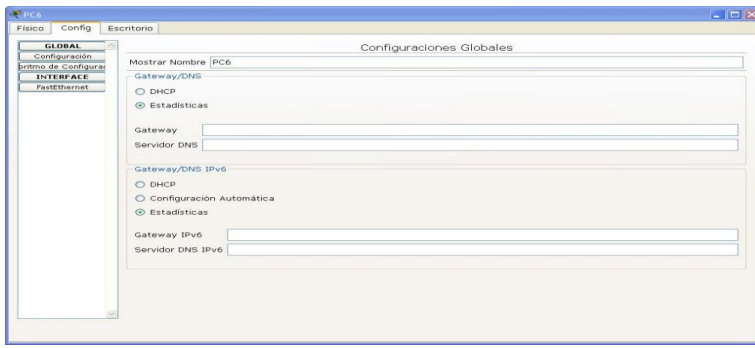
En cada una de las conexiones aparecerá un indicador de conectividad a nivel físico que podrá estar rojo (no hay conectividad), naranja (la interface está en proceso de inicio) o verde (la interfaz está operativa). La configuración de los parámetros de red será un proceso que deberá realizar el usuario.

Al marcar un dispositivo se abrirá la ventana del dispositivo en la que aparecen tres pestañas seleccionables:

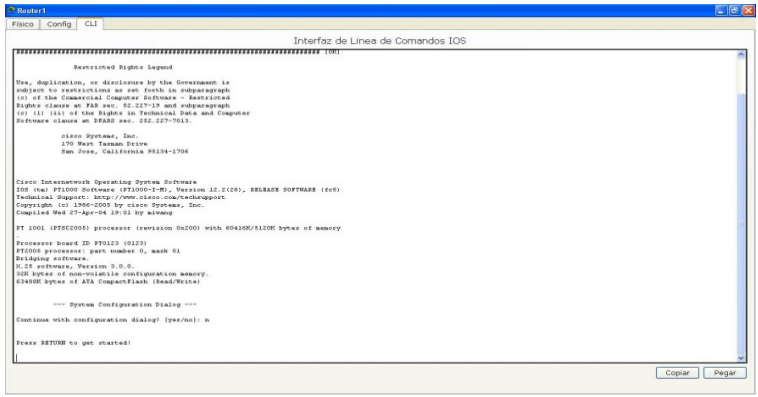
- ***Físico.*** Muestra una representación del equipo físico y los módulos de ampliación y/o configuración disponible para el citado equipo, de manera que es posible quitar o poner módulos a voluntad del operador. Para hacer esta operación será necesario primero apagar el dispositivo.



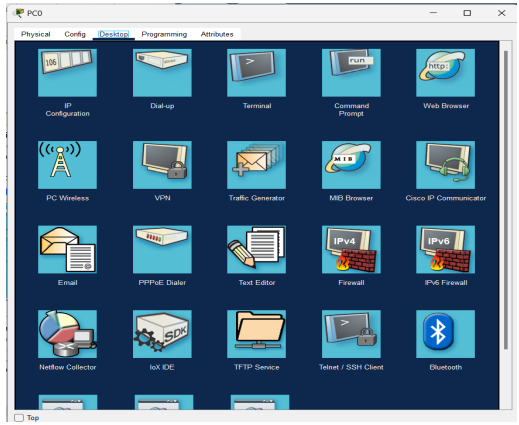
- ***Config.*** Ofrece las opciones de configuración del dispositivo a nivel general (Global), de enrutamiento en el caso de routers y de las interfaces instaladas de manera individual (Interfaz).



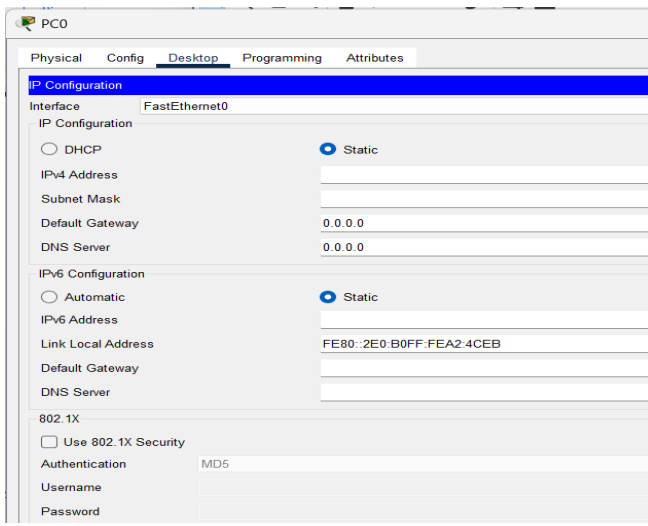
- ***CLI.*** Sólo disponible en routers y switches. Sirve para programar el dispositivo en modo comandos (CLI, Command Line Interface, Interfaz de línea de comandos) tal como se haría a través de la consola en un dispositivo real.



- ***Escritorio.*** Sólo disponible en los hosts. Ofrece distintas aplicaciones (simuladas) para operar sobre el dispositivo, según la configuración de las interfaces que tenga instaladas: IP Configuración, Dial-up, Terminal, Símbolo del sistema, Navegador Web, Configuración inalámbrica, VPN, Generador de tráfico, Navegador MIB, Comunicaciones Cisco, Correo, Marcador PPPoE, Editor de texto.



La comprobación de la correcta configuración de los dispositivos, una vez que todos los indicadores de conexión física están en color verde, se puede realizar de forma rápida situando el cursor en cada uno de los dispositivos y analizando el resumen de la configuración que se muestra en una ventana emergente. Damos un clic en "IP Configuration" y se coloca IP, mascara, Gateway del PC.

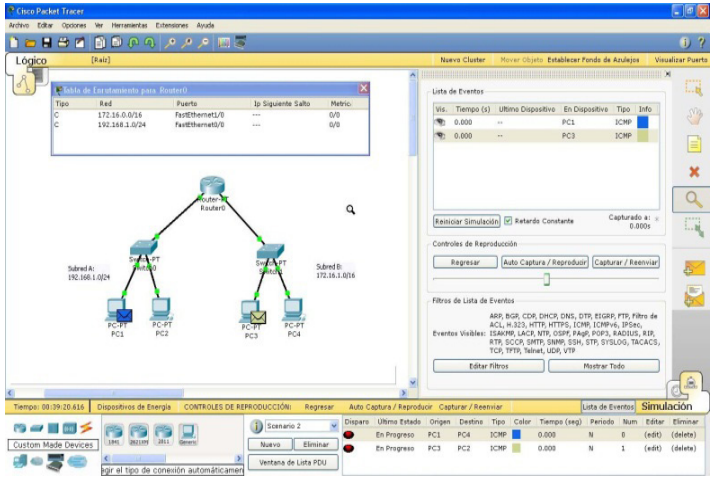


d. Comprobaciones básicas de funcionamiento

Las primeras comprobaciones tienen que ver con la conectividad IP de los dispositivos integrados en una red. En modo Tiempo real el proceso puede llevarse a cabo mediante el envío de PDUs simple

entre los equipos de una red y entre estos y el Gateway de la propia red, lo que sería equivalente a la utilización del comando ping. La utilización de distintos escenarios permite ir agrupando las pruebas de análisis. Si se utiliza el modo Simulación en el área de trabajo podrá comprobarse el movimiento de las PDUs representadas mediante sobres de distintos colores, lo que permite hacer un seguimiento más detallado del tráfico entre los dispositivos en la ventana de Lista de eventos.

Además, en el modo Simulación, desde la Lista de eventos que se despliega en la parte derecha del área de trabajo facilita ese seguimiento y activando el ratón sobre los rectángulos coloreados en esta lista se accede a la Ventana de información de la PDU según el dispositivo al que corresponda esa PDU. En esta ventana se puede analizar detalladamente todos los campos de bytes que conforman la citada PDU los valores que contienen.



3.5. Calidad de servicio (QoS)

La Calidad de Servicio (QoS, por sus siglas en inglés, Quality of Service) es un concepto fundamental en redes de computadoras que se refiere a la capacidad de garantizar un rendimiento óptimo para aplicaciones críticas o sensibles al tiempo. En un entorno donde múltiples tipos de tráfico (voz, video, datos, etc.) compiten por los mismos recursos de red, el QoS permite priorizar y gestionar el tráfico para asegurar que las aplicaciones más importantes funcionen sin interrupciones. Esto es especialmente relevante en redes con ancho de banda limitado o en situaciones donde la congestión puede afectar negativamente la experiencia del usuario.

Importancia del QoS

En una red sin QoS, todos los paquetes de datos son tratados por igual, lo que puede llevar a problemas como latencia alta, pérdida de paquetes o jitter. Estos problemas son particularmente críticos en aplicaciones en tiempo real, como las llamadas de voz sobre IP (VoIP) o las videoconferencias, donde incluso un pequeño retraso puede degradar significativamente la calidad de la comunicación. Por ejemplo, en una llamada de VoIP, una latencia alta puede hacer que las conversaciones se vuelvan incoherentes, mientras que la pérdida de paquetes puede causar cortes en el audio. El QoS aborda estos problemas al priorizar el tráfico crítico y garantizar que reciba los recursos necesarios.

Métricas Clave del QoS

Para entender cómo se mide y se garantiza la calidad del servicio, es importante conocer las métricas clave que definen el rendimiento de una red:

1. ***Ancho de Banda:*** Es la cantidad de datos que se pueden transmitir a través de una red en un período de tiempo determinado. Se mide en bits por segundo (bps), kilobits por segundo (kbps), megabits por segundo (Mbps) o gigabits por segundo (Gbps). Un ancho de banda insuficiente puede causar congestión y retrasos.
2. ***Latencia:*** Es el tiempo que tarda un paquete en viajar desde el origen hasta el destino. Se mide en milisegundos (ms). Una latencia alta puede ser problemática para aplicaciones en tiempo real, como VoIP o juegos en línea.
3. ***Jitter:*** Es la variación en la latencia de los paquetes. Un jitter alto puede causar problemas en aplicaciones que requieren una transmisión constante, como el streaming de video o las llamadas de voz.
4. ***Pérdida de Paquetes:*** Ocurre cuando uno o más paquetes de datos no llegan a su destino. Esto puede ser causado por congestión en la red o por errores en la transmisión. La pérdida de paquetes puede afectar negativamente la calidad de las comunicaciones en tiempo real.

Técnicas de QoS

Para garantizar una calidad de servicio adecuada, se utilizan diversas técnicas que permiten gestionar el tráfico de manera eficiente. Estas técnicas se pueden clasificar en varias categorías:

1. ***Clasificación y marcado:*** La clasificación consiste en identificar el tipo de tráfico (voz, video, datos, etc.) y asignarle una prioridad. El marcado es el proceso de etiquetar los paquetes con información que indica su prioridad. Por ejemplo, en redes IP, se puede utilizar el campo DSCP (Differentiated Services Code Point) en el encabezado del paquete para indicar su nivel de prioridad.
2. ***Colas prioritarias:*** Las colas prioritarias permiten gestionar el tráfico en función de su importancia. Se crean colas separadas para diferentes tipos de tráfico, y se asigna una prioridad a cada cola. Por ejemplo, el tráfico de VoIP puede colocarse en una cola de alta prioridad, mientras que el tráfico de correo electrónico puede colocarse en una cola de baja prioridad.
3. ***Limitación de Ancho de Banda (Traffic Shaping):*** Esta técnica consiste en controlar la tasa de transmisión de datos para evitar la congestión en la red. Por ejemplo, se puede limitar el ancho de banda disponible para aplicaciones que consumen muchos recursos, como las descargas P2P, para garantizar que las aplicaciones críticas tengan suficiente ancho de banda.
4. ***Compresión de cabeceras:*** La compresión de cabeceras reduce el tamaño de las cabeceras de los paquetes, lo que permite optimizar el uso del ancho de banda. Esta técnica es especialmente útil en aplicaciones como VoIP, donde los paquetes son pequeños y las cabeceras representan una proporción significativa del tráfico total.
5. ***Fragmentación y entrelazado:*** La fragmentación consiste en dividir paquetes grandes en fragmentos más pequeños, lo que reduce la latencia para aplicaciones en tiempo real. El entrelazado permite intercalar paquetes de diferentes tipos de tráfico, lo que ayuda a garantizar que los paquetes críticos no se retrasen debido a paquetes grandes.

3.5.1. Importancia del QoS en el Diseño y la Gestión de Redes

La Calidad de Servicio (QoS) es un elemento crítico en el diseño y la gestión de redes modernas, especialmente en un mundo donde las aplicaciones y servicios dependen cada vez más de una conectividad rápida, confiable y eficiente. La implementación de QoS no solo mejora el rendimiento de la red, sino que también garantiza que las aplicaciones críticas funcionen sin interrupciones, incluso en entornos con alta demanda de recursos. A continuación, se explora en detalle la importancia del QoS en el diseño y la gestión de redes, abordando sus beneficios, desafíos y aplicaciones prácticas.

a. Garantizar el Rendimiento de Aplicaciones Críticas

En una red, no todo el tráfico es igual. Algunas aplicaciones, como las llamadas de voz sobre IP (VoIP), las videoconferencias, el streaming de video y los juegos en línea, son extremadamente sensibles a la latencia, el jitter y la pérdida de paquetes. Si estos tipos de tráfico no se priorizan, pueden verse gravemente afectados por la congestión de la red, lo que resulta en una experiencia de usuario deficiente. Por ejemplo, en una llamada de VoIP, una latencia alta puede hacer que las conversaciones se vuelvan incoherentes, mientras que la pérdida de paquetes puede causar cortes en el audio.

El QoS permite priorizar este tipo de tráfico crítico, asegurando que reciba los recursos necesarios para funcionar correctamente. Esto es especialmente importante en entornos empresariales, donde las comunicaciones en tiempo real son esenciales para la productividad y la colaboración.

b. Optimización del Uso del Ancho de Banda

El ancho de banda es un recurso finito, y en muchas redes, especialmente en aquellas con limitaciones de infraestructura, puede ser un cuello de botella. Sin QoS, aplicaciones que consumen mucho ancho de banda, como las descargas de archivos grandes o el tráfico P2P, pueden monopolizar los recursos de la red, dejando poco ancho de banda disponible para aplicaciones más importantes.

El QoS permite gestionar el ancho de banda de manera eficiente, asignando prioridades a diferentes tipos de tráfico. Por ejemplo, se puede limitar el ancho de banda disponible para aplicaciones no críticas, como las descargas, mientras se garantiza que aplicaciones críticas, como las videoconferencias, tengan suficiente ancho de banda para funcionar sin problemas.

c. Reducción de la Congestión de la Red

La congestión de la red ocurre cuando la demanda de recursos supera la capacidad disponible. Esto puede resultar en una degradación del rendimiento de la red, incluyendo aumentos en la latencia, la pérdida de paquetes y el jitter. La congestión es particularmente problemática en redes con tráfico mixto, donde coexisten aplicaciones en tiempo real y no críticas.

El QoS ayuda a prevenir la congestión mediante técnicas como la limitación de ancho de banda (traffic shaping) y la gestión de colas. Estas técnicas permiten controlar la tasa de transmisión de datos y priorizar el tráfico crítico, reduciendo así la probabilidad de congestión y mejorando el rendimiento general de la red.

d. Mejora de la Experiencia del Usuario

En última instancia, el objetivo del QoS es mejorar la experiencia del usuario. En un entorno donde los usuarios dependen de aplicaciones en tiempo real y servicios basados en la nube, cualquier interrupción o degradación del rendimiento puede tener un impacto significativo en la satisfacción del usuario.

Por ejemplo, en una empresa que utiliza VoIP para comunicaciones internas, un problema de latencia o pérdida de paquetes puede afectar negativamente la productividad y la eficiencia. Al implementar QoS, se puede garantizar que estas aplicaciones funcionen de manera óptima, lo que resulta en una experiencia de usuario más fluida y satisfactoria.

e. Soporte para Redes Convergentes

Las redes modernas son convergentes, lo que significa que transportan múltiples tipos de tráfico (voz, video, datos) sobre la misma infraestructura. Esto presenta un desafío, ya que cada tipo de tráfico tiene requisitos diferentes en términos de ancho de banda, latencia y pérdida de paquetes.

El QoS es esencial para gestionar estas redes convergentes, ya que permite priorizar el tráfico crítico y garantizar que cada tipo de tráfico reciba los recursos necesarios. Por ejemplo, en una red que transporta tanto VoIP como tráfico de datos, el QoS puede garantizar que las llamadas de voz tengan prioridad sobre el tráfico de datos menos crítico.

f. Cumplimiento de Acuerdos de Nivel de Servicio (SLA)

En entornos empresariales y de proveedores de servicios, los Acuerdos de Nivel de Servicio (SLA) son contratos que garantizan un nivel mínimo de rendimiento y disponibilidad de la red. El incumplimiento de estos acuerdos puede resultar en penalizaciones económicas y daños a la reputación.

El QoS es una herramienta clave para cumplir con los SLA, ya que permite garantizar que los niveles de rendimiento acordados se mantengan incluso en condiciones de alta demanda. Por ejemplo, un proveedor de servicios puede utilizar QoS para garantizar que sus clientes empresariales tengan un ancho de banda mínimo disponible para sus aplicaciones críticas.

g. Escalabilidad y Futuro de las Redes

A medida que las redes crecen y evolucionan, la demanda de recursos también aumenta. Nuevas aplicaciones y servicios, como el Internet de las Cosas (IoT), la realidad virtual (VR) y la inteligencia artificial (IA), requieren un rendimiento de red cada vez más robusto y confiable.

El QoS es esencial para garantizar que las redes puedan escalar de manera efectiva y soportar estas nuevas demandas. Al implementar QoS desde el diseño inicial de la red, las organizaciones pueden asegurarse de que su infraestructura esté preparada para el futuro y pueda adaptarse a las necesidades cambiantes.

La importancia del QoS en el diseño y la gestión de redes no puede subestimarse. En un mundo donde las aplicaciones críticas y los servicios en tiempo real dependen de una conectividad rápida y confiable, el QoS es esencial para garantizar un rendimiento óptimo, evitar la congestión y mejorar la experiencia del usuario. Además, el QoS permite a las organizaciones cumplir con los SLA, gestionar el ancho de banda de manera eficiente y preparar sus redes para el futuro. En resumen, el QoS no es solo una herramienta técnica, sino un componente estratégico que contribuye al éxito y la eficiencia de las redes modernas.

Ejercicios Resueltos

Ejercicio 1: Cálculo de Ancho de Banda necesario

Supongamos que tienes una red con los siguientes requisitos:

- 10 llamadas VoIP simultáneas, cada una usando 100 kbps.
- Tráfico de video que requiere 2 Mbps.
- Tráfico de datos que requiere 5 Mbps.

Pregunta: ¿Cuál es el ancho de banda total necesario para garantizar QoS?

Solución:

a. Ancho de banda para VoIP:
   10×100 kbps=1000 kbps=1 Mbps
b. Ancho de banda para video: 2 Mbps
c. Ancho de banda para datos: 5 Mbps

Total: 1+2+5=8 Mbps

Ejercicio 2: Priorización de tráfico

En una red, se tienen los siguientes tipos de tráfico:

- VoIP (alta prioridad).
- Videoconferencia (media prioridad).
- Navegación web (baja prioridad).

Pregunta: ¿Cómo configurarías las colas de prioridad en un router para garantizar QoS?

Solución:

a. Crear tres colas:
   - Cola 1: Prioridad alta para VoIP.
   - Cola 2: Prioridad media para videoconferencia.
   - Cola 3: Prioridad baja para navegación web.
b. Asignar ancho de banda:
   - Cola 1: 30% del ancho de banda.
   - Cola 2: 50% del ancho de banda.
   - Cola 3: 20% del ancho de banda.

c. Configurar el router para que siempre procese primero los paquetes de la Cola 1, luego los de la Cola 2 y finalmente los de la Cola 3.

Ejercicio 3: Cálculo de Latencia

Un paquete tarda 50 ms en viajar desde el origen hasta el destino. Si el jitter es de 10ms, ¿cuál es el rango de latencia posible?

Solución:

- Latencia mínima: 50ms-10ms=40ms
- Latencia máxima: 50ms+10ms=60ms

Respuesta: El rango de latencia es de 40 ms a 60 ms.

3.6. Protocolos de aplicación

Los ***protocolos de aplicación*** son un conjunto de reglas y estándares que permiten la comunicación entre aplicaciones o software en redes de datos. Estos protocolos definen cómo los dispositivos intercambian información, asegurando que los datos se transmitan de manera eficiente, segura y confiable. A continuación, te explico de forma clara y detallada todo lo que necesitas saber sobre ellos.

Los protocolos de aplicación son parte de la capa más alta del modelo OSI (Capa 7) y del modelo TCP/IP (Capa de Aplicación). Su función principal es permitir que las aplicaciones en diferentes dispositivos se comuniquen entre sí, independientemente del hardware o sistema operativo que utilicen.

Ejemplos comunes incluyen:

- ***HTTP/HTTPS:*** Para navegación web.
- ***FTP:*** Para transferencia de archivos.
- ***SMTP/IMAP/POP3:*** Para correo electrónico.
- ***DNS:*** Para resolver nombres de dominio a direcciones IP.
- ***SSH:*** Para conexiones seguras a servidores.

Los protocolos de aplicación pueden tener las siguientes características:

- ***Interoperabilidad:*** Permiten que aplicaciones de diferentes fabricantes o plataformas se comuniquen.
- ***Estandarización:*** Siguen normas internacionales para garantizar la compatibilidad.
- ***Seguridad:*** Muchos protocolos modernos incluyen cifrado (como HTTPS o SSH) para proteger los datos.
- ***Eficiencia:*** Optimizan el uso de recursos de red para evitar congestiones.

Los protocolos de aplicación trabajan en conjunto con otras capas de red (como transporte, red y enlace) para enviar y recibir datos. Por ejemplo:

- Un usuario escribe una URL en su navegador (aplicación).
- El protocolo ***HTTP*** envía una solicitud al servidor web.
- El servidor responde con la página web solicitada.
- El navegador interpreta y muestra la información.

Los protocolos de aplicación se clasifican según su función:

a) ***Protocolos para la web***
- ***HTTP (HyperText Transfer Protocol):*** Transfiere páginas web desde servidores a navegadores.
- ***HTTPS (HTTP Secure):*** Versión segura de HTTP con cifrado SSL/TLS.

b) ***Protocolos para correo electrónico***
- ***SMTP (Simple Mail Transfer Protocol):*** Envía correos electrónicos.
- ***IMAP (Internet Message Access Protocol):*** Permite acceder y gestionar correos en el servidor.
- ***POP3 (Post Office Protocol):*** Descarga correos al dispositivo local.

c) ***Protocolos para transferencia de archivos***
- ***FTP (File Transfer Protocol):*** Transfiere archivos entre cliente y servidor.
- ***SFTP (SSH File Transfer Protocol):*** Versión segura de FTP con cifrado SSH.
- d) ***Protocolos para resolución de nombres***
- ***DNS (Domain Name System):*** Convierte nombres de dominio (como google.com) en direcciones IP.

e) ***Protocolos para acceso remoto***
- ***SSH (Secure Shell):*** Permite conexiones seguras a servidores.
- ***Telnet:*** Similar a SSH, pero sin cifrado (menos seguro).

f) ***Protocolos para voz y video***
- ***SIP (Session Initiation Protocol):*** Gestiona sesiones de voz y video (usado en VoIP).
- ***RTP (Real-time Transport Protocol):*** Transmite audio y video en tiempo real.

Importancia de los protocolos de aplicación:

- Facilitan la comunicación global a través de Internet.
- Permiten el desarrollo de aplicaciones multiplataforma.
- Garantizan la integridad y seguridad de los datos.
- Establecen estándares para la interoperabilidad entre dispositivos.

Ejemplos

- ***Navegación web:*** Cuando visitas un sitio web, tu navegador usa HTTP/HTTPS para solicitar y recibir la página.
- ***Envío de correos:*** Al enviar un email, tu cliente de correo usa SMTP para enviar el mensaje al servidor.
- ***Descarga de archivos:*** Al usar FTP, puedes subir o bajar archivos de un servidor remoto.

Los protocolos de aplicación son esenciales para el funcionamiento de las redes de datos y las aplicaciones que usamos diariamente. Sin ellos, la comunicación entre dispositivos y servicios en Internet no sería posible.

3.7 Casos de estudio prácticos en simulador

CASO 1

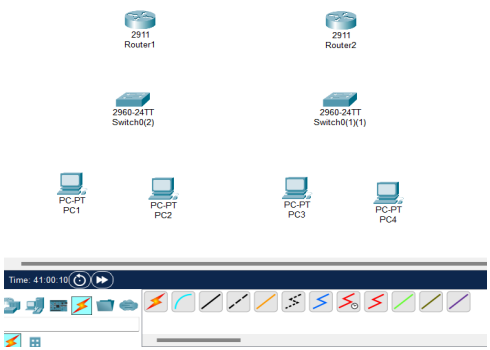
Configurar una red LAN con dos routers, dos switches y cuatro computadoras en Cisco Packet Tracer es un ejercicio común para entender cómo funcionan las redes. A continuación, te guiaré paso a paso para realizar esta simulación.

Materiales necesarios:

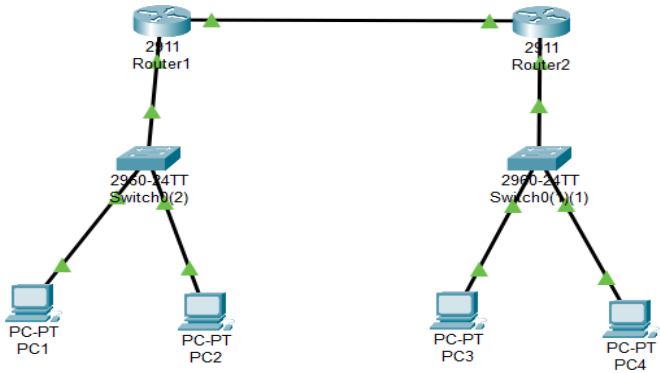
- 2 Routers (pueden ser del tipo ***Router-2911***).
- 2 switches (pueden ser del tipo ***Switch-2960).***
- 4 computadoras.
- Cables:
  - ***Cable de consola*** (para configurar los routers).
  - ***Cable cruzado (Copper Cross-Over)*** para conectar routers a switch.
  - ***Cable directo (Copper Straight-Through)*** para conectar switches a computadoras.

Paso 1: Diseñar la topología

a. Abre Cisco Packet Tracer.
b. Arrastra los siguientes dispositivos al área de trabajo:
   - 2 Routers.
   - 2 switches.
   - 4 computadoras.



c. Conecta los dispositivos de la siguiente manera:
- Conecta el Router1 al Switch1 usando un cable cruzado.
- Conecta el Router2 al Switch2 usando un cable cruzado.
- Conecta PC1 y PC2 al Switch1 usando cables directos.
- Conecta PC3 y PC4 al Switch2 usando cables directos.



Paso 2: Configurar las interfaces de los routers

a. Haz clic en el ***Router1*** y selecciona la pestaña ***«Config».***

b. Configura la interfaz ***GigabitEthernet0/0:***
- IP Address: ***192.168.1.1***
- Subnet Mask: ***255.255.255.0***
- Activa la interfaz (enciéndela).

c. Repite el proceso para el ***Router2:***
- Configura la interfaz ***GigabitEthernet0/0:***
  - IP Address: ***192.168.2.1***
  - Subnet Mask: ***255.255.255.0***
  - Activa la interfaz.

Paso 3: Configurar las computadoras

a. Haz clic en ***PC1*** y selecciona la pestaña ***«Desktop»*** > ***«IP Configuration».***
- IP Address: ***192.168.1.10***
- Subnet Mask: ***255.255.255.0***
- Default Gateway: ***192.168.1.1*** (IP del Router1).

b. Configura ***PC2***:
- IP Address: ***192.168.1.11***
- Subnet Mask: ***255.255.255.0***
- Default Gateway: ***192.168.1.1.***

c. Configura ***PC3***:
- IP Address: ***192.168.2.10***
- Subnet Mask: ***255.255.255.0***
- Default Gateway: ***192.168.2.1*** (IP del Router2).

d. Configura ***PC4***:
- IP Address: ***192.168.2.11***
- Subnet Mask: ***255.255.255.0***
- Default Gateway: ***192.168.2.1.***

Paso 4: Configurar el enrutamiento entre routers

Para que las computadoras de ambas redes puedan comunicarse, debes configurar el enrutamiento entre los routers.

a. Haz clic en el ***Router1*** y selecciona la pestaña ***«CLI»*** (Command Line Interface).
b. Configura una ruta estática para llegar a la red del ***Router2***:

```
enable
configure terminal
ip route 192.168.2.0 255.255.255.0 192.168.1.2
exit
```

(Aquí, ***192.168.1.2*** es la IP de la interfaz del Router1 que se conectará al Router2).

a. Haz clic en el Router2 y selecciona la pestaña «CLI».
b. Configura una ruta estática para llegar a la red del Router1:
c. Haz clic en el Router2 y selecciona la pestaña "CLI".
d. Configura una ruta estática para llegar a la red del Router1:

```
enable
configure terminal
ip route 192.168.1.0 255.255.255.0 192.168.2.2
exit
```

(Aquí, ***192.168.2.2*** es la IP de la interfaz del Router2 que se conectará al Router1).

Paso 5: Verificar la conectividad

a. En ***PC1***, abre la pestaña ***"Desktop"*** > ***«Command Prompt».***
b. Realiza un ping a ***PC3*** (192.168.2.10):

```
ping 192.168.2.10
```

Si la configuración es correcta, deberías recibir respuestas exitosas.

c. Repite el proceso desde ***PC3*** hacia ***PC1*** para verificar la conectividad en ambos sentidos.

Paso 6: Guardar la configuración

a. En cada router, guarda la configuración para que no se pierda al reiniciar:

```
enable
write memory
```

Resumen de la configuración:

- ***Router1:***
    - Interfaz GigabitEthernet0/0: 192.168.1.1/24
    - Ruta estática: ip route 192.168.2.0 255.255.255.0 192.168.1.2
- ***Router2:***
    - Interfaz GigabitEthernet0/0: 192.168.2.1/24
    - Ruta estática: ip route 192.168.1.0 255.255.255.0 192.168.2.2
- ***PC1:*** 192.168.1.10/24, Gateway: 192.168.1.1
- ***PC2:*** 192.168.1.11/24, Gateway: 192.168.1.1
- ***PC3:*** 192.168.2.10/24, Gateway: 192.168.2.1
- ***PC4:*** 192.168.2.11/24, Gateway: 192.168.2.1

Consejos adicionales:

- Si no hay conectividad, verifica las IPs, las máscaras de subred y las rutas estáticas.
- Usa el comando `show ip route` en los routers para verificar las rutas configuradas.
- Asegúrate de que todas las interfaces estén activas (`no shutdown`).

CASO 2

Configurar una red LAN con dos routers, dos switches por router y dos computadoras por switch en Cisco Packet Tracer es un ejercicio un poco más complejo, pero te ayudará a entender mejor el enrutamiento y la segmentación de redes.

Materiales necesarios:

- 2 Routers (pueden ser del tipo ***Router-PT***).
- 4 switches (pueden ser del tipo ***Switch-PT***).
- 8 computadoras (pueden ser del tipo ***PC-PT***).
- Cables:
    - ***Cable de consola*** (para configurar los routers).
    - ***Cable cruzado (Copper Cross-Over)*** para conectar routers a switch.
    - ***Cable directo (Copper Straight-Through)*** para conectar switches a computadoras.

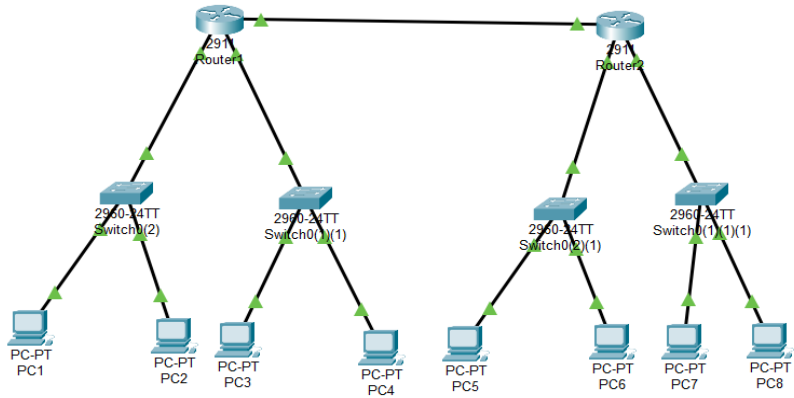
Paso 1: Diseñar la topología

a. Abre Cisco Packet Tracer.

b. Arrastra los siguientes dispositivos al área de trabajo:
    - 2 Routers.
    - 4 switches.
    - 8 computadoras.

c. Conecta los dispositivos de la siguiente manera:
    - Conecta el ***Router1*** al ***Switch1*** y ***Switch2*** usando ***cables cruzados.***
    - Conecta el ***Router2*** al ***Switch3*** y ***Switch4*** usando ***cables cruzados.***

- Conecta ***PC1*** y ***PC2*** al ***Switch1*** usando ***cables directos***.
- Conecta ***PC3*** y ***PC4*** al ***Switch2*** usando ***cables directos.***
- Conecta ***PC5*** y ***PC6*** al ***Switch3*** usando ***cables directos.***
- Conecta ***PC7*** y ***PC8*** al ***Switch4*** usando ***cables directos.***



Paso 2: Configurar las interfaces de los routers

a. Haz clic en el ***Router1*** y selecciona la pestaña ***«Config"***.

b. Configura las interfaces:

- ***GigabitEthernet0/0*** (conectada a Switch1):
  - IP Address: ***192.168.1.1***
  - Subnet Mask: ***255.255.255.0***
  - Activa la interfaz (enciéndela).
- ***GigabitEthernet0/1*** (conectada a Switch2):
  - IP Address: ***192.168.2.1***
  - Subnet Mask: ***255.255.255.0***
  - Activa la interfaz.

c. Repite el proceso para el ***Router2:***

- ***GigabitEthernet0/0*** (conectada a Switch3):
  - IP Address: ***192.168.3.1***
  - Subnet Mask: ***255.255.255.0***
  - Activa la interfaz.
- ***GigabitEthernet0/1*** (conectada a Switch4):
  - IP Address: ***192.168.4.1***
  - Subnet Mask: ***255.255.255.0***
  - Activa la interfaz.

Paso 3: Configurar las computadoras

a. Configura las IPs de las computadoras conectadas al ***Router1:***

- ***PC1:***
  - IP Address: ***192.168.1.10***
  - Subnet Mask: ***255.255.255.0***
  - Default Gateway: ***192.168.1.1.***

- ***PC2:***
  - IP Address: ***192.168.1.11***
  - Subnet Mask: ***255.255.255.0***
  - Default Gateway: ***192.168.1.1.***
- ***PC3:***
  - IP Address: ***192.168.2.10***
  - Subnet Mask: ***255.255.255.0***
  - Default Gateway: ***192.168.2.1.***
- ***PC4:***
  - IP Address: ***192.168.2.11***
  - Subnet Mask: ***255.255.255.0***
  - Default Gateway: ***192.168.2.1***.

b. Configura las IPs de las computadoras conectadas al ***Router2:***

- ***PC5***:
  - IP Address: ***192.168.3.10***
  - Subnet Mask: ***255.255.255.0***
  - Default Gateway: ***192.168.3.1***.
- ***PC6:***
  - IP Address: ***192.168.3.11***
  - Subnet Mask: ***255.255.255.0***
  - Default Gateway: ***192.168.3.1***.
- ***PC7***:
  - IP Address: ***192.168.4.10***
  - Subnet Mask: ***255.255.255.0***
  - Default Gateway: ***192.168.4.1***.
- ***PC8***:
  - IP Address: ***192.168.4.11***
  - Subnet Mask: ***255.255.255.0***
  - Default Gateway: ***192.168.4.1***.

Paso 4: Configurar el enrutamiento entre routers

Para que las computadoras de todas las redes puedan comunicarse, debes configurar el enrutamiento entre los routers.

a. Conecta el Router1 y el Router2 usando un cable cruzado en las interfaces disponibles (por ejemplo, GigabitEthernet0/2 en ambos routers).

b. Configura las interfaces de conexión entre routers:

- ***En el Router1:***
  - IP Address: 10.0.0.1
  - Subnet Mask: 255.255.255.252
  - Activa la interfaz.
- ***En el Router2:***
  - IP Address: 10.0.0.2
  - Subnet Mask: 255.255.255.252

- Activa la interfaz.

c. Configura rutas estáticas en ambos routers:

- *En el Router1:*

```
enable
configure terminal
ip route 192.168.3.0 255.255.255.0 10.0.0.2
ip route 192.168.4.0 255.255.255.0 10.0.0.2
exit
```

- *En el Router2:*

```
enable
configure terminal
ip route 192.168.1.0 255.255.255.0 10.0.0.1
ip route 192.168.2.0 255.255.255.0 10.0.0.1
exit
```

Paso 5: Verificar la conectividad

a. En PC1, abre la pestaña "Desktop" > «Command Prompt».
b. Realiza un ping a PC5 (192.168.3.10):

```
ping 192.168.3.10
```

Si la configuración es correcta, deberías recibir respuestas exitosas.

a. Repite el proceso desde PC5 hacia PC1 para verificar la conectividad en ambos sentidos.

Paso 6: Guardar la configuración

a. En cada router, guarda la configuración para que no se pierda al reiniciar:

```
enable
write memory
```

Resumen de la configuración:

- *Router1:*
  - Interfaz GigabitEthernet0/0: 192.168.1.1/24
  - Interfaz GigabitEthernet0/1: 192.168.2.1/24
  - Interfaz GigabitEthernet0/2: 10.0.0.1/30
  - Rutas estáticas:
    - ip route 192.168.3.0 255.255.255.0 10.0.0.2
    - ip route 192.168.4.0 255.255.255.0 10.0.0.2
- *Router2:*
  - Interfaz GigabitEthernet0/0: 192.168.3.1/24
  - Interfaz GigabitEthernet0/1: 192.168.4.1/24
  - Interfaz GigabitEthernet0/2: 10.0.0.2/30

- ***Rutas estáticas:***
  - ip route 192.168.1.0 255.255.255.0 10.0.0.1
  - ip route 192.168.2.0 255.255.255.0 10.0.0.1

Consejos adicionales:

- Trabajar por bloques, es decir de router en router, de esa forma podemos darnos cuenta si hay algún error desde el inicio.
- Si no hay conectividad, verifica las IPs, las máscaras de subred y las rutas estáticas.
- Usa el comando `show ip route` en los routers para verificar las rutas configuradas.
- Asegúrate de que todas las interfaces estén activas (`no shutdown`).

CASO 3

Configurar una red LAN con dos routers, dos switches por router, dos computadoras por switch, un servidor DHCP y una sola IP con subneteo en Cisco Packet Tracer es un ejercicio avanzado que te permitirá entender cómo segmentar una red y configurar servicios como DHCP. A continuación, te guiaré paso a paso para realizar esta simulación.

Materiales necesarios:

- 2 Routers
- 4 switches
- 8 computadoras
- 1 servidor
- Cables:
  - ***Cable de consola*** (para configurar los routers).
  - ***Cable cruzado (Copper Cross-Over)*** para conectar routers a switch.
  - ***Cable directo (Copper Straight-Through)*** para conectar switches a computadoras y al servidor.

Paso 1: Diseñar la topología

a. Abre Cisco Packet Tracer.

b. Arrastra los siguientes dispositivos al área de trabajo:
   - 2 Routers.
   - 4 switches.
   - 8 computadoras.
   - 1 servidor.

c. Conecta los dispositivos de la siguiente manera:
   - Conecta el ***Router1*** al ***Switch1*** y ***Switch2*** usando ***cables cruzados***.
   - Conecta el ***Router2*** al ***Switch3*** y ***Switch4*** usando ***cables cruzados***.
   - Conecta ***PC1*** y ***PC2*** al ***Switch1*** usando ***cables directos***.
   - Conecta ***PC3*** y ***PC4*** al ***Switch2*** usando ***cables directos***.

- Conecta ***PC5*** y ***PC6*** al ***Switch3*** usando ***cables directos***.
- Conecta ***PC7*** y ***PC8*** al ***Switch4*** usando ***cables directos***.
- Conecta el ***Servidor*** al ***Switch2*** usando un ***cable directo***.

Paso 2: Realizar el subneteo

Supongamos que tienes la dirección IP ***192.168.1.0/24*** y necesitas dividirla en subredes para las cuatro redes LAN (una por cada switch). Usaremos ***VLSM*** (Variable Length Subnet Mask) para optimizar el espacio de direcciones.

1. Divide la red 192.168.1.0/24 en cuatro subredes:
    - ***Subred 1***: 192.168.1.0/26 (64 direcciones, para Switch1).
    - ***Subred 2***: 192.168.1.64/26 (64 direcciones, para Switch2).
    - ***Subred 3***: 192.168.1.128/26 (64 direcciones, para Switch3).
    - ***Subred 4***: 192.168.1.192/26 (64 direcciones, para Switch4).

Paso 3: Configurar las interfaces de los routers

a. Haz clic en el Router1 y selecciona la pestaña «Config».
b. Configura las interfaces:
    - ***GigabitEthernet0/0*** (conectada a Switch1):
        - IP Address: ***192.168.1.1***
        - Subnet Mask: ***255.255.255.192***
        - Activa la interfaz (enciéndela).
    - ***GigabitEthernet0/1*** (conectada a Switch2):
        - IP Address: ***192.168.1.65***
        - Subnet Mask: ***255.255.255.192***
        - Activa la interfaz.
c. Repite el proceso para el Router2:
    - ***GigabitEthernet0/0*** (conectada a Switch3):
        - IP Address: ***192.168.1.129***
        - Subnet Mask: ***255.255.255.192***
        - Activa la interfaz.
    - ***GigabitEthernet0/1*** (conectada a Switch4):
        - IP Address: ***192.168.1.193***
        - Subnet Mask: ***255.255.255.192***
        - Activa la interfaz.

Paso 4: Configurar el servidor DHCP

a. Haz clic en el Servidor y selecciona la pestaña «Desktop» > «IP Configuration».
b. Configura la IP estática del servidor:
    - IP Address: ***192.168.1.66***
    - Subnet Mask: ***255.255.255.192***
    - Default Gateway: ***192.168.1.65***.

c. Configura el servicio DHCP:
- Ve a la pestaña ***"Services"*** > ***«DHCP»***.
- Crea un nuevo pool DHCP para cada subred:
  - ***Pool para Subred 1 (Switch1)***:
    - Default Gateway: ***192.168.1.1***
    - DNS Server: ***192.168.1.66***
    - Start IP Address: ***192.168.1.10***
    - Subnet Mask: ***255.255.255.192***
  - ***Pool para Subred 2 (Switch2)***:
    - Default Gateway: ***192.168.1.65***
    - DNS Server: ***192.168.1.66***
    - Start IP Address: ***192.168.1.70***
    - Subnet Mask: ***255.255.255.192***
  - ***Pool para Subred 3 (Switch3)***:
    - Default Gateway: ***192.168.1.129***
    - DNS Server: ***192.168.1.66***
    - Start IP Address: ***192.168.1.130***
    - Subnet Mask: ***255.255.255.192***
  - ***Pool para Subred 4 (Switch4)***:
    - Default Gateway: ***192.168.1.193***
    - DNS Server: ***192.168.1.66***
    - Start IP Address: ***192.168.1.194***
    - Subnet Mask: ***255.255.255.192***

Paso 5: Configurar el enrutamiento entre routers

a. Conecta el Router1 y el Router2 usando un cable cruzado en las interfaces disponibles (por ejemplo, GigabitEthernet0/2 en ambos routers).

b. Configura las interfaces de conexión entre routers:
- En el ***Router1:***
  - IP Address: ***10.0.0.1***
  - Subnet Mask: ***255.255.255.252***
  - Activa la interfaz.
- En el ***Router2***:
- IP Address: ***10.0.0.2***
- Subnet Mask: ***255.255.255.252***
- Activa la interfaz.

c. Configura rutas estáticas en ambos routers:
- En el Router1:

```
enable
configure terminal
ip route 192.168.1.128 255.255.255.192 10.0.0.2
ip route 192.168.1.192 255.255.255.192 10.0.0.2
exit
```

- En el Router2:

```
enable
configure terminal
ip route 192.168.1.0 255.255.255.192 10.0.0.1
ip route 192.168.1.64 255.255.255.192 10.0.0.1
exit
```

Paso 6: Verificar la conectividad

a. En PC1, abre la pestaña "Desktop" > «Command Prompt».
b. Realiza un ping a PC5 (192.168.1.130):

```
ping 192.168.1.130
```

Si la configuración es correcta, deberías recibir respuestas exitosas.

a. Repite el proceso desde PC5 hacia PC1 para verificar la conectividad en ambos sentidos.

Paso 7: Guardar la configuración

1. En cada router, guarda la configuración para que no se pierda al reiniciar:

```
enable
write memory
```

Resumen de la configuración:

- Router1:
  - Interfaz GigabitEthernet0/0: 192.168.1.1/26
  - Interfaz GigabitEthernet0/1: 192.168.1.65/26
  - Interfaz GigabitEthernet0/2: 10.0.0.1/30
  - Rutas estáticas:
    - ip route 192.168.1.128 255.255.255.192 10.0.0.2
    - ip route 192.168.1.192 255.255.255.192 10.0.0.2
- Router2:
  - Interfaz GigabitEthernet0/0: 192.168.1.129/26
  - Interfaz GigabitEthernet0/1: 192.168.1.193/26
  - Interfaz GigabitEthernet0/2: 10.0.0.2/30
  - Rutas estáticas:
    - ip route 192.168.1.0 255.255.255.192 10.0.0.1
    - ip route 192.168.1.64 255.255.255.192 10.0.0.1

Consejos adicionales:

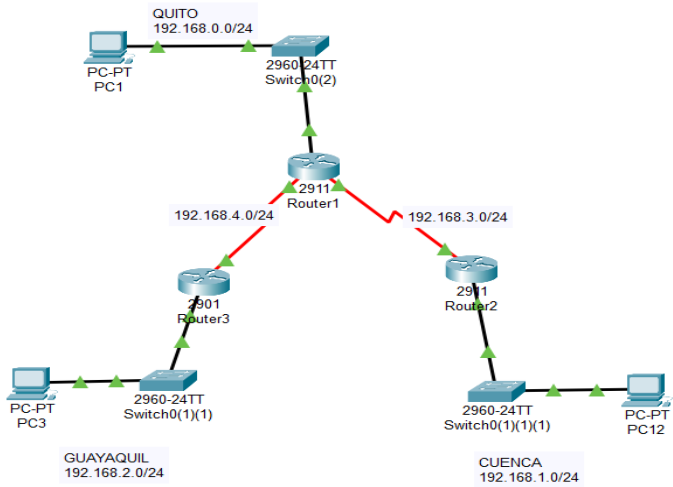
- Si no hay conectividad, verifica las IPs, las máscaras de subred y las rutas estáticas.
- Usa el comando `show ip route` en los routers para verificar las rutas configuradas.
- Asegúrate de que todas las interfaces estén activas (`no shutdown`).

CASO 4

Simulación de una red de datos con 3 routers

- Tres Router 2620XM
- Tres switches 2950-24
- Cuatro Módulos seriales WIC – 1T

1. Topología de la red y direccionamiento IP



a. Arrastrar al área trabajo los dispositivos (switch, router y dispositivos)

- Con base en la topología de la red arrastre tres router Cisco 2620XM.
- Realice de forma similar para pasar los Tres Switches 2950-24
- De igual forma seleccione en dispositivos finales (End Devices) el computador y arrastre tres computadores genéricos

b. Adicionar los módulos seriales a los router

Se debe adicionar a los router los módulos seriales para la interconexión WAN de las redes.

En el router de Quito se le deben adicionar dos módulos seriales WIC – 1T (Uno para interconectar cada ciudad) y en los otros dos router un solo serial. Para realizarlos realice los siguientes pasos.

- Selección el router (dar clic)
- Apague el router, dando clic en el interruptor del router
- Adicione el módulo WIC – 1T seleccione Physical/Modules/ WIC – 1T y arrastre el módulo a los slots pequeños, en el Router de Quito adicione dos módulos y debe quedar como aparece en la siguiente figura.
- Prenda el router, dando clic en el interruptor del router.
- En el router de Cuenca y Guayaquil adicione un módulo serial WIC – 1T de forma similar.

c. Interconectar los dispositivos LAN Y WAN

Usando los Switches interconecte en cada ciudad el computador y el router para lo cual realice los siguientes pasos:

- Con base en la topología de la red seleccione ***Connections*** (Conexiones) parte inferior izquierda (Reset Networks) y en la ventana siguiente seleccione ***Cooper Straight-Through*** (cable de cobre directo) y realice una línea entre el Computador y Switch, seleccionando el puerto ethernet del computador y cualquier puerto libre del switch. De Igual forma entre el Router y el Switch.
- Realice de igual forma en las otras dos ciudades

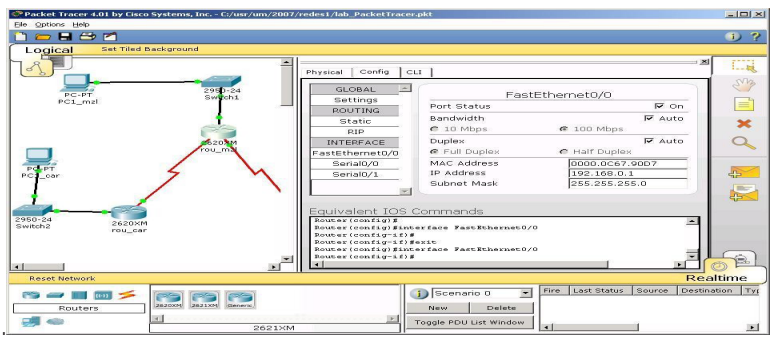
Usando los puertos seriales de los router interconecte las ciudades para lo cual realice el siguiente paso:

- Con base en la topología de la red seleccione ***Connections*** (Conexiones) parte inferior izquierda (Reset Networks) y en la ventana siguiente seleccione ***Serial DCE*** (cable Serial del equipo de Control de Datos) y realice una línea entre el Router de Quito y Router de Guayaquil.
- Realice de igual forma entre los router de Quito y Cuenca.

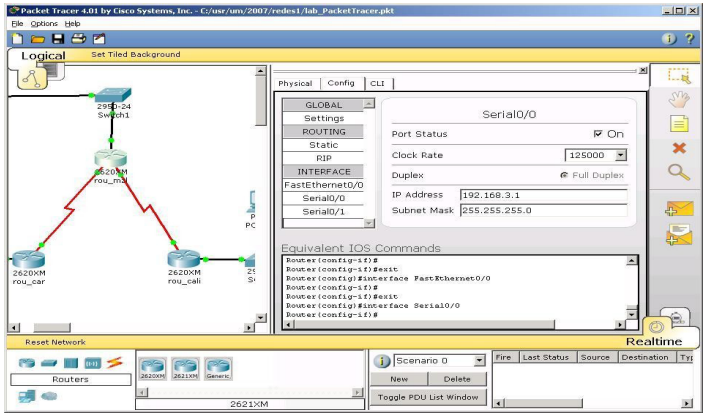
Realizar la configuración del direccionamiento IP de los dispositivos LAN y WAN

Para la configuración del direccionamiento IP de los interfaces LAN (FastEthernet – Fa0/0) y de las interfaces WAN (Serial 0/0 – S0/0) Realice el siguiente proceso:

- Selección el router de la red de Quito (doble clic)
- Para configurar el nombre del router en el Menú seleccione Config/Global/Settings y en los campos Display Name y Hostname escriba el nombre del router en el caso de Quito.
- Para configurar la dirección IP del router en la Interface LAN, en el Menú seleccione Interfaces/FastEthernet0/0, active la interface seleccionada el campo Port Status y en los campos IP Address y Subnet Mask escriba la dirección IP y la máscara de subred, para el router de Quito la dirección IP sería 192.168.0.1 y la máscara 255.255.255.0 y debe quedar como aparece en la siguiente figura



- Para configurar la dirección IP del router en la Interface Wan entre Quito y Cuenca, en el Menú seleccione Config/Interfaces/Serial0/0, active la interface seleccionado el campo Port Status, como el router de Quito es el DCE (Equipo Control de Datos – MODEM) configure la velocidad de transmisión a 125000 bits por segundo en el campo Clock Rate y en los campos IP Address y Subnet Mask escriba la dirección IP y la máscara de subred, para el router de Quito la dirección IP sería 192.168.3.1 y la máscara 255.255.255.0 y debe quedar como aparece en la siguiente figura.



- Configure la dirección IP del router en la Interface WAN entre Quito y Guayaquil (Serial 0/1) con los siguientes datos:

Campo	*Valor*
Interface	Serial 0/1
Port Status	Activo
Clock Rate	125000 bps
IP Address	192.168.4.1
Subnet Mask	255.255.255.0

- Configure la interface LAN del router de Cuenca con los datos de la siguiente tabla de igual forma que lo hizo en el router de la red de Quito.

Campo	*Valor*
Display Name	Rou_Cuenca
Hostname	Rou_Cuenca
Interface	FastEthernet 0/0
IP Address	192.168.1.1
Subnet Mask	255.255.255.0

- Configure la dirección IP del router en la Interface WAN entre Cuenca y Quito (Serial 0/0) con los siguientes datos:

Campo	*Valor*
Interface	Serial 0/0
Port Status	Activo
Clock Rate	Not Set
Ip Address	192.168.3.2
Subnet Mask	255.255.255.0

- Configure la interface LAN del router de Guayaquil con los datos de la siguiente tabla, de igual forma que lo hizo en el router de la red de Quito.

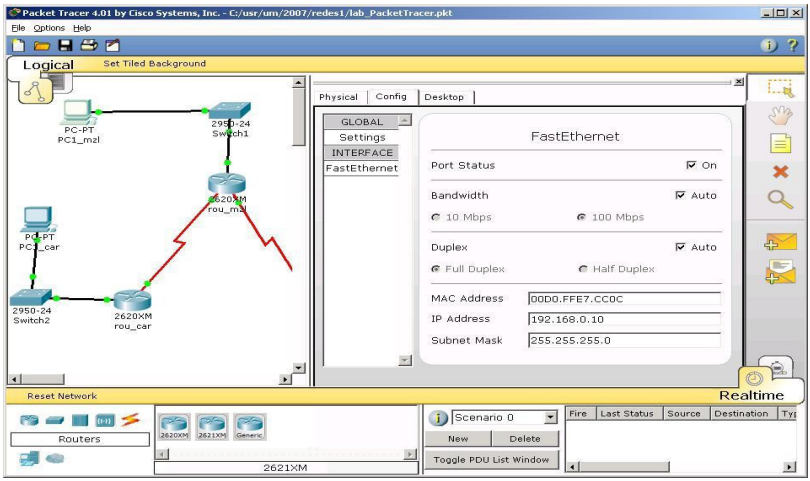
Campo	*Valor*
Display Name	Rou_car
Hostname	Rou_car
Interface	FastEthernet 0/0
Ip Address	192.168.2.1
Subnet Mask	255.255.255.0

- Configure la dirección IP del router en la Interface WAN entre Guayaquil y Quito (Serial 0/0) con los siguientes datos:

Campo	*Valor*
Interface	Serial 0/0
Port Status	Activo
Clock Rate	Not Set
Ip Address	192.168.4.2
Subnet Mask	255.255.255.0

- Para configurar la dirección IP de los computadores seleccione el computador de la red de Quito (dando clic).
- Para configurar el nombre del computador y la puerta de enlace en el Menú seleccione Config/Global/Settings y en los campos Display Name y Gateway escriba el nombre del computador en el caso de Quito y como puerta de enlace 192.168.0.1.
- Para configurar la dirección IP del computador en la Interface LAN, en el Menú seleccione Interfaces/FastEthernet0/0, active la interface seleccionada el campo Port Status y en los campos IP Address y Subnet Mask escriba la dirección IP y la máscara de subred, para el computador

de Quito la dirección IP sería 192.168.0.10 y la máscara 255.255.255.0 y debe quedar como aparece en la siguiente figura.



- Configure la interface LAN del computador de Cuenca con los datos de la siguiente tabla, de igual forma que lo hizo en el computador de la red de Quito.

Campo	*Valor*
Display Name	Pc1_Cuenca
Gateway	192.168.1.1
Interface	FastEthernet 0/0
Ip Address	192.168.1.10
Subnet Mask	255.255.255.0

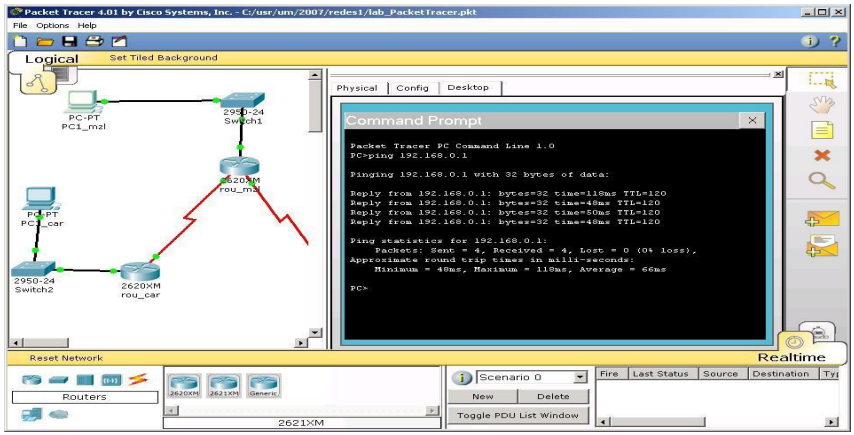
- Configure la interface LAN del computador de Guayaquil con los datos de la siguiente tabla de igual forma que se hizo en el computador de la red de Quito.

Campo	*Valor*
Display Name	Pc1_car
Gateway	192.168.2.1
Interface	FastEthernet 0/0
Ip Address	192.168.2.10
Subnet Mask	255.255.255.0

2.Probar conectividad LAN

Desde el computador de cada red realizar un ping a la puerta de enlace para probar conectividad en cada LAN, siga los siguientes pasos

- Selección el computador de la red de Quito (doble clic), para realizar un ping a la puerta de enlace, seleccione ***Desktop/Command Prompt,*** y escriba el comando ***ping 192.168.0.1*** y debe aparecer como lo muestra la siguiente figura.



- Realizar la misma prueba en los computadores de cada ciudad. En caso de problemas revisar todo el proceso.

3.Configurar el enrutamiento dinámico (RIP)

Para configurar el enrutamiento dinámico en cada router se debe informar que direcciones de red tiene conectada directamente a cada router (adyacentes) y el protocolo de enrutamiento se encarga de averiguar y actualizar las tablas de enrutamiento.

En el router de Quito tiene tres redes adyacentes:

Red	*Dirección de Red*
LAN Quito	192.168.0.0
WAN entre Quito y Cuenca	192.168.3.0
WAN entre Quito y Guayaquil	192.168.4.0

En el router de Cuenca tiene dos redes adyacentes:

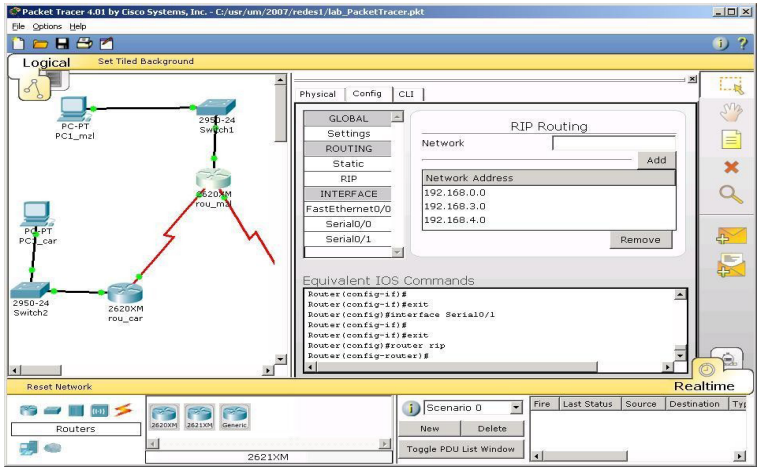
Red	*Dirección de Red*
LAN Cuenca	192.168.1.0
WAN entre Cuenca y Quito	192.168.3.0

En el router de Guayaquil dos redes adyacentes:

Red	*Dirección de Red*
LAN Guayaquil	192.168.2.0
WAN entre Guayaquil y Quito	192.168.4.0

Para configurar el enrutamiento dinámico en el router siga los siguientes pasos

- Selección el router de la red de Quito (doble clic)
- Para configurar el enrutamiento rip en el router de Quito en el Menú seleccione ***Config/Routing/RIP*** y adicione las tres direcciones de red adyacentes en el campo ***Network***, que están en la tabla 8 y queda como aparece en la siguiente figura.



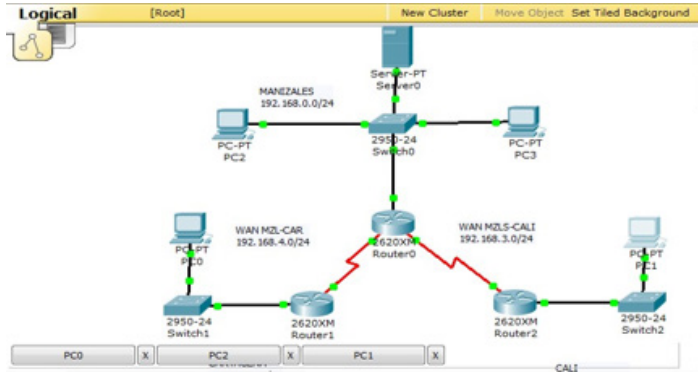
Realice el mismo proceso en los router de Cuenca y GUAYAQUIL adicionando las redes que están conectadas directamente a cada router (adyacentes).

4.Probar conectividad Wan

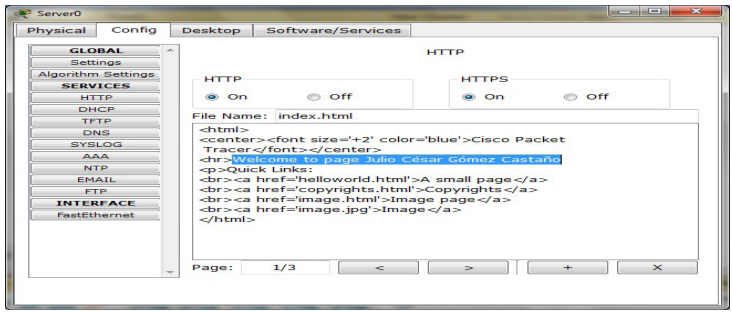
Desde el computador de cada red realizar un ping y un tracert a los computadores de las otras redes, para probar conectividad en cada LAN. Selección el computador de la red de Quito (de clic), para realizar un ping al computador de la red de Cuenca, seleccione Desktop/Command Prompt, y escriba el comando ping 192.168.1.10 y tracert 192.168.1.10.

5.Configurar un servidor con HTTP, DNS, DHCP, SMTP, POP3, FTP, NTP

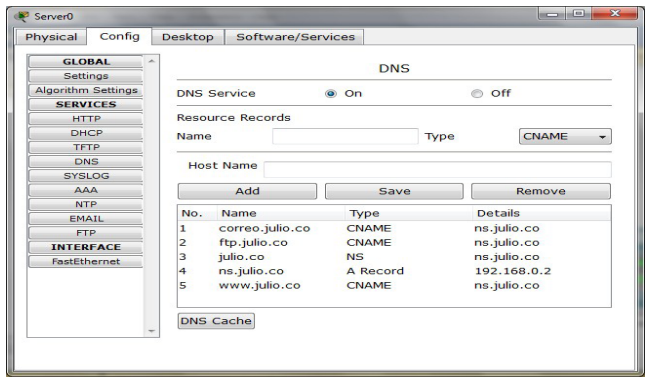
Configurar un servidor en la red de Quito con la dirección IP 192.168.0.2 como aparece en la siguiente figura.



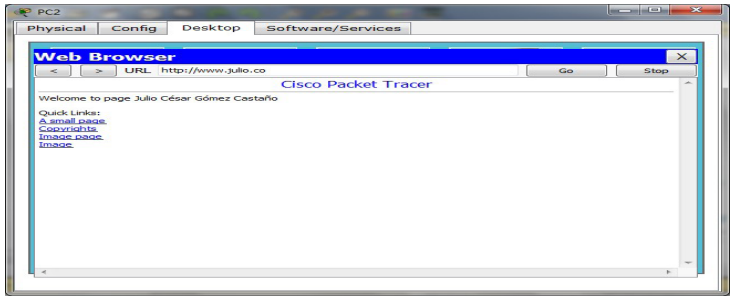
Configurar el servicio de http por las opciones Config/HTTP y modifique la página web con su nombre completo como aparece en la figura 10. Y desde un pc con el navegador cargue la página de la dirección IP del servidor 192.168.0.2, como aparece en la siguiente figura.



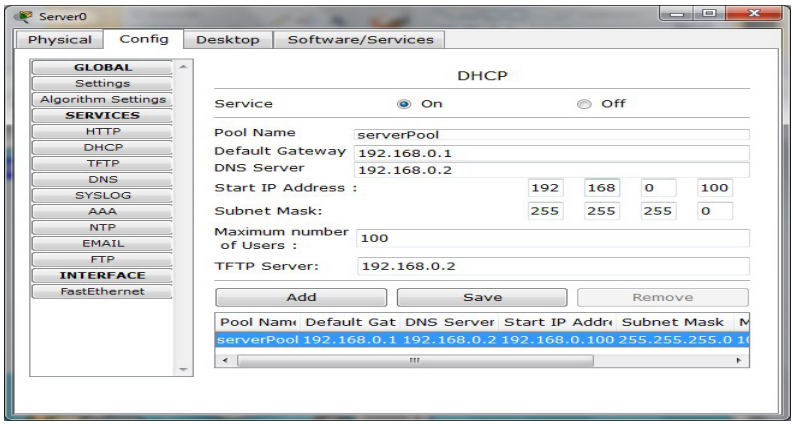
Configurar el servicio de DNS por las opciones Config/DNS y adicione los registros CNAME (Nombre canónico) NS (nameserver) y A Record (Apuntador a registro) con su nombre (su_nombre.co, por ejemplo julio.co, pero cambie julio por el nombre suyo), como aparece en la siguiente figura.



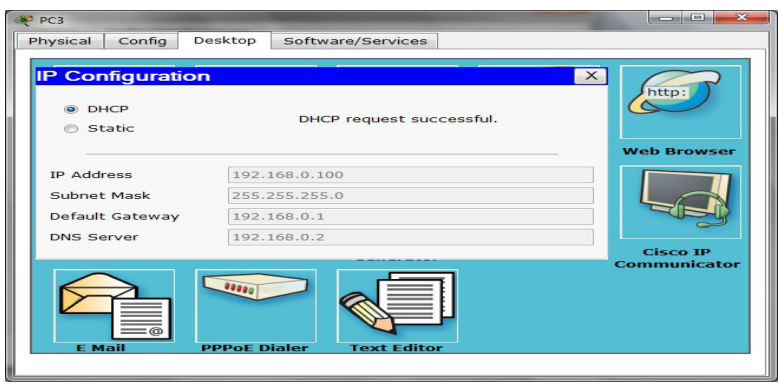
Desde el pc de QUITO cargue la página del servidor con el URL de su dominio, como aparece en la siguiente figura.



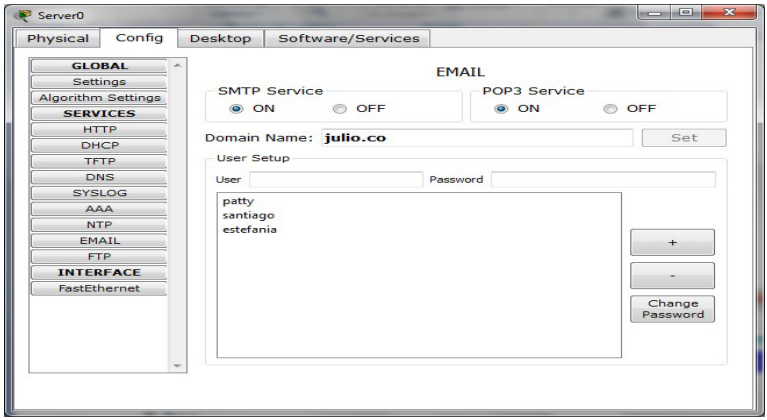
Configura el servidor DHCP con los siguientes datos (Puerta de enlace 192.168.0.1, DNS server 192.168.0.2, IP de inicio 192.168.0.100 y Máscara 255.255.255.0) sola para la red de QUITO, como aparece en la siguiente figura.



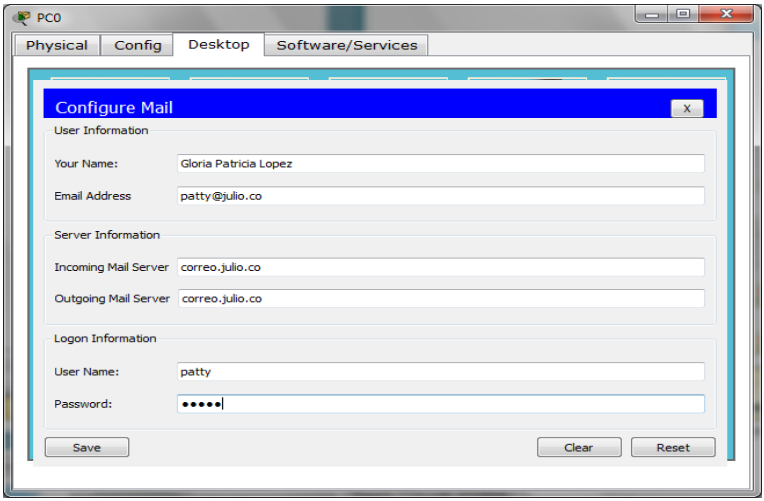
Adicionar un computador a la red de QUITO y que la IP se la asigne el servidor DHCP y realice la prueba, como se aprecia en la siguiente figura.



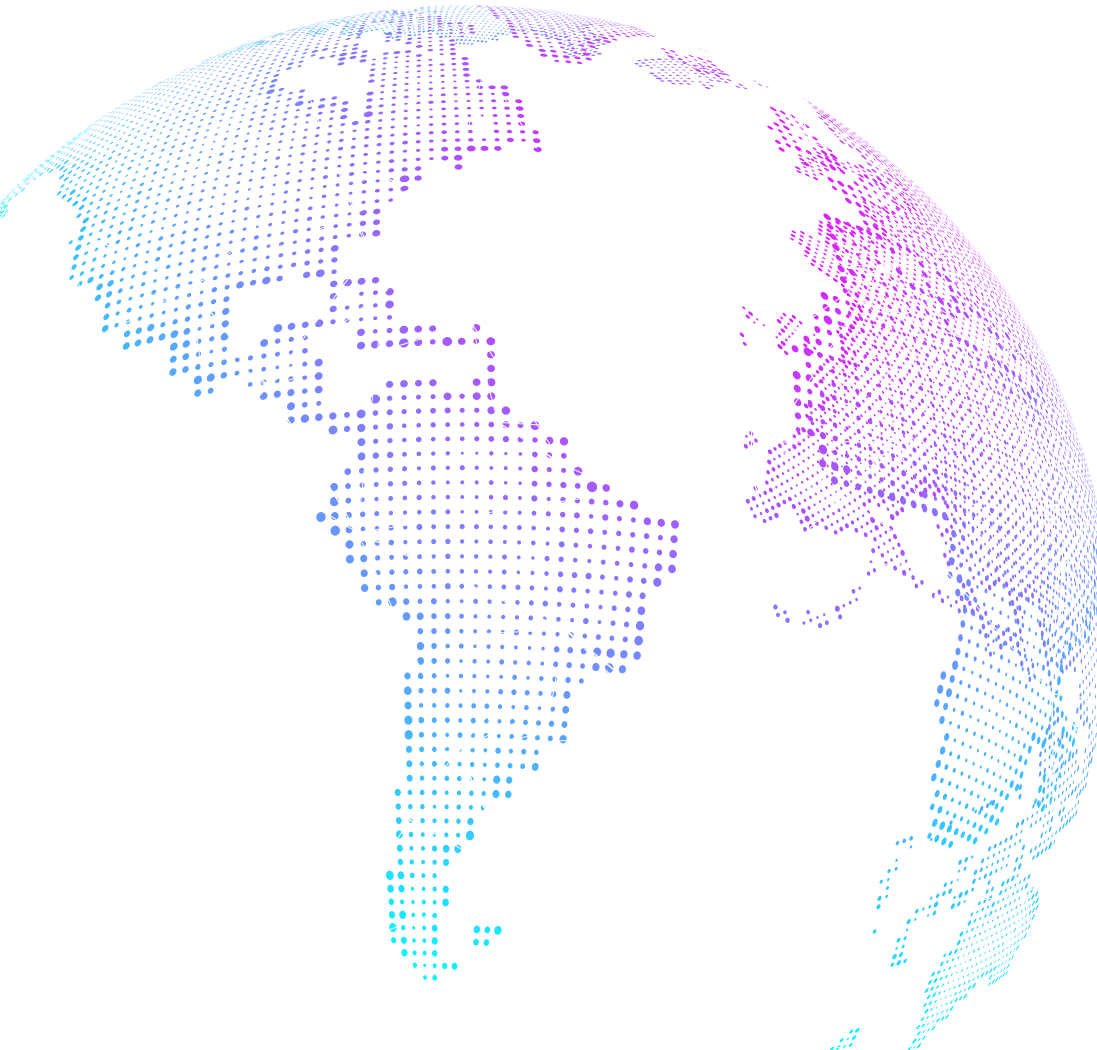
Configurar el servicio de SMTP y POP3 en el servidor por las opciones Config/EMAIL con su dominio y adicione dos o tres cuentas de correo, con los nombres que quiera, como ejemplo mire la siguiente figura.



Configure en el PC de GUAYAQUIL una de las cuentas de correo creadas y la otra cuenta en el PC de Cuenca, como aparece en la siguiente figura.



CAPITULO IV TECNOLOGÍAS DE ACCESO: REDES FIJAS, REDES INALÁMBRICAS Y REDES MÓVILES



CAPITULO IV

TECNOLOGÍAS DE ACCESO: REDES FIJAS, REDES INALÁMBRICAS Y REDES MÓVILES

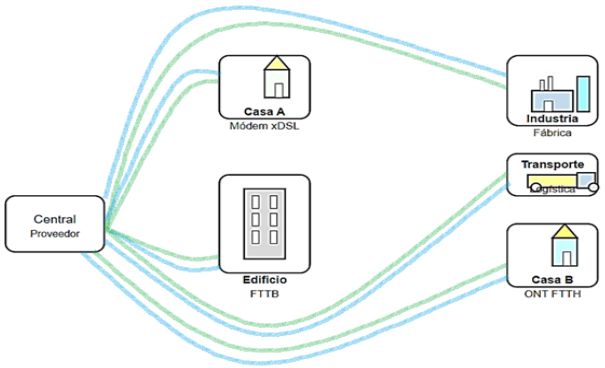
En el panorama actual de las telecomunicaciones, la conectividad se ha vuelto el eje central de la vida moderna. Este trabajo explora la diversidad de tecnologías de acceso que hacen posible esta conexión, sentando las bases para comprender la convergencia de redes fijas y móviles. Comenzaremos analizando las redes fijas, donde examinaremos la evolución desde las soluciones basadas en cobre, como xDSL, hasta las infraestructuras de fibra óptica (FTTx). Luego, nos adentraremos en las redes inalámbricas, incluyendo Wi-Fi para entornos locales y la histórica WiMAX, que prometió conectividad metropolitana. Finalmente, recorreremos el desarrollo de las redes móviles, desde las primeras generaciones (2G) centradas en la voz, pasando por el auge de los datos con 3G y 4G, hasta llegar a la revolucionaria 5G, que redefine la velocidad, latencia y capacidad. Este viaje a través de las diferentes tecnologías de acceso es crucial para entender los desafíos y oportunidades que presenta la integración de estas redes, un punto central en el análisis de protocolos de enrutamiento para lograr una convergencia eficiente y sin interrupciones.

4.1. Introducción y fundamentos de las redes de acceso fijo (xdsl, fttx)

Las redes de telecomunicaciones se dividen en redes esenciales, que transportan grandes volúmenes de datos a larga distancia, y redes de acceso, que conectan a los usuarios finales con la red principal. Las tecnologías de acceso fijo son el último eslabón de esta cadena y su evolución ha sido impulsada por la creciente demanda de ancho de banda para servicios como: el streaming de video, los videojuegos en línea, y el teletrabajo. Este trabajo examinará las dos tecnologías de acceso fijo predominantes: xDSL, basada en el cobre, y FTTx, basada en la fibra óptica.

Dentro de los fundamentos técnicos. Las redes de acceso fijo representan la base de la conectividad digital moderna, permitiendo la transmisión eficiente de datos, voz y video hacia hogares y empresas a través de infraestructuras físicas dedicadas. A diferencia de las redes móviles, las redes fijas ofrecen mayor estabilidad, velocidad y capacidad, lo que las convierte en la opción preferida para servicios de banda ancha, televisión por cable y telefonía IP. Su evolución ha sido clave para el desarrollo económico y social, facilitando el acceso a recursos educativos, laborales y de entretenimiento. En el ámbito técnico, las principales tecnologías de acceso fijo son xDSL y FTTx. La familia xDSL utiliza el par de cobre de las líneas telefónicas tradicionales, permitiendo la coexistencia de servicios de voz y datos mediante técnicas de modulación avanzada. Por otro lado, FTTx emplea fibra óptica para acercar la conectividad al usuario final, ya sea directamente al hogar (FTTH), al edificio (FTTB) o a puntos cercanos (FTTC, FTTN). La fibra óptica destaca por su alta capacidad, baja atenuación y velocidades superiores, habilitando servicios avanzados como streaming en alta definición y teletrabajo. El análisis de estas tecnologías es fundamental para comprender el presente y futuro de la conectividad fija.

Figura 39. Muestra visual de las redes fijas (Azul=xDSL cobre, Verde=FTT fibra óptica)



Nota: Se muestra visualmente cómo las redes fijas pueden utilizar tanto el cobre (xDSL) como la fibra óptica (FTTx) para conectar la central de telecomunicaciones con casas y edificios, resaltando la coexistencia y evolución de ambas tecnologías.

Las redes de acceso fijo se evalúan en base a tres métricas principales: La velocidad de una red fija corresponde a la tasa de transferencia de datos, expresada en Mbps o Gbps, e incluye tanto la descarga (downstream) como la subida (upstream). La latencia es el tiempo de respuesta para el envío y retorno de paquetes de datos, siendo fundamental para aplicaciones en tiempo real. La fiabilidad se refiere a la estabilidad y consistencia de la conexión, influida por factores como la atenuación de la señal y las interferencias.

La Era del Cobre: La Tecnología xDSL

El origen y principios de funcionamiento de xDSL (Línea de Abonado Digital) es una familia de tecnologías que revolucionó la conectividad al permitir la transmisión de datos a alta velocidad a través de los cables de cobre de la red telefónica tradicional. Su principio fundamental es la división de frecuencias: las frecuencias bajas se reservan para el servicio de voz (llamadas telefónicas), mientras que las altas se destinan a los datos. Esta separación permite a los usuarios disfrutar de una conexión a Internet de banda ancha y usar el teléfono simultáneamente, sin interferencias. Esta innovación fue clave para la masificación del acceso a Internet en los hogares y empresas antes del auge de la fibra óptica. ADSL y VDSL son variantes de xDSL para acceso a Internet. ADSL fue la primera versión popular, con velocidad asimétrica y máximos de 8 Mbps de descarga y 1 Mbps de subida, ideal para consumo de contenido. VDSL es su evolución, ofreciendo velocidades mucho mayores (hasta 100 Mbps), pero su rendimiento depende fuertemente de la cercanía a la central telefónica, disminuyendo a mayor distancia.

Tabla. Cuadro de la familia xDSL (9a)

Tipo de DSL	*Descripción*	*Downstream/Upstream*	*Límite distancias*	*Aplicaciones*
ISDN	ISDN Digital Subscriber line	128 Kbps	5,5 Km con 24 AWG	Similar al ISDN BRI, solamente para servicios de datos (sin voz sobre la misma línea)
CDSL	Consumer DSL from Rockwell	1 Mbps downstream sin Upstream	5,5 Km con 24 AWG	Sin filtro, para hogares y pymes (SOHO), similar al DSL Lite
DSL Lite	DSL sin filtro	1.544 - 6 Mbps según servicio	5,5 km con 24 AWG	El estándar ADSL, sacrifica velocidad a condición de no instalar el filtro en el usuario final
G. Lite	DSL sin filtro	1.544 - 6 Mbps según servicio	5,5 km con 24 AWG	El estándar ADSL, sacrifica velocidad a condición de no instalar el filtro en el usuario final
HDSL	High bit-rate digital subscriber line	1.544 Mbps dúplex sobre 2 pares trenzados; 2.048 Mbps dúplex sobre 3 pares trenzados	3,6 Km con 24 AWG	T1/E1 - Servicio entre servidores WAN, LAN, servidores de acceso

Nota: Variantes xDSL históricas, como ISDN y HDSL, con velocidades limitadas y aplicaciones básicas, muchas ya en desuso o poco conocidas. Ejemplo: ISDN y HDSL eran usados más en empresas y para interconexión de redes.

Tabla Cuadro de la familia xDSL (9b)

Tipo de DSL	*Descripción*	*Downstream / Upstream*	*Límite distancias*	*Aplicaciones*
SDSL	Symmetric DSL	1.544 Mbps dúplex (U.S. y Canadá); 2.048 Mbps (Europa). Línea dúplex downstream y upstream	3,6 km con 24 AWG	Similar a HDSL, pero requiere solamente un único par trenzado

Tipo de DSL	*Descripción*	*Downstream / Upstream*	*Límite distancias*	*Aplicaciones*
ADSL	Asymmetric Digital Subscriber Line	1.544 a 6.1 Mbps downstream, 16 a 640 Kbps upstream	1.544 Mbps - 5,5 km; 2.048 Mbps - 4,8 km; 6.312 Mbps - 3,6 km; 8.448 Mbps - 2,7 km	Usado para Internet, video, full motion, videoconferencia, telemedicina, teleducación, etc.
RADSL	Rate-Adaptive DSL from Westell	Adaptado a la línea, 640 Kbps a 2.2 Mbps downstream; 272 Kbps a 1.085 Mbps upstream	Desconocido	Similar al ADSL
UDSL	Unidirectional DSL propuesto por una compañía Europea	Desconocido	Desconocido	Similar al ADSL
VDSL	Very High Digital Subscriber Line	12.9 a 52.8 Mbps downstream; 1.5 a 2.3 Mbps upstream	1,35 Km - 12.96 Mbps; 0,9 Km - 25.82 Mbps; 300 mts. - 51.84 Mbps	Red ATM, Fibra

Nota: Destaca variantes modernas de xDSL, como ADSL y VDSL, que ofrecen mayores velocidades y eficiencia, adaptándose a las demandas actuales de Internet residencial y servicios multimedia (Pérez Romero, 2005). Ejemplo: ADSL y VDSL son los más comunes en hogares para acceso a Internet de banda ancha

Tabla. Cuadro de la familia xDSL. Relación entre 9a y 9b.

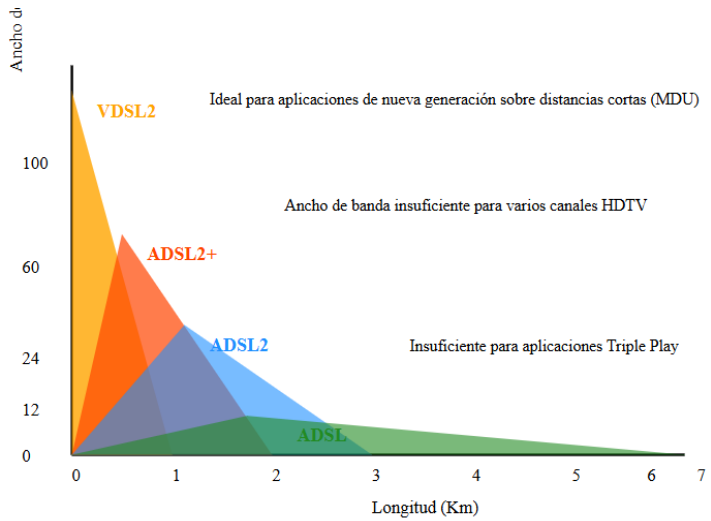
Cuadro	*Tecnologías incluidas*	*Enfoque principal*	*Velocidades/Aplicaciones*
Tabla1. 9ª	ISDN, CDSL, DSL Lite, G. Lite, HDSL	Variantes históricas/básicas	Básicas, empresariales, datos
Tabla 2. 9b	SDSL, ADSL, RADSL, UDSL, VDSL	Variantes avanzadas/modernas	Altas velocidades, Internet, video

Nota: La Tabla 1. Muestra las variantes ***iniciales y menos avanzadas*** de xDSL, mientras. La Tabla 2. presenta las ***versiones modernas y de mayor capacidad*** que se utilizan actualmente para acceso a Internet de alta velocidad.

Los dos cuadros presentan variantes de la familia xDSL, pero difieren en enfoque y evolución tecnológica. El primer cuadro incluye tecnologías básicas y pioneras como ISDN, CDSL y HDSL, orientadas a servicios empresariales y conexiones de baja velocidad, muchas ya en desuso. El segundo cuadro muestra variantes modernas como ADSL, SDSL y VDSL, que ofrecen mayores velocidades, mejor adaptabilidad y están diseñadas para satisfacer la demanda actual de Internet de banda ancha en hogares y empresas. En resumen, el primer cuadro refleja la etapa inicial y el segundo la evolución y sofisticación de las tecnologías xDSL.

La tecnología xDSL ha sido fundamental en la expansión del acceso a Internet de banda ancha, permitiendo aprovechar la infraestructura de cobre existente para ofrecer servicios rápidos y eficientes. A través de sus diferentes variantes, xDSL ha evolucionado desde soluciones básicas y empresariales hasta opciones avanzadas que satisfacen las crecientes demandas de velocidad y conectividad de hogares y empresas. Su desarrollo ha facilitado la inclusión digital y ha impulsado el crecimiento de aplicaciones modernas como videoconferencias, streaming y telemedicina, consolidándose como una pieza clave en la historia de las telecomunicaciones.

Figura.40 Ancho de banda vs la distancia. Relación entre 9a y 9b.

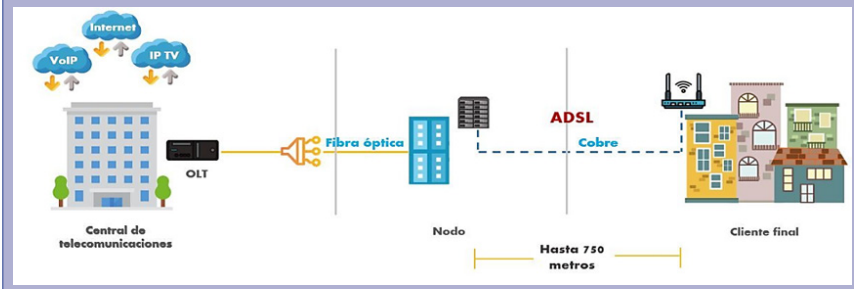
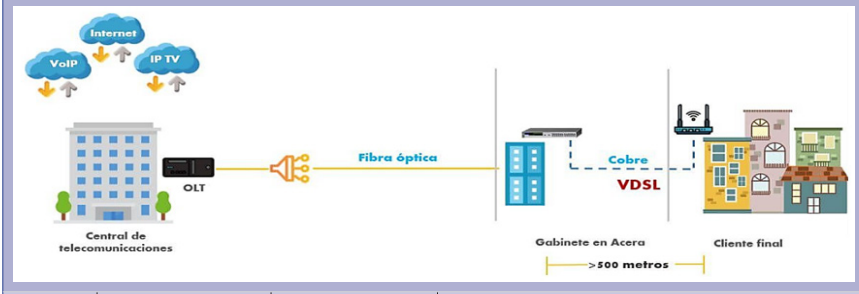
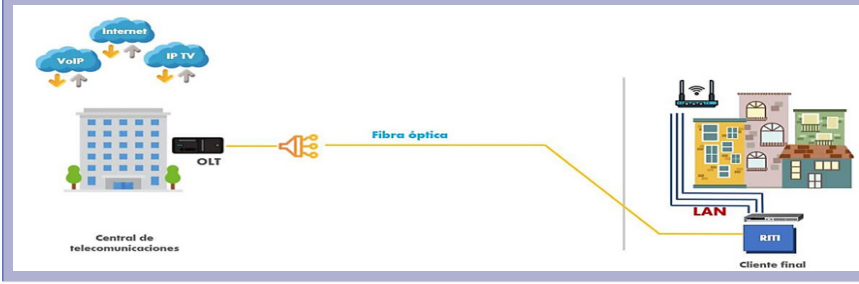


Nota: El gráfico muestra cómo el ancho de banda disminuye con la distancia para cada tecnología. Incluye anotaciones similares a la imagen que enviaste. Los colores y posiciones son aproximados para facilitar la comparación visual.

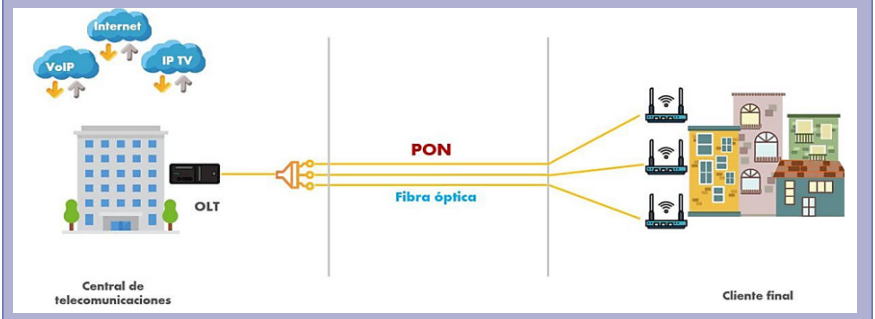
La Solución del Futuro: La Tecnología FTTx

Principios de la Fibra Óptica. FTTx (Fiber-to-the-x) es una tecnología de acceso que utiliza hilos de fibra óptica para transmitir datos mediante pulsos de luz, ofreciendo velocidades muy superiores y mayor alcance que el cobre. Gracias a su inmunidad a interferencias electromagnéticas y mínima pérdida de señal, la fibra óptica garantiza conexiones estables y confiables, convirtiéndose en la opción ideal para satisfacer las crecientes demandas de Internet de alta velocidad y servicios avanzados.

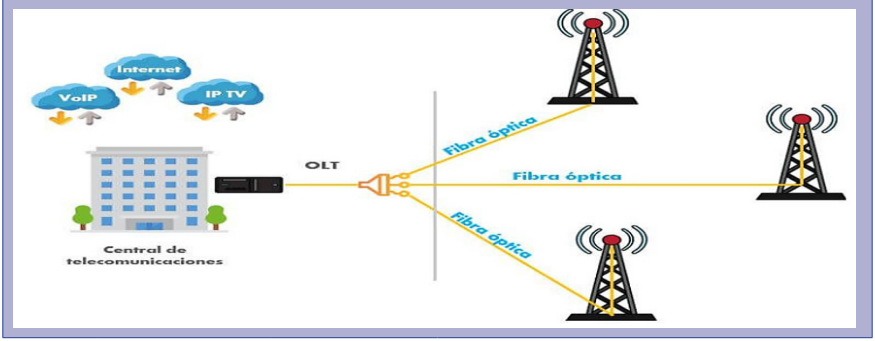
Tabla. Arquitectura de FTTx y los diferentes tipos

Tipo	*Hasta dónde llega la fibra*	*Último tramo hacia el usuario*	*Características principales*
FTTN	Nodo o armario de distribución	Cable de cobre largo	Fibra hasta nodo; cobre hasta usuario; rendimiento limitado.
			
FTTC	Punto de distribución cercano	Cable de cobre corto	Fibra más cerca del usuario; cobre más corto; mejor rendimiento que FTTN.
			
FTTB	Interior del edificio/apartamento	Ethernet o coaxial	Fibra hasta el edificio; distribución interna por cable; alto rendimiento.
			

FTTH	Directamente al hogar	Fibra óptica	Fibra hasta el hogar; máximo rendimiento y velocidad.



FTTA	unidades de radio remotas	Fibra óptica	Fibra hasta el hogar; máximo rendimiento y velocidad.



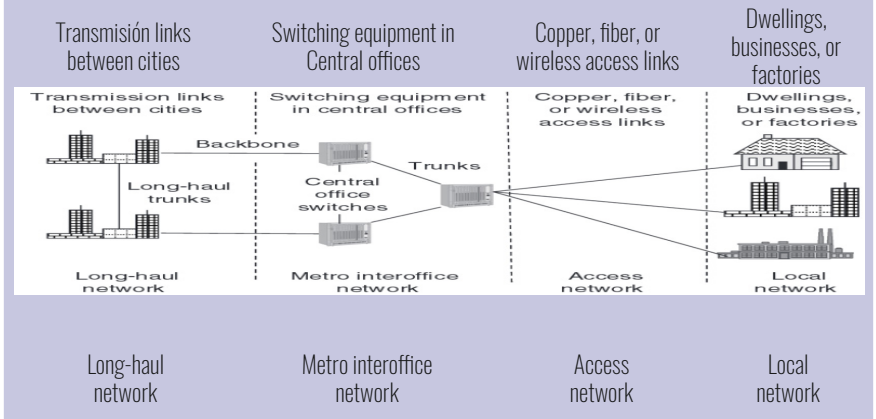
Nota: Cinco tipos principales de FTTx, mostrando hasta dónde llega la fibra y qué tecnología se usa en el tramo final.

Análisis Comparativo: xDSL vs. FTTx

La principal diferencia entre xDSL y FTTx está en el rendimiento. Mientras que xDSL utiliza cables de cobre, FTTx emplea fibra óptica, lo que permite velocidades de transmisión mucho más altas, mayor estabilidad y alcance. La fibra óptica supera al cobre en prácticamente todas las métricas clave, como velocidad, capacidad, resistencia a interferencias y calidad de servicio, convirtiéndose en la opción preferida para redes modernas y de alta demanda.

Tabla. Diferencia fundamental entre xDSL vs. FTTx

Característica	*xDSL (VDSL2)*	*FTTx (GPON)*
Medio	Cobre	Fibra Óptica
Velocidad de Descarga	Hasta 100 Mbps	Hasta 2.5 Gbps (simétrica o asimétrica)
Velocidad de Subida	Hasta 50 Mbps	Hasta 1.25 Gbps
Latencia	Media (10-50 ms)	Baja (< 5 ms)
Fiabilidad	Susceptible a interferencias	Alta, inmune a interferencias
Distancia	Limitada (< 1 km)	Larga (20 km o más)



Nota: La diferencia fundamental entre ambas tecnologías radica en su rendimiento. Centrándonos sobre las redes de acceso, vamos a dejar de lado tecnologías basadas en cobre (xDSL) o inalámbricas (3G, 4G) para centrarnos en las sustentadas sobre infraestructuras de fibra óptica, bien en su totalidad o bien hibridadas con algún otro tipo de portador

Despliegue y Tendencias Futuras

El despliegue de redes FTTx presenta desafíos tanto técnicos como regulatorios. La complejidad de la ingeniería civil para el tendido de cables en áreas urbanas densamente pobladas y el diseño de políticas públicas que fomenten la inversión privada son factores cruciales. En zonas rurales, el bajo retorno de la inversión hace que el despliegue de fibra sea un reto aún mayor. Para 2025, el sector de las redes fijas se centra en el abandono definitivo de las redes de cobre (xDSL), un proceso impulsado por la necesidad de una mayor capacidad. Esta transición ha dado paso a un despliegue masivo y acelerado de la fibra óptica (FTTx) (Cristian, 2025). Las empresas de telecomunicaciones están desmantelando las antiguas infraestructuras de cobre para dar paso a redes más eficientes y fiables, utilizando técnicas de instalación más rápidas, como las soluciones preconectorizadas. Las tendencias futuras se centran en la velocidad, la sostenibilidad y la automatización. Se espera que las tecnologías de ultra banda ancha, como XGS-PON y 10G-PON, se conviertan en el nuevo estándar, ofreciendo velocidades de hasta 10 Gbps para satisfacer la creciente demanda de servicios de alta capacidad.

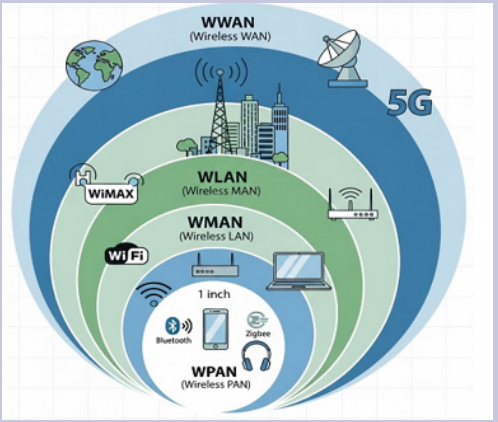
Además, la industria se compromete a una mayor eficiencia energética mediante arquitecturas de red pasivas que reducen la huella de carbono. Finalmente, la integración de la inteligencia artificial (IA) está transformando la gestión de la red, permitiendo a los operadores optimizar el rendimiento y resolver problemas de forma proactiva.

4.2. Redes inalámbricas (WIFI, WIMAX)

Las redes inalámbricas, sistemas de comunicación que prescinden de cables físicos y utilizan ondas de radio, han revolucionado la conectividad moderna. Tecnologías como Wi-Fi, un pilar en la conectividad de áreas locales, y WiMAX, que ofrecía cobertura metropolitana, han impulsado esta transformación. La capacidad de estas redes para conectar dispositivos sin fisuras ha sido crucial para la proliferación del Internet de las Cosas (IoT) y las casas inteligentes. En la industria de telecomunicaciones, 2025 marca el fin de las redes de cobre (xDSL), reemplazadas por la fibra óptica (FTTx). Esta transición, enfocada en velocidades de 10 Gbps (XGS-PON) y la eficiencia energética, se complementa con la inteligencia artificial (IA) para automatizar la gestión de red. Esta visión global de modernización se aplica a proyectos locales. Así, se demuestra cómo la adopción de tecnologías inalámbricas y de fibra mejora tangiblemente la conectividad para optimizar procesos y la calidad educativa, conectando la teoría global con la práctica local.

A pesar de sus ventajas, enfrentan desafíos significativos. La seguridad sigue siendo una preocupación principal, con vulnerabilidades en protocolos de Wi-Fi y ataques cibernéticos. La competencia también ha sido feroz; la tecnología WiMAX, por ejemplo, ha sido eclipsada por el auge de LTE y 5G, lo que plantea dudas sobre la sostenibilidad a largo plazo de ciertas tecnologías. La convergencia con las redes celulares ilustra un panorama dinámico y en constante evolución. El futuro de la conectividad inalámbrica es prometedor. La continua evolución con nuevos estándares como Wi-Fi 6 y Wi-Fi 7, junto con los avances en la tecnología 5G, promete mejorar la experiencia del usuario y superar las limitaciones actuales, manteniéndolas en la vanguardia de la revolución digital, reflejando la visión de un futuro prometedor y en constante cambio.

Tabla. Tipos de redes inalámbricas según su alcance

Redes inalámbricas


	Wireless LAN (WLAN)	Wireless MAN (WMAN)	Wireless PAN (WPAN)	Wireless WAN (WWAN)
Tipo de red	Red de área local	Red de área metropolitana	Red de área personal	Red de área extensa
Objetivo	Proporcionar acceso a internet dentro de un edificio o área exterior limitada	Proporcionar acceso fuera de la oficina y en redes domésticas, típicamente regional	Transmitir señales entre dispositivos en áreas limitadas, típicamente 10 metros	Proporcionar acceso fuera del rango de WLANs y WMANs
Conectividad	Ondas de radio, IEEE 802.11 Wi-Fi	IEEE 802.16 WiMAX	Bluetooth, Zigbee e infrarrojos	Celular, LTE, 5G

Nota: Clasifica las redes inalámbricas en cuatro categorías principales basadas en su área de cobertura. Cada tipo de red utiliza una tecnología específica para la conectividad y tiene un propósito distinto, desde el corto alcance personal hasta la conectividad a nivel global.

Las redes inalámbricas se pueden clasificar en cuatro tipos principales según su tamaño, alcance y requisitos de conectividad: red de área local inalámbrica (WLAN), red de área metropolitana inalámbrica (WMAN), red de área personal inalámbrica (WPAN) y red de área amplia inalámbrica (WWAN). Cada tipo de red inalámbrica cumple funciones diferentes y está diseñada para casos de uso específicos, por lo que es crucial que las organizaciones seleccionen el tipo de red adecuado a sus necesidades. Las redes inalámbricas se basan en arquitecturas como Wi-Fi y WiMAX, cada una con un propósito diferente. La arquitectura Wi-Fi ha evolucionado de redes en malla a una estructura celular para mejorar el rendimiento local. Por su parte, la arquitectura WiMAX fue diseñada para comunicaciones de largo alcance y tiene la capacidad de integrarse con tecnologías más nuevas como LTE y 5G. A pesar de sus beneficios, estas redes enfrentan importantes desafíos de seguridad. Las vulnerabilidades en protocolos antiguos como WEP han sido reemplazadas por estándares más robustos como WPA2 con AES, pero la amenaza de ciberataques como DDoS sigue siendo una preocupación principal. Para mitigar estos riesgos, es crucial implementar estrategias de seguridad de múltiples capas y adoptar un modelo de confianza cero. La creciente proliferación del Internet de las Cosas (IoT) y 5G introduce nuevas amenazas, lo que requiere soluciones de seguridad proactivas.

Las tendencias futuras en el campo de las redes inalámbricas están experimentando una rápida evolución, impulsada por la llegada de tecnologías como 5G y los nuevos estándares de Wi-Fi. La baja latencia de 5G habilita aplicaciones avanzadas como la telemedicina y la realidad aumentada, mientras que los estándares Wi-Fi 6E y Wi-Fi 7 ofrecen mayor velocidad y capacidad. La industria 4.0 está adoptando estas redes para transformar la fabricación con IIoT y automatización. La integración de la Inteligencia Artificial (IA) se presenta como una tendencia clave para optimizar la gestión de red y reducir costos. Este panorama muestra un futuro donde las redes inalámbricas no solo conectan dispositivos, sino que también impulsan la innovación en múltiples sectores.

Tabla. Tendencias futuras en redes inalámbricas

Tendencia	*Tecnologías clave*	*Impacto y aplicaciones*
Avances en tecnología inalámbrica (5G	5G (Quinta Generación)	Baja latencia (1 ms) para telemedicina y cirugía robótica. Habilita realidad virtual/aumentada (VR/AR) y sistemas domésticos inteligentes, impulsando el crecimiento del metaverso.
Integración de Wi-Fi e IoT	Wi-Fi e Internet de las Cosas (IoT)	El mercado de Wi-Fi crecerá sustancialmente por la adopción de dispositivos IoT. Las empresas usarán esta integración para mejorar la eficiencia operativa y la experiencia del cliente.
IA y eficiencia de costos	Inteligencia Artificial (IA)	La IA se integrará en las redes inalámbricas para reducir costos operativos y acelerar la entrega de proyectos. Se espera que impulse la innovación en la gestión de infraestructura.
Industria 4.0	5G Privado, Realidad Aumentada (RA), Internet Industrial de las Cosas (IIoT)	Transformación de la fabricación a través de la automatización y la monitorización en tiempo real. Aumenta la productividad y minimiza el tiempo de inactividad en la industria.
Evolución de Wi-Fi	Wi-Fi 7 y Wi-Fi 6E	Wi-Fi 7 ofrecerá velocidades y rendimiento mejorados. Wi-Fi 6E extenderá las redes a la banda de 6 GHz, proporcionando mayor ancho de banda y capacidad para entornos densos de dispositivos.

Nota: Principales tendencias que están dando forma al futuro de las redes inalámbricas. Desde la llegada de 5G y su capacidad para la baja latencia, que es vital para aplicaciones críticas, hasta la evolución de Wi-Fi con los nuevos estándares Wi-Fi 7 y 6E.

4.3. Redes Móviles (2G A 5G)

Las redes móviles han evolucionado desde la primera generación (1G) analógica hasta la actual 5G, una transformación marcada por avances en velocidad, capacidad y funcionalidad. Cada generación ha impulsado un cambio: la 2G digitalizó la voz y habilitó los SMS, la 3G y 4G ampliaron las capacidades a datos multimedia e internet móvil, y la 5G ha habilitado nuevas aplicaciones de IoT y servicios en tiempo real. Esta evolución ha impactado sectores clave como la salud y el transporte, pero también ha generado desafíos. La preocupación pública por los efectos en la salud del 5G y la necesidad de proteger la infraestructura de las ciberamenazas son problemas actuales (Beltrán Muñoz, 2024). A medida que la industria avanza hacia el 6G y la integración de la inteligencia artificial, el panorama de las telecomunicaciones móviles sigue siendo dinámico, esencial para el desarrollo de la conectividad global y la interacción humana con la tecnología.

Tabla. Evolución de las redes móviles 2G a 5G

Evolución cronológica de las redes móviles por generación

Generación	Año de introducción	Avances clave	Tecnologías y estándares
2G	Principios de 1990	Transición de analógico a digital. Introducción de SMS y MMS. Mejora en la calidad de voz y seguridad.	GSM, GPRS, EDGE
3G	2001	Acceso a internet móvil. Servicios multimedia como videollamadas y navegación GPS. Velocidades de hasta 3,1 Mbps.	CDMA, UMTS
4G	Finales de 2000	Redes completamente IP. Velocidades de banda ultra ancha (hasta 1 Gbps). Habilitación de streaming de video HD e IoT.	LTE, Mobile WiMAX
5G	2019	Velocidad de hasta 10 Gbps. Latencia ultra baja (1 ms). Conectividad masiva para IoT y vehículos autónomos.	5G NR

La evolución de las redes móviles, desde la digitalización de la voz con 2G hasta la conectividad masiva del 5G. Cada generación ha marcado un hito tecnológico, introduciendo mejoras significativas en velocidad, capacidad y funcionalidad. Mientras que la 3G habilitó el acceso a internet móvil y los servicios multimedia, la 4G consolidó la banda ancha y el streaming de alta calidad. La 5G, la última generación, se distingue por su latencia ultra baja y su capacidad para conectar un vasto número de dispositivos, sentando las bases para tecnologías futuras como la telemedicina y los vehículos autónomos.

Los marcos regulatorios y estándares son esenciales para la gestión de las redes móviles. Un régimen regulatorio eficaz incluye una Autoridad Reguladora Nacional (ARN) independiente, leyes y políticas claras. Su objetivo es garantizar una competencia justa, lo que fomenta la innovación y protege a los consumidores. Los reguladores enfrentan el desafío constante de mantenerse al día con los rápidos avances tecnológicos y la creciente complejidad del mercado. Para abordar estos desafíos, se apoya en estándares internacionales establecidos por organizaciones como el 3GPP y la UIT. Estos estándares definen los límites operativos de las redes, desde la 2G hasta la 5G, y son fundamentales para garantizar la seguridad y la eficiencia global. Su adopción facilita la conectividad y una transición fluida entre las diferentes generaciones de tecnología móvil.

El futuro de la telefonía móvil se centrará en la próxima generación de redes, como el 6G, actualmente en fase de investigación. El objetivo es integrar la inteligencia artificial (IA) para crear experiencias de comunicación inmersivas en tiempo real. Esta evolución busca satisfacer la demanda de

una mejor conectividad global y reducir las brechas de comunicación, incluso en entornos complejos y remotos. El aumento constante del uso móvil ha impulsado la necesidad de mayores velocidades, lo que ha llevado a la industria a superar las limitaciones de las generaciones anteriores, como la transición de la 2G a la 3G. Este progreso ha hecho posible la conectividad en lugares extremos, como el Monte Everest, lo que demuestra el potencial para las comunicaciones en tiempo real en cualquier lugar del mundo.

Las empresas del sector se están preparando activamente para estos avances con soluciones innovadoras que optimizan la gestión de datos y la facturación, asegurando que estén equipadas para gestionar el crecimiento exponencial del uso móvil. En esencia, el futuro de las redes móviles estará impulsado por la IA y una conectividad sin precedentes para satisfacer las crecientes expectativas de los usuarios en un mundo cada vez más interconectado.

4.4. Tecnologías Emergentes

El acceso a las redes de telecomunicaciones, especialmente a Internet, es uno de los pilares del desarrollo moderno. La capacidad de conectar personas, empresas, instituciones y dispositivos ha transformado la manera en que vivimos, trabajamos y aprendemos. Sin embargo, el acceso sigue siendo desigual y dependiente de factores tecnológicos, geográficos, económicos y sociales. La tecnología de acceso abarca todos los métodos, infraestructuras y protocolos que permiten la conexión a redes de telecomunicaciones. Desde los primeros módems de línea telefónica hasta los satélites de órbita baja y las redes móviles de sexta generación, el avance ha sido constante y revolucionario. En este capítulo se profundiza en las tecnologías emergentes, se presentan casos prácticos que ilustran su impacto, se analizan tendencias actuales y se ofrecen recursos para continuar el estudio y la investigación.

Las tecnologías emergentes de acceso a Internet están redefiniendo los límites de la conectividad, permitiendo superar obstáculos físicos, económicos y sociales. Estas tecnologías están redefiniendo las redes de comunicación. El 6G, la próxima generación móvil, busca integrar la inteligencia artificial (IA) para habilitar experiencias inmersivas y conectar entornos remotos, superando las capacidades del 5G. Finalmente, la integración de la IA en las redes automatiza la gestión, predice fallos y refuerza la seguridad. Juntas, estas tecnologías están construyendo una infraestructura más inteligente, rápida y eficiente.

Las redes móviles han evolucionado de un modelo centrado en la voz (2G) a uno centrado en los datos (3G y 4G). La quinta generación (5G) representa una ruptura con este paradigma, ofreciendo una arquitectura de red flexible y basada en software (SDN) que prioriza la baja latencia, la alta capacidad y la fiabilidad. El 5G se divide en tres bandas de frecuencia: banda baja (mayor cobertura), banda media (equilibrio entre velocidad y alcance) y banda alta (velocidades multi-gigabit para áreas densas). Sus tres casos de uso principales son la banda ancha móvil mejorada (eMBB), las comunicaciones ultra fiables de baja latencia (URLLC) y las comunicaciones masivas tipo máquina (mMTC), que habilitan el Internet de las Cosas (IoT) y aplicaciones críticas. En el futuro, las redes 6G se encuentran en la fase de investigación. Su visión va más allá de la conectividad humana, buscando la integración de la inteligencia artificial (IA) en la propia red para habilitar la computación perimetral, las comunicaciones holográficas y la interconexión de entornos inteligentes. El 6G no solo aumentará la velocidad, sino que transformará la red en una plataforma inteligente que predice y optimiza la conectividad en tiempo real.

El año 2025, marca un punto de inflexión para la tecnología 5G, ya que se ha consolidado como la principal tecnología de acceso móvil. A diferencia de sus predecesores, sus características técnicas están diseñadas para ir más allá de la conectividad de smartphones, habilitando un ecosistema de aplicaciones y servicios totalmente nuevos.

Tabla. Tendencia de las tecnologías emergentes

Tipo de Tecnología	*Características clave*	*Aplicaciones y uso en 2025*	*Tendencias futuras*
Redes Fijas	xDSL (cobre): Límite en velocidad. FTTx (fibra): Velocidad ultra alta, baja latencia, gran fiabilidad.	xDSL: Se mantiene en zonas rurales. FTTx: Estándar para hogares y empresas, reemplazando al cobre.	Despliegue masivo y acelerado de fibra óptica (FTTH) para cerrar la brecha digital.
Redes Inalámbricas	Wi-Fi: Red de área local (WLAN). WiMAX: Red metropolitana (WMAN).	Wi-Fi: Conectividad principal en interiores. WiMAX: Mayormente reemplazado por 4G/5G.	Evolución a Wi-Fi 6E y 7 para mayor velocidad y menor latencia en interiores.
Redes Móviles	5G: Velocidad ultra alta, latencia ultra baja, conectividad masiva. Arquitectura flexible.	5G: Habilita IoT, vehículos autónomos, telemedicina y banda ancha mejorada (eMBB).	6G: Integración de IA, comunicación holográfica y conectividad ubicua.
Tecnologías Emergentes	Li-Fi: Transmisión de datos por luz. Computación Perimetral: Procesamiento local de datos. IA: Optimización y seguridad de la red.	Li-Fi: Uso en entornos seguros como hospitales y aviones. Edge: Crucial para vehículos autónomos y fábricas inteligentes.	Fusión del Edge Computing y la IA para redes más inteligentes, proactivas y eficientes.
Nube	Inteligencia artificial	Colaboración. Servicios	Tecnología 5G

Nota: Principales tecnologías de acceso y su evolución, destacando sus características técnicas y el impacto en 2025. Muestra la transición de tecnologías heredadas como xDSL y WiMAX a las soluciones de vanguardia como FTTx y 5G. Integra las tendencias emergentes como la IA y el 6G, que marcarán el futuro de la conectividad al ofrecer redes más inteligentes, rápidas y eficientes.

El futuro próximo, aunque aún en desarrollo es la conectividad 6G que promete velocidades superiores a 100 Gbps, integración total de inteligencia artificial, comunicaciones holográficas y soporte para aplicaciones de realidad extendida. Se espera que habilite servicios como telepresencia avanzada, redes táctiles y conectividad universal.

4.5. Retos y oportunidades

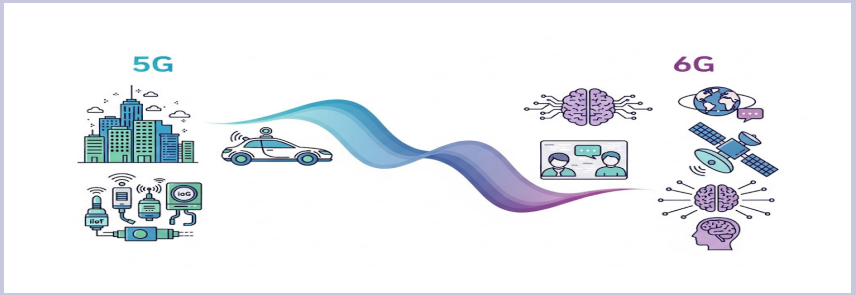
El despliegue de las nuevas redes móviles como 5G y 6G presenta retos y oportunidades. Por un lado, la infraestructura requiere una inversión masiva en nuevas estaciones base y fibra óptica

para garantizar una cobertura total. Por otro, la seguridad y la privacidad se vuelven cruciales ante el aumento de la hiperconectividad, ya que surgen nuevos riesgos cibernéticos. La inclusión digital es otro desafío fundamental. A medida que estas tecnologías se vuelven más avanzadas, existe el riesgo de que se amplíe la brecha digital, dejando atrás a las comunidades sin acceso. Superar estos retos es vital para aprovechar las oportunidades que estas redes de próxima generación ofrecen para un futuro más conectado.

Las tecnologías de acceso están diversificando la conectividad para superar las limitaciones geográficas y de infraestructura. Los satélites de órbita baja (LEO), como Starlink, están reduciendo la brecha digital en áreas remotas con menor latencia, aunque enfrentan el desafío de los residuos espaciales. Paralelamente, las redes comunitarias emergen como una solución sostenible y autogestionada, utilizando tecnología Wi-Fi mesh para conectar a comunidades sin servicio. En entornos urbanos y complejos, la tecnología PLC (Internet a través de la red eléctrica) aprovecha la infraestructura eléctrica existente para ofrecer conectividad de bajo costo, mientras que la fibra óptica continúa siendo el estándar de oro para la alta velocidad, complementada por tecnologías híbridas (FTTx) que la llevan más cerca del usuario. En situaciones de crisis, los drones y globos estratosféricos proporcionan soluciones de emergencia para restablecer la comunicación. Todas estas tecnologías, desde las redes gestionadas por la comunidad hasta las constelaciones de satélites, reflejan un esfuerzo global por hacer que la conectividad sea más accesible, fiable y resiliente.

Tabla. Tecnologías alternativas y de alta capacidad para la conectividad

Evolución de las redes móviles: del 5G al 6G



Tecnología	*Principio de Funcionamiento*	*Ventajas Principales*	*Desafíos y Limitaciones*
Satélites LEO	Pequeños satélites en órbita baja (500-2,000 km) que ofrecen cobertura global.	Menor latencia que satélites GEO, cobertura en zonas remotas y rurales, escalabilidad de la constelación.	Altos costos iniciales, posible congestión orbital, requiere terminales de usuario específicos.

Tecnología	*Principio de Funcionamiento*	*Ventajas Principales*	*Desafíos y Limitaciones*
Redes Comunitarias	Infraestructuras gestionadas por la propia comunidad con tecnologías como Wi-Fi mesh y antenas direccionales.	Adaptabilidad a necesidades locales, inclusión digital mediante la autogestión, uso de equipos reciclados para reducir costos.	Financiamiento limitado, necesidad de capacitación técnica local y de modelos de negocio sostenibles.
PLC (Power Line Communication)	Transmite datos a través de la red eléctrica existente, usando módems PLC.	Instalación rápida y de bajo costo, no requiere nuevo cableado, ideal para edificios históricos y zonas urbanas densas.	Interferencias eléctricas, alcance limitado y velocidad variable.
Drones y Globos	Plataformas aéreas que despliegan una red temporal en la estratósfera o a baja altura.	Despliegue rápido en situaciones de emergencia, cobertura temporal en zonas de desastre o eventos masivos, gran flexibilidad.	Regulación aérea compleja, duración limitada de la operación y costos operativos elevados.
Fibra Óptica y Tecnologías Híbridas	Transmite datos a través de pulsos de luz. Tecnologías híbridas como FTTx combinan fibra con otros medios.	Velocidades ultra altas (hasta 1 Tbps), baja latencia y alta fiabilidad, considerada el estándar de oro en conectividad fija.	Costo elevado de infraestructura, despliegue concentrado en áreas urbanas, desafío para llegar a zonas rurales.

Nota: Tecnologías alternativas y de alta capacidad que están expandiendo la conectividad más allá de las redes tradicionales, abordando desafíos de inclusión, costos y resiliencia en un panorama tecnológico en constante evolución.

4.6. Tendencias actuales

La era actual de las telecomunicaciones está definida por una convergencia sin precedentes de tecnologías y la creciente demanda de una conectividad ubicua y de alto rendimiento. Las tecnologías de acceso están en el epicentro de esta transformación, evolucionando rápidamente para satisfacer las expectativas de una sociedad cada vez más digitalizada. Si bien las redes fijas, con el despliegue masivo de la fibra óptica (FTTx), continúan siendo la columna vertebral de la banda ancha, las redes móviles (5G) han trascendido su papel tradicional. Hoy, el 5G no solo ofrece una velocidad sin precedentes, sino que su arquitectura flexible permite casos de uso tan diversos como el Internet de las Cosas (IoT) masivo, la telemedicina y la conducción autónoma, redefiniendo por completo el concepto de conectividad. El futuro de estas tecnologías apunta a una simbiosis. La industria se mueve hacia la convergencia del 5G y el Wi-Fi para ofrecer una experiencia de usuario fluida. Además, la inteligencia artificial (IA) y la computación perimetral (Edge Computing) están siendo integradas para optimizar la gestión de las redes, predecir fallos y reforzar la seguridad. En este contexto, las tecnologías de acceso no son solo un medio para la conexión, sino la base sobre la que se construyen las innovaciones del mañana.

Tabla. Tendencias de las tecnologías de acceso

Representación visual de la integración global de tecnológías emergentes en en telecomucaciones.

Tendencias actuales en tecnologías de acceso y su impacto futuro

Tendencia	*Ventajas Clave*	*Aplicaciones Actuales y Futuras*	*Proyección a Futuro*
Expansión de 5G y 6G	Velocidad ultra alta, latencia ultra baja, alta capacidad.	Streaming 8K, realidad aumentada/ virtual, telemedicina, fábricas inteligentes.	El 6G habilitará la "Internet de los sentidos" con interacción sensorial en tiempo real.
Proliferación de Satélites LEO	Cobertura global en zonas remotas, menor latencia que los satélites GEO.	Conectividad en regiones rurales y aisladas, internet en aviones y barcos, reducción de la brecha digital.	Más de 50,000 satélites en órbita para una conectividad omnipresente y de bajo costo.
Redes Inteligentes (IA)	Optimización y automatización de la red, predicción de fallos, asignación dinámica de recursos.	Gestión de red autónoma, seguridad proactiva contra ciberataques, mejora de la experiencia del usuario.	Las redes se gestionarán a sí mismas, volviéndose más eficientes, resilientes y seguras.
Inclusión Digital y Equidad	Acceso a la información y servicios esenciales para todos, sin importar la ubicación.	Programas de conectividad universal en escuelas y hospitales, apoyo a comunidades rurales, teletrabajo y educación a distancia.	El acceso a internet será considerado un derecho humano fundamental, con políticas que garanticen su disponibilidad global.

Tendencia	*Ventajas Clave*	*Aplicaciones Actuales y Futuras*	*Proyección a Futuro*
Sostenibilidad y Economía Circular	Menor impacto ambiental, uso eficiente de energía, reducción de residuos.	Infraestructuras energéticamente eficientes, reciclaje de equipos electrónicos, diseño de redes con materiales sostenibles.	La sostenibilidad se convertirá en un pilar del diseño y la gestión de redes, con énfasis en el impacto ambiental y social.
Personalización y Flexibilidad	El usuario puede elegir y combinar tecnologías según sus necesidades (híbrido).	Combinación de fibra óptica para el hogar con 5G para movilidad, uso de satélite en zonas sin cobertura terrestre.	El usuario tendrá un control total sobre su conectividad, mezclando tecnologías para una experiencia óptima y adaptada.
Seguridad y Privacidad	Protección de datos, gestión de riesgos en entornos de alta conectividad.	Nuevas estrategias de seguridad para dispositivos IoT y redes críticas, protocolos avanzados de encriptación.	La seguridad será un componente integral del diseño de la red, con defensas automatizadas y proactivas para la protección de la infraestructura.

Nota: Convergencia de redes avanzadas (5G/6G, LEO), inteligencia artificial, inclusión digital y sostenibilidad, configurando el futuro de la conectividad global.

4.7. Referencias y recursos adicionales

En la actualidad, el campo de las tecnologías de acceso está en constante evolución, impulsado por la demanda de una conectividad ubicua y de alto rendimiento. Las redes de próxima generación, como el 5G, han transformado la comunicación móvil. Este salto cualitativo se basa en una arquitectura flexible que utiliza la virtualización de funciones de red (NFV) y el "network slicing". Esto habilita el Internet de las Cosas (IoT), la telemedicina y la conducción autónoma. El futuro de estas redes se dirige hacia el 6G, que buscará integrar la inteligencia artificial (IA) a nivel de red para la comunicación holográfica y la computación perimetral. Más allá de las redes móviles, otras tecnologías están revolucionando el acceso. Los satélites de órbita baja (LEO), como Starlink y OneWeb, están llevando internet de baja latencia a zonas remotas, reduciendo la brecha digital. Sin embargo, su despliegue masivo plantea desafíos como la gestión de residuos espaciales. Las redes comunitarias, que usan tecnologías como Wi-Fi mesh, ofrecen una alternativa sostenible y autogestionada para comunidades sin acceso, promoviendo la inclusión digital.

La fibra óptica sigue siendo el estándar de oro en redes fijas, con velocidades de más de 1 Gbps y alta fiabilidad, aunque su despliegue es costoso. Las tecnologías híbridas (FTTx) combinan fibra y otros medios para extender su alcance. Finalmente, las tecnologías de nicho, como los drones y globos estratosféricos, ofrecen soluciones de emergencia, y el PLC (Internet por red eléctrica) aprovecha

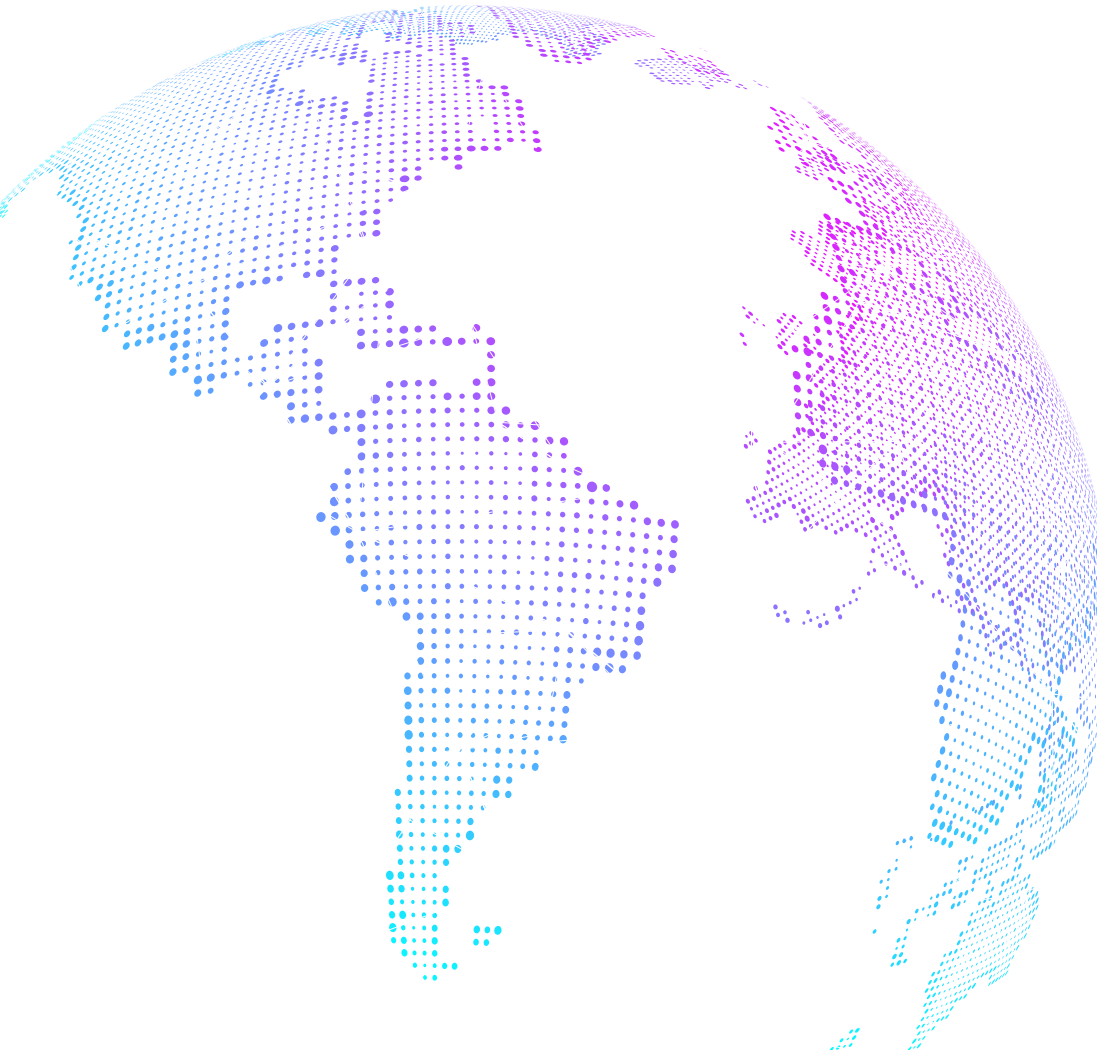
la infraestructura existente para la conectividad en entornos densos. Todos estos avances reflejan una tendencia hacia redes más inteligentes, seguras y personalizadas. Para las personas que están interesados en profundizar en el tema de las tecnologías de acceso, los siguientes recursos ofrecen información técnica, análisis de tendencias y perspectivas sobre la evolución de las redes de telecomunicaciones.

Tabla. Recursos y Referencias Clave sobre Tecnologías de Acceso

Tipo de Recurso	***Descripción***	***Ejemplos***
Organizaciones y Empresas	Entidades que definen estándares, gestionan redes o investigan nuevas tecnologías.	UIT, Starlink, OneWeb, Internet Society, Community Networks Group, Project Loon
Publicaciones y Bases de Datos	Fuentes académicas y de la industria para estudios técnicos, informes y análisis de mercado.	IEEE Xplore, informes de la GSMA, consultoras como Deloitte
Material Educativo	Libros, cursos y conferencias que ofrecen una comprensión estructurada del tema.	Libros de William Stallings y Alberto Leon-Garcia, cursos en Coursera y edX, TED Talks y webinars de la UIT
Unión Internacional de Telecomunicaciones (UIT): https://www.itu.int Informes, estándares y estadísticas globales.	Starlink: https://www.starlink.com Información sobre cobertura y tecnología satelital.	OneWeb: https://oneweb.net Proyectos de conectividad rural.
IEEE Xplore: https://ieeexplore.ieee.org Artículos científicos sobre 5G, PLC, fibra óptica y tecnologías emergentes.	Internet Society: https://www.internetsociety.org Recursos sobre inclusión digital y redes comunitarias.	Community Networks Group: https://communitynetworks.group Guías y estudios de caso sobre redes comunitarias.
Project Loon: https://loon.com Información sobre globos estratosféricos para conectividad.	Libros recomendados: Stallings, William. “Redes de Telecomunicaciones”. Leon-Garcia, Alberto. “Fundamentos de Redes de Comunicaciones”. Castells, Manuel. “La era de la información: economía, sociedad y cultura”.	Videos y conferencias: TED Talks sobre inclusión digital. Webinars de la UIT sobre tendencias tecnológicas.

Nota: Principales organizaciones, bases de datos y recursos educativos que sirven como referencias clave para el estudio de las tecnologías de acceso.

CAPÍTULO V
REDES DE NUEVA GENERACIÓN



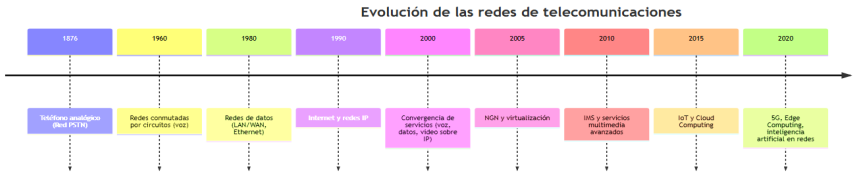
CAPÍTULO V

REDES DE NUEVA GENERACIÓN

5.1. Introducción

En este capítulo abordaremos en primera instancia la línea cronológica de la evolución de las redes convergentes especialmente las de nueva generación. Las redes de telecomunicación han evolucionado desde sus inicios como se presenta en la siguiente cronología resumida:

Figura 41. Evolución de las redes de telecomunicaciones



En síntesis, se puede destacar tres momentos importantes inicialmente, las redes eran analógicas y dedicadas a la voz (PSTN), para luego continuar en los 80 y 90, en donde aparecen las redes de datos (LAN/WAN) y posterior la convergencia con Internet. Desde los 2000, las redes evolucionan hacia la integración de servicios y la virtualización, dando paso a NGN, IMS, IoT, 5G y Edge Computing.

La convergencia de redes se puede definir como la integración de diferentes servicios de comunicación (voz, datos, video) sobre una única infraestructura y protocolo, generalmente IP. Esto permite que empresas y usuarios accedan a múltiples servicios usando la misma red física y lógica, optimizando recursos, costos y gestión.

5.2. Arquitectura

La arquitectura de convergencia de redes es el diseño que permite integrar múltiples servicios (voz, datos, video y aplicaciones multimedia) sobre una única infraestructura de red, generalmente basada en el protocolo IP. Esta convergencia elimina la necesidad de redes separadas para cada servicio, optimizando recursos y facilitando la administración.

Componentes técnicos fundamentales
Red de acceso unificada

Tecnologías como fibra óptica (FTTH), xDSL, cable coaxial, WiFi y redes móviles (4G/5G) permiten la conexión de usuarios y dispositivos a la red convergente.

Red de transporte multiservicio

Basada en IP/MPLS, esta capa transporta todo tipo de tráfico (voz, video, datos) usando mecanismos de calidad de servicio (QoS) para priorizar aplicaciones sensibles a la latencia.

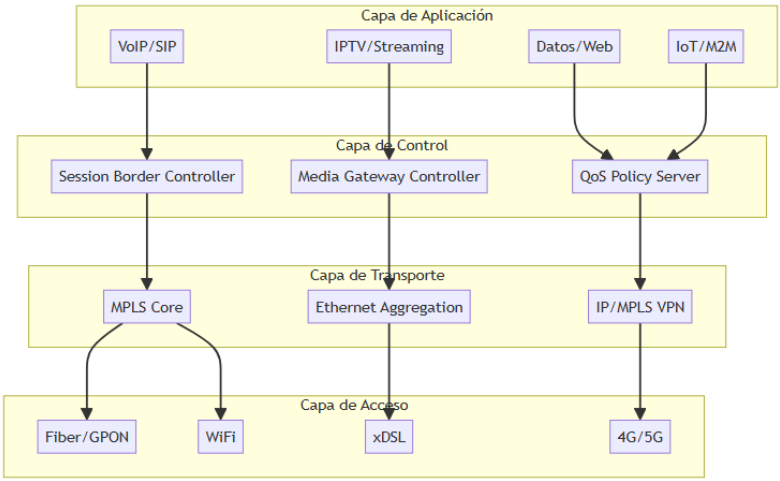
Plataforma de servicios

Incluye servidores de aplicaciones (VoIP, videollamadas, IPTV, mensajería) y sistemas de control de sesión como IMS (IP Multimedia Subsystem).

Planos de control y gestión

Utilizan protocolos de señalización (SIP, H.323) y plataformas de gestión centralizada para garantizar la orquestación eficiente de todos los servicios.

Figura 42. Arquitectura técnica de convergencia de redes.



5.3. Características de la convergencia de redes

Figura 43. Convergencia de redes

Ejemplo: Triple play o un proveedor de servicio que ofrece: telefonía VoIP, IPTV e Internet sobre fibra óptica.

Dentro de las ventajas más importantes de la convergencia de redes se puede mencionar:

- Optimización de recurso, un solo backbone para todos los servicios.
- Reducción de gastos operativos, menos infraestructura.
- Mejor administración de la red.
- Flexibilidad y escalabilidad para añadir nuevos servicios y tecnologías.

NGN e IMS

Las Redes de Nueva Generación (NGN) y el Subsistema Multimedia IP (IMS) representan la evolución más avanzada en la arquitectura de las telecomunicaciones modernas. Ambos conceptos responden a la necesidad de integrar múltiples servicios (voz, datos, video, mensajería) sobre una infraestructura única, flexible y basada en el protocolo IP.

5.4. NGN (Next Generation Networks)

Las NGN son redes basadas en paquetes (principalmente IP), diseñadas para transportar voz, datos y multimedia de manera eficiente y flexible., sobre una infraestructura común.

Componentes principales:

- Red de acceso (fibra, cobre, inalámbrica).
- Plano de transporte: Basado en IP/MPLS.
- Plano de control: Protocolos de señalización como SIP, H.323.
- Plano de servicios: Plataformas de aplicaciones y servidores multimedia (VoIP, IPTV, etc.).

Figura 44. Principios redes NGN

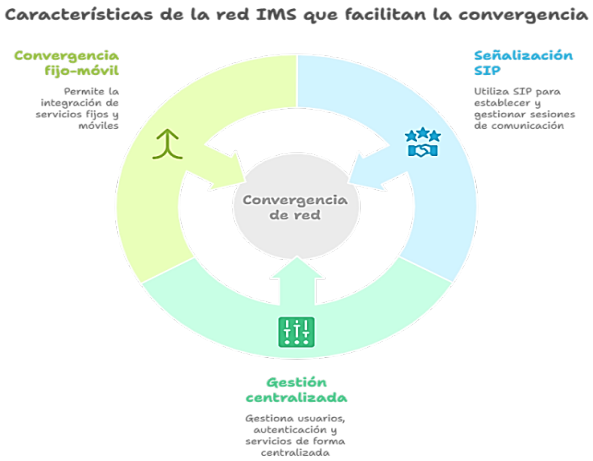
IMS (IP Multimedia Subsystem)

El IMS es una arquitectura estandarizada por 3GPP que opera sobre NGN y soporta la gestión de servicios multimedia avanzados. Es una arquitectura de control de sesión/servicio. IMS utiliza protocolos como IETF como SIP para el control de sesiones, permitiendo la convergencia de servicios tradicionales (telefonía) y nuevos (videollamadas, mensajería instantánea) sobre redes IP.

5.4.1. Componentes principales:

- Núcleo de IMS: P-CSCF/S-CSCF/I-CSCF elementos de control de sesión SIP. P-CSCF o función de control de llamada proxy es el punto de entrada en el mundo. S-CSCF o Función de control de sesión de llamada servidora es el punto de anclaje a la red doméstica. I-CSCF o función de control de sesión de llamada interrogante que proporciona ocultamiento de topología. MS (Servidor de Medios), que hospeda recursos especiales. MGF (Puente de Medios) para interoperar con redes heredadas. PDF (Función de Decisión de Políticas) para Control de QoS utilizando Políticas (COPS)
- Capa de aplicación IMS: HSS (Home Subscriber Server): Base de datos centralizada de usuarios. AS ((Application Server Function), para hospedar aplicaciones.
- Sistema final de IMS (Cliente IMS), importante en los servicios multimedia/IMS.

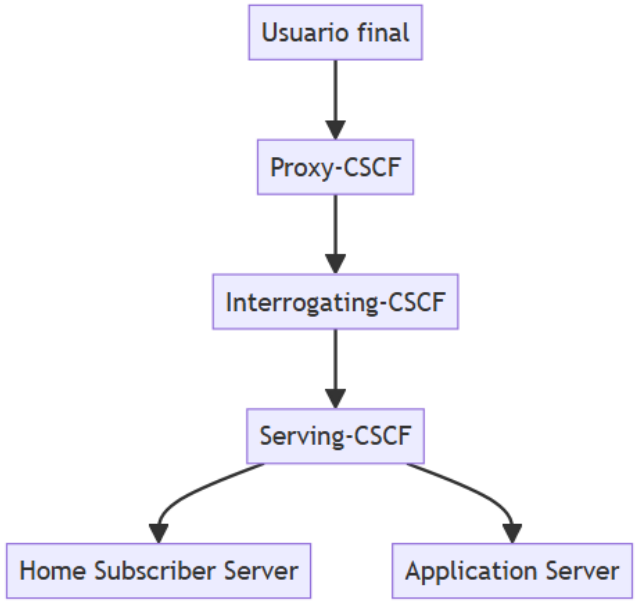
Figura 45. Características arquitectura IMS



5.4.2. Funcionamiento técnico

IMS utiliza SIP para la señalización y control de sesiones multimedia, permitiendo autenticación, autorización y provisión de servicios avanzados.

Figura 46: Funcionamiento técnico IMS



Ejemplo:

Llamadas VoIP, videollamadas, mensajería instantánea sobre LTE/5G.

Tabla. Tabla comparativa NGN e IMS

Aspecto	*NGN (Next Generation Networks)*	*IMS (IP Multimedia Subsystem)*
Definición	Plataforma de red multiservicio basada en IP/MPLS que separa transporte y servicios.	Arquitectura estándar para gestión de servicios multimedia sobre IP, definida por 3GPP.
Propósito	Integrar voz, datos y video en una sola infraestructura.	Facilitar la provisión y control de servicios multimedia avanzados.
Plano de transporte	IP/MPLS, Ethernet, ATM, etc.	IP (sobre NGN), depende de la infraestructura subyacente.
Plano de control	Protocolos de señalización (SIP, H.323, MGCP).	SIP (principal), Diameter, Cx, Sh, etc.
Servicios soportados	Voz, datos, video, IPTV, mensajería, IoT.	Voz sobre IP, videollamadas, mensajería instantánea, presencia, conferencias.
Gestión de usuarios	Integración con sistemas de autenticación y billing.	HSS (Home Subscriber Server) para autenticación y perfil de usuario.

Aspecto	*NGN (Next Generation Networks)*	*IMS (IP Multimedia Subsystem)*
Escalabilidad	Alta, permite agregar nuevos servicios y tecnologías.	Muy alta, arquitectura modular y orientada a servicios.
Interoperabilidad	Entre redes fijas, móviles y diferentes tecnologías.	Entre redes móviles y fijas, soporta portabilidad y roaming.
Control de sesiones	General, depende del servicio implementado.	Centralizado, mediante CSCF (Call Session Control Function).
Estandarización	ITU-T, ETSI, IETF.	3GPP, ETSI, IETF.
Aplicación actual	Backbone de operadores, transición a 4G/5G, IoT.	Servicios multimedia avanzados, VoLTE, Rich Communication Services (RCS).

NGN proporciona la infraestructura de transporte y acceso para todos los servicios. IMS se monta sobre NGN y gestiona los servicios multimedia, controlando sesiones, usuarios y aplicaciones. El usuario final accede a los servicios a través de la red de acceso y transporte, recibiendo aplicaciones avanzadas ofrecidas por IMS

5.5. Virtualización

La virtualización de redes es el proceso de abstraer las funciones de red del hardware físico y ejecutarlas como software sobre servidores estándar, creando recursos virtuales (servidores, redes, almacenamiento) sobre infraestructuras físicas, permitiendo múltiples redes virtuales independientes, optimizando recursos y permitiendo una mayor flexibilidad en el diseño, administración y escalabilidad en las redes.

De forma puntual las ventajas de la virtualización de las redes las podemos enumerar a continuación:

- ***Flexibilidad:*** Permite crear, modificar o eliminar redes virtuales sin afectar el hardware físico.
- ***Aislamiento:*** Las redes virtuales pueden operar de manera independiente, garantizando seguridad y privacidad.
- ***Optimización de recursos:*** Mejor aprovechamiento del hardware disponible.
- ***Automatización y gestión centralizada:*** Facilita la administración mediante software.
- ***Escalabilidad:*** Permite adaptar la red rápidamente a nuevas necesidades o cargas de trabajo.

5.5.1. Tipos de virtualización

Existen varios enfoques y tecnologías para la virtualización de redes, los principales son:

Figura 47. ¿Qué tipo de virtualización de red debería implementarse?

De igual forma, se podrían mencionar algunos ejemplos puntuales de cada tipo de virtualización, estos se observan en la tabla 2.

Tabla. Ejemplos tipos de virtualización de red

Tipo de virtualización de red	*Ejemplo*
Virtualización de Red a Nivel de Hardware	Virtual Routing and Forwarding (VRF) en routers, que permite múltiples tablas de enrutamiento independientes en el mismo equipo.
Virtualización de Red basada en Software	Software Defined Networking (SDN), donde el control de la red se separa del hardware y se gestiona mediante controladores centralizados.
Virtualización de Red a Nivel de Host	Virtual switches en plataformas de virtualización como VMware vSphere o Microsoft Hyper-V.
Redes Virtuales Privadas (VPN)	VPN basadas en IPsec, MPLS VPN.
Virtualización de Funciones de Red (NFV)	Un firewall virtual que corre en una máquina virtual en vez de un dispositivo dedicado.

A continuación, se va a profundizar en dos tipos principales de virtualización de redes SDN y NFV.

Virtualización de redes (SDN y NFV)

SDN (Software Defined Networking)

SDN es una arquitectura de red que separa el plano de control (donde se toman las decisiones de enrutamiento y gestión) del plano de datos (donde se procesan y encaminan los paquetes). Esto se

logra mediante un controlador centralizado, generalmente implementado en software, que administra y programa el comportamiento de los dispositivos de red físicos y virtuales.

Dentro de las características principales se puede mencionar:

- Separación de planos: El plano de control está centralizado en el controlador SDN, mientras que el plano de datos reside en los dispositivos de red.
- Programabilidad: Permite modificar el comportamiento de la red mediante software, facilitando la automatización y la adaptación dinámica.
- Visibilidad y gestión centralizada: El controlador SDN tiene una visión global de la red, optimizando la gestión y el monitoreo.

En este contexto es evidente mencionar que dispone de ciertas ventajas como:

- Flexibilidad y agilidad: Cambios rápidos en la topología y políticas de red.
- Automatización: Reducción de tareas manuales y errores humanos.
- Optimización de recursos: Mejor uso del ancho de banda y de los dispositivos.

Un ejemplo de uso de SDN puede ser la implementación de políticas de seguridad, calidad de servicio (QoS) o balanceo de carga de manera dinámica y centralizada, realizada por un operador, sin la necesidad de reconfigurar manualmente cada dispositivo.

NFV (Network Function Virtualization)

NFV es una tecnología que virtualiza funciones de red tradicionalmente implementadas en hardware dedicado (como firewalls, routers, balanceadores de carga), permitiendo ejecutarlas como software sobre servidores estándar. Esto transforma la infraestructura de red en un entorno más flexible y escalable.

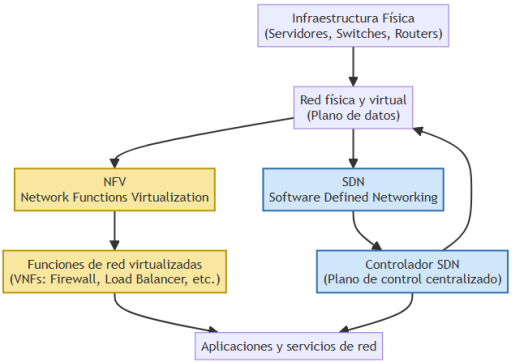
- Dentro de sus características más importantes se puede mencionar:
- Desacoplamiento de funciones: Las funciones de red se ejecutan como instancias virtuales (VNFs) sobre hardware generalista.
- Escalabilidad: Fácil despliegue y escalado de funciones según demanda.
- Reducción de costos: Menor dependencia de hardware propietario y reducción de gastos operativos.

En este contexto resulta evidente mencionar algunas de sus ventajas:

- Agilidad en el despliegue: Nuevos servicios pueden implementarse rápidamente.
- Eficiencia: Consolidación de múltiples funciones en menos equipos.
- Innovación: Facilita la introducción de nuevos servicios y actualizaciones.

Un ejemplo de uso puede ser el despliegue de un firewall virtual en minutos para un nuevo cliente, sin necesidad de instalar un dispositivo físico en el sitio.

Figura 48. Relación y diferencia entre SDN y NFV



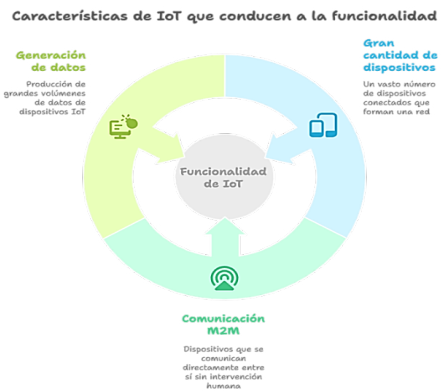
5.6. IoT (Internet of Things) y 5G

En la era de conectividad e intercambio de información dos tecnologías han evolucionado de manera acelerada. Estas han transformado la manera como interactuamos con las personas y con el mundo, lo mencionado hace referencia a las redes 5G y los dispositivos IoT. La combinación de ambas permite impulsar la automatización, la eficiencia y la creación de nuevos servicios en sectores industriales, de la salud, transporte y hogar.

El IoT es un paradigma tecnológico que consiste en la interconexión de objetos físicos (sensores, actuadores, electrodomésticos, vehículos) a través de la red (internet), permitiendo recopilar, intercambiar, visualizar y analizar datos (información). Estos dispositivos pueden interactuar de forma autónoma o coordinada mejorando la toma de decisiones y la eficiencia en múltiples ámbitos.

Las características principales del IoT se enfocan en la conectividad entre dispositivos y sistemas centralizados, sensores y actuadores para captar información y ejecutar acciones, automatización y escalabilidad de pocos hasta millones.

Figura 49. Características de IoT que conducen a la funcionalidad



Existen varias ventajas al utilizar esta tecnología (IoT), dentro de las cuales podemos mencionar: optimización de recursos, mejora en la calidad de vida sobre todo en ámbitos como hogares, salud, servicios, etc. Incremento de la productividad a nivel industrial y logística. Por último, se puede mencionar el auge de nuevos modelos de negocio, basados en datos y mantenimiento preventivo.

Así mismo, aún tiene algunos desafíos que hay que tener en cuenta, como es la seguridad de ellos datos, interoperabilidad sobre todo con dispositivos de diferentes fabricantes y la gestión de grandes volúmenes de datos.

Los protocolos y arquitecturas:

- Redes LPWAN (LoRa, Sigfox, NB-IoT): Bajo consumo y largo alcance.
- Gateways IoT: Conectan sensores a la red IP.
- Plataformas de gestión: AWS IoT, Azure IoT Hub.

Existen varios campos de aplicación como: salud, industria, agricultura, ciudades inteligentes, domótica.

5.6.1. 5G

El 5G es a quinta generación de redes móviles, diseñada para soportar altas velocidades de transmisión, baja latencia y gran cantidad de dispositivos conectados. Se puede considerar como la base tecnológica para el despliegue masivo de IoT, vehículos autónomos, realidad aumentada y aplicaciones críticas en tiempo real.

Dentro de las características principales de la red 5G se puede mencionar: alta velocidad, generalmente 10 Gbs superando ampliamente a las redes 4G, baja latencia con tiempos de respuesta menores a 1ms, gran capacidad de conexión por kilómetro cuadrado, y alta eficiencia energética.

Figura 50. Características de las redes 5G

En este contexto es evidente las ventajas de las redes 5G, las cuales se mencionan a continuación:

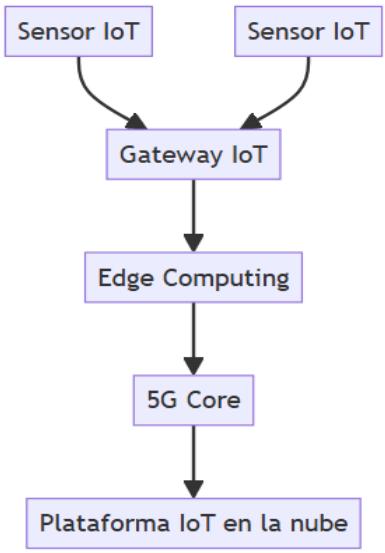
- Soporte para IoT masivo: Conexión eficiente de sensores y dispositivos en ciudades inteligentes, fábricas, agricultura, etc.
- Vehículos autónomos y comunicaciones críticas: Respuesta en tiempo real para seguridad y movilidad.
- Experiencias inmersivas: Realidad aumentada/virtual, streaming de alta calidad.
- Telemedicina: Cirugías remotas, monitoreo médico en tiempo real.

Aunque existen varias ventajas, también existen desafíos como la necesidad del cambio de la infraestructura, la seguridad y privacidad y normativas de regulación y compatibilidad de frecuencias que aun necesitan ser abordados y resueltos.

5.6.2. Aspectos técnicos:

- MIMO masivo: Uso de múltiples antenas para mejorar la capacidad.
- Beamforming: Direccionamiento inteligente de señales.
- Network Slicing: Segmentación de la red para diferentes aplicaciones (IoT, video, misión crítica).
- Baja latencia (<1 ms): Crucial para aplicaciones en tiempo real.

Figura 51. Relación entre el IoT y 5G



5G es la plataforma ideal para IoT masivo, soportando millones de dispositivos por km^2 y aplicaciones en tiempo real como ciudades inteligentes, vehículos autónomos y más.

Juntas, estas tecnologías están dando forma a la próxima revolución digital.

5.7. Edge Computing

El Edge Computing (Computación en el borde) es un paradigma de procesamiento de datos que traslada la computación, el almacenamiento y análisis de datos desde centros de datos centralizados hacia el borde de la red, cerca de donde estos datos son generados. Esto responde a la necesidad de

procesas grandes volúmenes de datos en tiempo real, reducir la latencia y optimizar el uso de la banda, especialmente en aplicaciones como el IoT.

En resumen, se puede decir que el Edge Computing surge debido al crecimiento exponencial de dispositivos conectados y las demandas en tiempo real, teniendo en consideración que tradicionalmente todos los datos generados por estos dispositivos se envían a servidores centrales, causando latencia elevada, consumo de ancho de banda, aumento de riesgo en el transporte de datos sensibles.

5.7.1. Arquitectura de Edge Computing

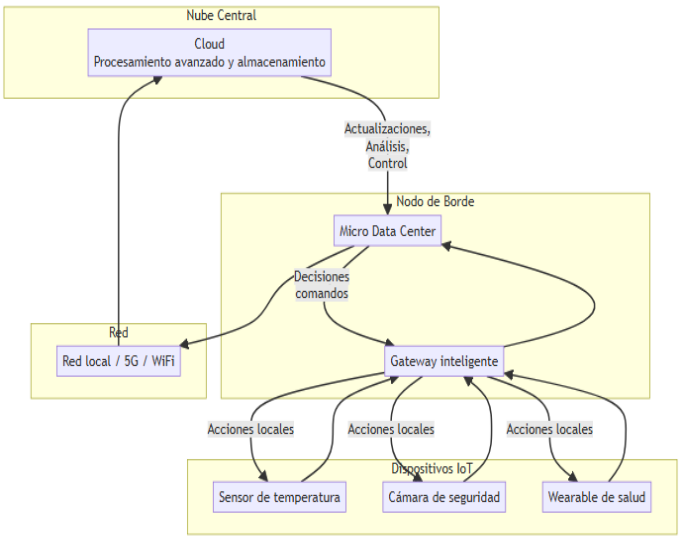
El Edge Computing tiene estructura a varios niveles:

Dispositivos de borde (Edge): Equipos que generan y pueden procesar los datos localmente como sensores, cámaras, routers, gateways, etc.

Nodos de borde (Edge nodes): Equipos con capacidad de cómputo y almacenamientos ubicados cerca de los dispositivos finales como gateways inteligentes, micro data centers, etc.

Cloud central: centros de datos tradicional encargado de procesamiento intensivo, almacenamiento a largo plazo y análisis avanzado de los datos.

Figura 52. Arquitectura del Edge Computing.



Dentro de las características importantes del Edge Computing se tiene: procesamiento local, reducción de latencia, optimización del ancho de banda, escalabilidad y mejora de la privacidad.

Figura 53. Explorando las dimensiones del Edge computing.

Ventajas:

- Reducción de latencia (respuesta más rápida).
- Menor tráfico hacia la nube.
- Ahorro en ancho de banda.
- Mayor seguridad y privacidad (datos procesados localmente).
- Respuesta en tiempo real.
- Ahorro de costos asociados ya que disminuye el tráfico hacia la nube.

Sin embargo, a pesar de las innumerables ventajas, aún existen desafíos a considerar como la coordinación de múltiples nodos de borde, actualizaciones, seguridad, interoperabilidad sobre todo en sistemas de diferentes fabricantes, escalabilidad y fiabilidad a medida que crece el número de dispositivos.

Aplicaciones:

- Vehículos autónomos: decisiones instantáneas para evitar accidentes.
- IoT industrial: sensores industriales, ciudades inteligentes y agricultura con precisión.
- Salud digital: Monitoreo de pacientes y respuestas inmediatas en caso de emergencia.
- Video vigilancia: Análisis de imágenes y alertas locales.

5.7.2. Laboratorio y ejercicio

Red Convergente con VoIP y Datos en Packet Tracer

Objetivo

Configurar una red que integre servicios de datos (Internet) y voz (VoIP) usando Cisco Packet Tracer. Los usuarios podrán navegar y realizar llamadas IP entre sí.

Dispositivos a utilizar

1 Router (2811)

1 Switch (2960)

2 PCs

2 Cisco IP Phone 7960 (VoIP)

Diseño de VLANs

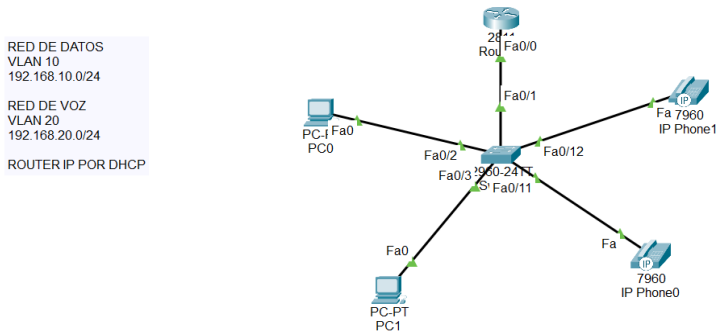
VLAN 10: Datos (PCs)

VLAN 20: Voz (IP Phones)

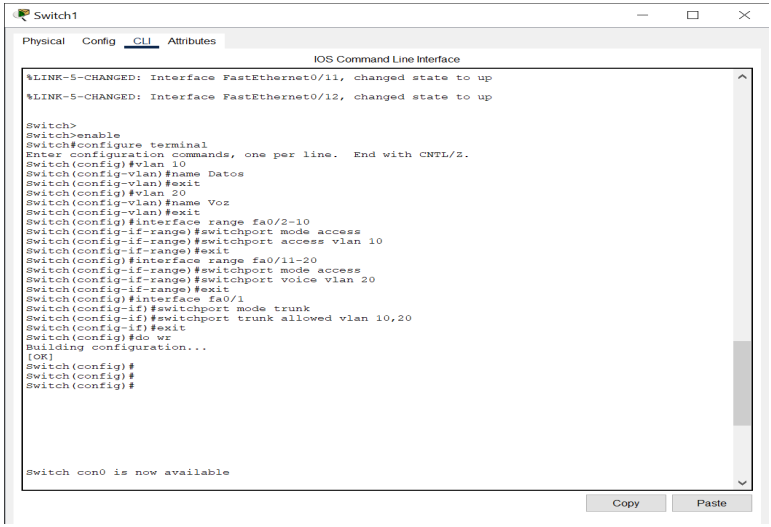
Conecta los dispositivos:

- Router Fa0/0 conectado al Switch (puerto Fa0/1).
- IP Phones conectados al switch (puertos Fa0/11 y Fa0/12).
- PCs conectados al switch (puertos Fa0/2 y Fa0/3).

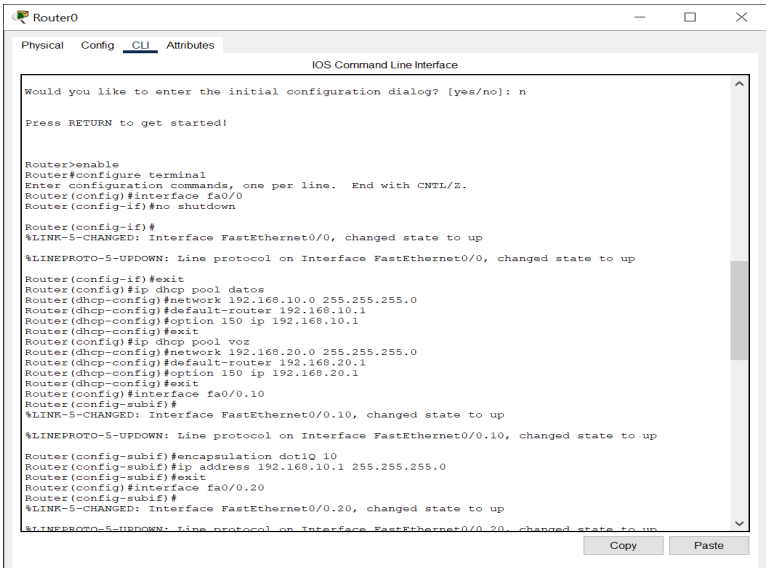
Figura 54. Conexión Red Convergente con VoIP y Datos en Packet Tracer

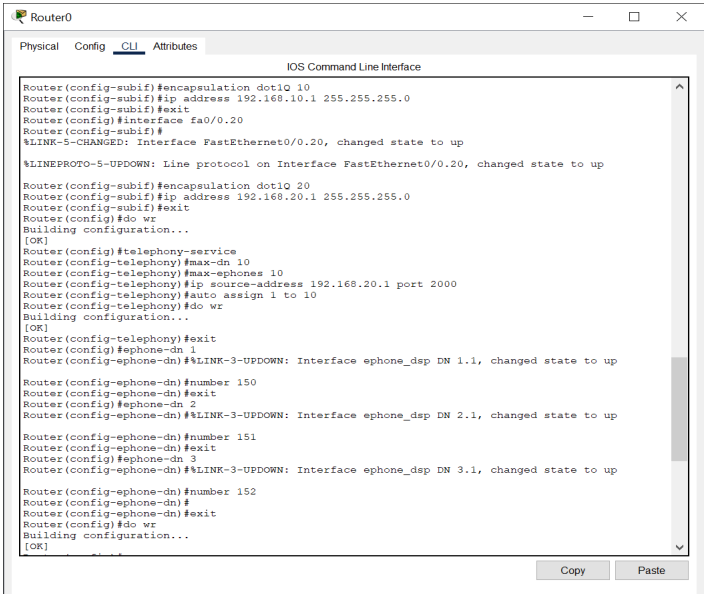


Configuración del switch



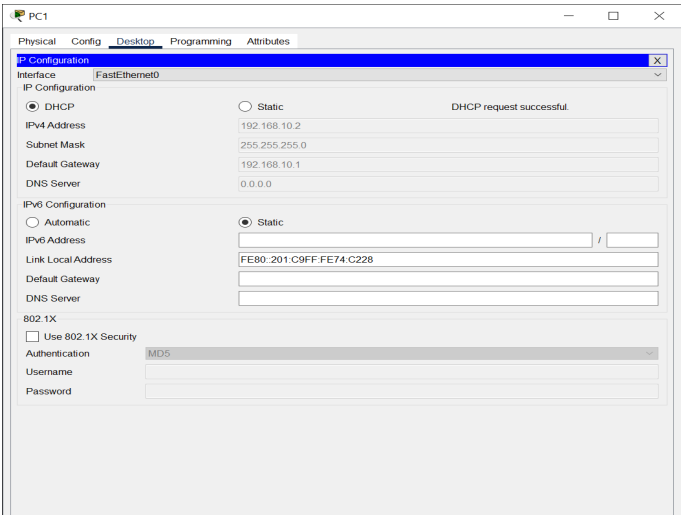
Configuración del router





PCs y teléfonos IP

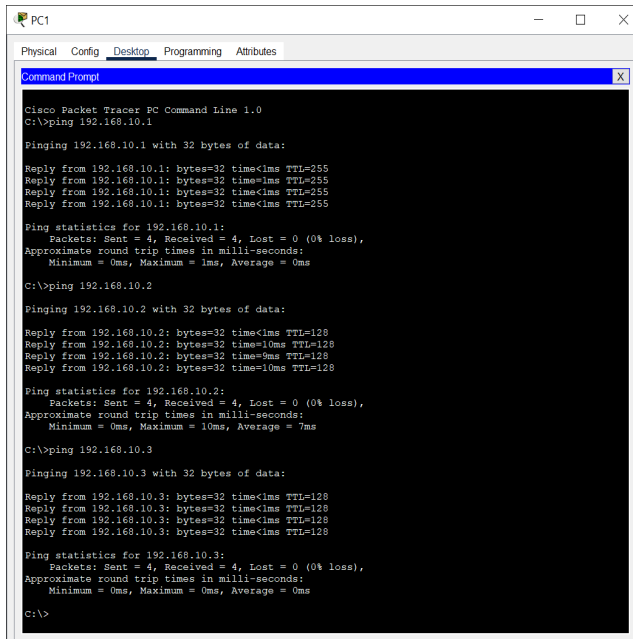
- Haz clic en cada PC.
- Ve a Desktop – IP Configuration
- Selecciona DHCP
- Verifica que la IP este en el rango 192.168.10...



- Haz clic en cada teléfono IP
- Conecta los teléfonos

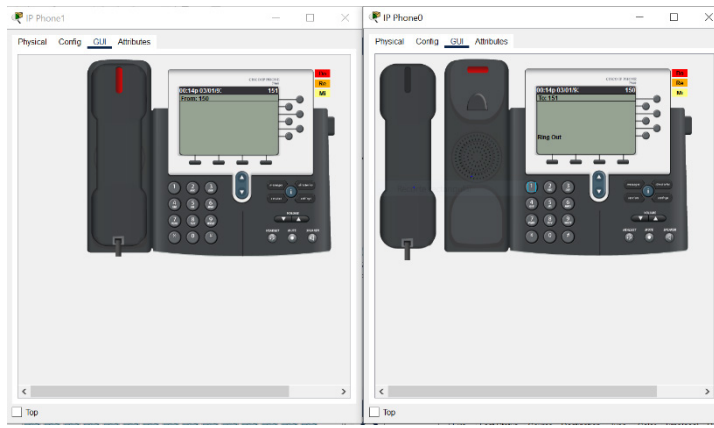
Verificación y pruebas

- Desde las PCs:
    - Ve a Desktop-Command Prompt y ejecuta:
    - Ping 192.168.10.1 (router)
    - Ping 192.168.10.3 (PC)



- Desde los teléfonos IP:
    - Marca la extensión del otro teléfono: (desde el 150 llama al 151)

Verificación Teléfonos IP



5.8. Ejemplos reales

- ***Telefónica y Movistar:*** Ofrecen triple play (Internet, TV, telefonía) sobre redes convergentes NGN.
- Enlace: *movistar.es/fibra-optica/*
- ***Amazon Web Services (AWS):*** Proporciona servicios de edge computing (AWS Greengrass) para procesamiento local de datos IoT.
- Enlace: *Inteligencia en la periferia de IoT - AWS IoT Greengrass - AWS*
- ***Smart Cities:*** Ciudades como Barcelona usan IoT y 5G para gestión inteligente de tráfico, alumbrado y residuos.
- Enlace: *Barcelona Smart City: Conoce el proyecto | Cloudworks*

Tendencias actuales

- ***Redes definidas por software (SDN):*** Control y automatización centralizada.
- ***Virtualización de funciones de red (NFV):*** Reducción de hardware dedicado.
- ***Inteligencia Artificial y Machine Learning:*** Automatización de gestión y seguridad.
- ***Redes 5G y 6G:*** Mayor velocidad, menor latencia y más dispositivos conectados.
- ***Ciberseguridad avanzada:*** Protección contra amenazas en entornos virtualizados y distribuidos.
- ***Redes orientadas a servicios (Service-Oriented Networks):*** Flexibilidad y personalización de servicios.
- ***Integración de IoT y Edge Computing:*** Procesamiento distribuido y aplicaciones inteligentes.
- ***Sostenibilidad:*** Redes energéticamente eficientes y ecológicas.

5.9. Referencias y recursos adicionales

"SDN and NFV Simplified" – Jim Doherty

Webs y artículos:

Cisco: Next Generation Networks

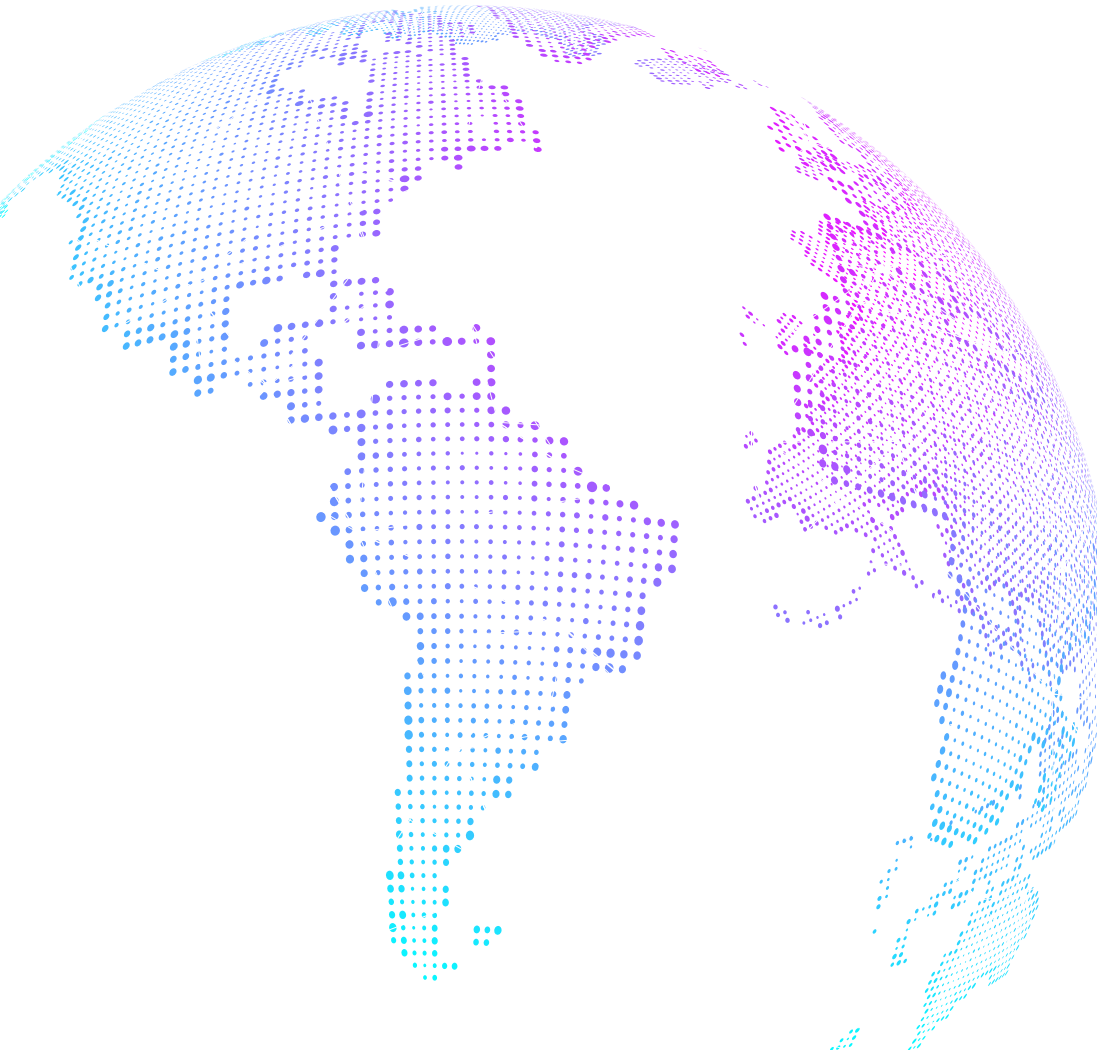
IEEE IoT Journal

5G Americas

Open Networking Foundation

Videos y cursos: *YouTube: "¿Qué es Edge Computing?"*

CAPÍTULO VI
REDES EMPRESARIALES



CAPÍTULO VI

REDES EMPRESARIALES

6.1. Diseño de Redes Corporativas

Es un proceso fundamental para cualquier organización que busque optimizar su infraestructura tecnológica, garantizar la conectividad, la seguridad y la escalabilidad de sus operaciones. Una red corporativa bien diseñada no solo permite la comunicación eficiente entre los distintos departamentos de una empresa, sino que también soporta aplicaciones críticas, el almacenamiento de datos y servicios en la nube. Este proceso implica la planificación, implementación y gestión de una infraestructura que integra hardware, software y protocolos de comunicación para satisfacer las necesidades específicas de la organización.

El diseño de una red corporativa implica la integración de diversos componentes hardware y software que trabajan en conjunto para garantizar el funcionamiento eficiente de la infraestructura. Entre los dispositivos más importantes se encuentran los routers, que conectan diferentes redes y enrutan el tráfico entre ellas, siendo esenciales para la conectividad entre sucursales o para acceder a Internet. Los switches, por su parte, conectan dispositivos dentro de una red local (LAN) y gestionan el tráfico de datos entre ellos, asegurando que la información llegue a su destino de manera eficiente. Los firewalls son otro componente crítico, ya que protegen la red contra amenazas externas mediante la filtración del tráfico entrante y saliente, mientras que los access points (AP) facilitan la conectividad inalámbrica (Wi-Fi) en la red.

Además de los dispositivos de red, los servidores desempeñan un papel central en la infraestructura corporativa. Estos equipos alojan aplicaciones, bases de datos y servicios críticos, y pueden ser físicos o virtuales, dependiendo de las necesidades de la organización. El cableado estructurado, que incluye fibra óptica y Ethernet, constituye la base física de la red y debe ser diseñado para soportar altas velocidades y volúmenes de datos. Por último, el software de gestión, como herramientas de monitoreo y sistemas de seguridad, es esencial para supervisar el rendimiento de la red, detectar fallos y proteger los datos de la empresa.

6.1.1. Principios de Diseño de Redes Corporativas

Para garantizar que una red corporativa sea eficiente, segura y escalable, es necesario seguir ciertos principios de diseño. Uno de los más importantes es la escalabilidad, que implica que la red debe poder crecer junto con la organización. Esto significa elegir equipos y tecnologías que permitan la expansión sin necesidad de reemplazar toda la infraestructura. La confiabilidad es otro principio clave, ya que la red debe ser resistente a fallos. Esto se logra mediante la implementación de redundancia, como enlaces de respaldo y servidores en clúster, así como protocolos de recuperación rápida.

La seguridad es un aspecto crítico en el diseño de redes corporativas. Las medidas de seguridad incluyen la implementación de firewalls, la encriptación de datos, la autenticación de usuarios y políticas de acceso estrictas. Además, el desempeño de la red debe estar garantizado, lo que implica una planificación adecuada del ancho de banda y la calidad de servicio (QoS) para manejar el tráfico

esperado sin cuellos de botella. Por último, la facilidad de gestión de una red bien diseñada debe ser fácil de administrar y monitorear, lo que reduce los costos operativos y mejora la eficiencia.

El diseño de redes corporativas requiere la adopción de mejores prácticas para garantizar su éxito. Una de las primeras etapas es la planificación y el análisis de requisitos, que implica realizar un estudio detallado de las necesidades de la organización. Esto incluye el número de usuarios, las aplicaciones críticas, los requisitos de ancho de banda y los planes de crecimiento. Una vez definidos estos aspectos, es recomendable segmentar la red en VLANs o subredes, lo que mejora la seguridad y el rendimiento al aislar el tráfico sensible y reducir la congestión.

La implementación de redundancia es otra práctica esencial, ya que garantiza la disponibilidad de la red en caso de fallos.

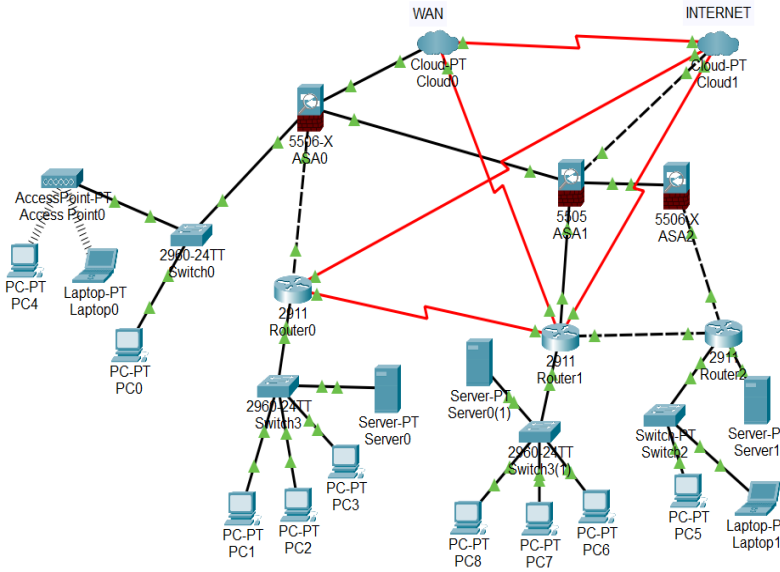
6.1.2. Desafíos comunes en el diseño de redes corporativas

A pesar de los avances tecnológicos, el diseño de redes corporativas enfrenta varios desafíos. Uno de los más significativos es la seguridad cibernética, ya que las amenazas están en constante evolución y requieren una actualización continua de las medidas de protección. La integración de tecnologías heterogéneas también representa un reto, ya que la coexistencia de equipos y soluciones de diferentes fabricantes puede complicar la gestión de la red. Además, el aumento del tráfico de datos, especialmente con el uso de aplicaciones en la nube y videoconferencias, puede saturar la red si no se planifica adecuadamente el ancho de banda.

Otro desafío importante es el cumplimiento normativo, ya que las redes corporativas deben ajustarse a regulaciones específicas, como el GDPR en Europa o el HIPAA en Estados Unidos. Estas normativas añaden complejidad al diseño y requieren que las organizaciones implementen controles adicionales para proteger la privacidad y la seguridad de los datos. Finalmente, la gestión del cambio es un aspecto que no debe subestimarse, ya que la implementación de nuevas tecnologías o la expansión de la red pueden generar resistencia por parte de los usuarios y requerir capacitación adicional.

El diseño de redes corporativas es un proceso complejo pero esencial para el éxito de cualquier organización. Una red bien diseñada no solo mejora la productividad y la colaboración, sino que también protege los activos digitales de la empresa. Al seguir principios como la escalabilidad, la confiabilidad, la seguridad y el desempeño, y al adoptar las mejores prácticas, las organizaciones pueden construir redes robustas que soporten sus operaciones actuales y futuras. Sin embargo, es importante estar preparado para enfrentar los desafíos que surgen en el camino, desde la seguridad cibernética hasta la gestión del ancho de banda. En última instancia, una red corporativa eficiente es un pilar fundamental para la transformación digital y la competitividad en el mundo empresarial actual.

En la siguiente figura se puede ver una topología de una red corporativa o empresarial, en donde existen redundancia para un mejor funcionamiento de la red y evitar que colapse en momentos de tráfico.



6.2. Modelo jerárquico de redes

A diferencia del modelo OSI, el modelo jerárquico está compuesto de 3 capas, cada una de ellas tiene funciones específicas y pueden trabajar de forma independiente. Este modelo tiene un enfoque organizacional que se basa en la estructuración de elementos en niveles o capas. Es ampliamente utilizado en diversas disciplinas, como la administración de empresas, informática, biología, ingeniería, entre otras. Su principal característica es la organización de elementos en una estructura de árbol, donde existe un elemento raíz que se divide en subelementos, los cuales a su vez pueden tener sus propias subdivisiones.

El modelo jerárquico se caracteriza por varias propiedades clave que lo distinguen de otros enfoques organizacionales. En primer lugar, la estructura en forma de árbol es una de sus características más destacadas. Esta estructura permite una representación visual clara de las relaciones entre los elementos, lo que facilita la comprensión y el análisis. Además, el modelo jerárquico es altamente ordenado, ya que cada elemento tiene una posición definida dentro de la jerarquía. Además, es escalable, lo que significa que puede adaptarse a organizaciones o sistemas de diferentes tamaños y complejidades. Sin embargo, esta escalabilidad tiene limitaciones, ya que la estructura rígida del modelo puede dificultar la incorporación de nuevas relaciones o elementos que no se ajusten a la jerarquía predefinida.

Al utilizar el modelo jerárquico se tiene varios beneficios, entre ellos se tiene:

- ***Escalabilidad mejorada:*** Facilita el crecimiento de la red. Permite agregar nuevos elementos sin afectar el diseño existente.
- ***Redundancia optimizada:*** Ofrece múltiples rutas para el tráfico. Garantiza alta disponibilidad.
- ***Rendimiento superior:*** Reduce la latencia y mejora la velocidad de conmutación.

- ***Seguridad fortalecida:*** Permite implementar políticas por capas. Facilita el aislamiento de amenazas.
- ***Administración simplificada:*** Facilita el diagnóstico de problemas. Permite mantenimiento modular

Consideraciones de Diseño

a. Separación de funciones:
   - Cada capa cumple roles específicos.
   - Evita sobrecarga de responsabilidades.

b. Modularidad:
   - Permite cambios independientes por capa.
   - Facilita actualizaciones y mantenimiento.

c. Flexibilidad:
   - Adaptable a diferentes tamaños de red.
   - Permite fusionar capas en redes pequeñas.

Recomendaciones de Implementación

a. Planificación cuidadosa:
   - Analizar requisitos actuales y futuros.
   - Considerar crecimiento potencial.

b. Documentación detallada:
   - Mantener registros de configuraciones.
   - Documentar políticas y procedimientos.

c. Monitoreo continuo:
   - Supervisar rendimiento por capa.
   - Identificar cuellos de botella.

d. Actualizaciones graduales:
   - Implementar cambios por fases.
   - Realizar pruebas exhaustivas.

El modelo jerárquico proporciona una estructura organizada y eficiente para el diseño de redes empresariales, facilitando la gestión, el mantenimiento y la escalabilidad de la infraestructura de red. Además, se basa en la idea de que los elementos pueden organizarse en una estructura de niveles, donde cada nivel tiene una relación clara y definida con los niveles superiores e inferiores. Esta estructura se asemeja a un árbol, donde el elemento raíz es el punto de partida y las ramas representan las subdivisiones.

6.2.1. Aplicaciones del Modelo Jerárquico en Redes de Datos

El modelo jerárquico de redes encuentra su aplicación en diversos sectores, adaptándose eficientemente a las necesidades específicas de cada organización. En el ámbito empresarial, este modelo permite una estructuración óptima de las comunicaciones corporativas, facilitando la separación efectiva entre departamentos mediante VLANs y garantizando una gestión centralizada del tráfico de red. Las grandes corporaciones con múltiples sedes se benefician particularmente de esta arquitectura, ya que permite una distribución organizada de servicios y recursos a través de diferentes ubicaciones.

En el sector educativo, la implementación del modelo jerárquico resulta fundamental para gestionar las complejas necesidades de comunicación en universidades y escuelas. Este enfoque permite separar eficientemente las redes administrativas de las académicas, garantizando un acceso controlado a recursos educativos mientras se mantiene la seguridad de la información institucional. Además, facilita la administración de laboratorios informáticos y bibliotecas digitales, asegurando una experiencia educativa fluida tanto para estudiantes como para docentes.

El sector salud representa otro campo donde el modelo jerárquico demuestra su valor estratégico. En hospitales y clínicas, la arquitectura permite aislar las redes médicas críticas, protegiendo datos sensibles de pacientes y garantizando el funcionamiento ininterrumpido de equipos médicos conectados. La capacidad de priorizar el tráfico de emergencia y mantener la confidencialidad de los historiales clínicos se vuelve crucial en estos entornos donde la vida de los pacientes puede depender de la eficiencia de las comunicaciones.

En instituciones financieras, la implementación del modelo jerárquico cobra especial relevancia debido a los altos requerimientos de seguridad y confiabilidad. Los bancos y aseguradoras utilizan esta arquitectura para separar sus redes transaccionales, implementar múltiples capas de seguridad en operaciones financieras y mantener redundancia en servicios críticos. La protección de datos de clientes y la gestión de servicios en línea se benefician significativamente de esta estructura organizada.

El sector gubernamental aprovecha el modelo jerárquico para gestionar sus complejas redes de comunicación. Las oficinas públicas requieren una segmentación efectiva por departamentos y un control riguroso del acceso a recursos estatales. Los servicios de emergencia, en particular, dependen de esta arquitectura para garantizar la priorización de comunicaciones críticas y mantener la redundancia en servicios esenciales para la comunidad.

En plantas de producción, el modelo permite separar las redes de control industrial del tráfico administrativo, facilitando el monitoreo de procesos y la gestión de inventarios. Los almacenes logísticos pueden mantener sistemas automatizados eficientes mientras gestionan aspectos críticos como el control de condiciones ambientales y la logística de distribución.

Se puede decir que el modelo jerárquico es una herramienta poderosa para organizar elementos en una estructura clara y ordenada. Su simplicidad, eficiencia y claridad en las relaciones de dependencia lo hacen ideal para aplicaciones en diversos campos, desde la administración de empresas hasta la biología y la informática. Sin embargo, su rigidez y dificultad para representar relaciones complejas limitan su aplicabilidad en contextos dinámicos o altamente interconectados.

6.2.2. Las Capas de la Red Jerárquica: Estructura y Funcionalidad

La red jerárquica es un modelo de diseño de redes que organiza los dispositivos y funciones de la red en capas o niveles, cada uno con responsabilidades específicas. Este enfoque permite una gestión más eficiente, escalabilidad y facilidad de mantenimiento, ya que divide la red en segmentos lógicos que pueden ser diseñados, implementados y gestionados de manera independiente. El modelo de red jerárquica es ampliamente utilizado en el diseño de redes corporativas y de gran escala, y se compone tradicionalmente de tres capas principales: la capa de núcleo (core), la capa de distribución (distribution) y la capa de acceso (access). A continuación, se explica en detalle cada una de estas capas, su función y su importancia en la estructura general de la red.

La capa superior es la de Núcleo (Core Layer), tiene las siguientes características:

- Representa el backbone de alta velocidad de la red.
- Proporciona conmutación de paquetes ultra rápida.
- No realiza manipulación de paquetes (como filtrado).
- Debe ser altamente confiable y redundante.
- Se optimiza para máxima disponibilidad y rendimiento.
- Ejemplo de dispositivos en la capa de núcleo: Routers de alta capacidad. Switches de capa 3 (Layer 3 switches) diseñados para manejar grandes volúmenes de tráfico.

Características de la Capa de Núcleo:

- ***Alta velocidad:*** Utiliza enlaces de alta capacidad, como fibra óptica, para garantizar un rendimiento óptimo.
- ***Redundancia:*** Implementa múltiples rutas y dispositivos para evitar puntos únicos de fallo.
- ***Simplicidad:*** Evita funciones complejas, como filtrado o enrutamiento avanzado, para mantener la velocidad.
- ***Conectividad:*** Conecta la capa de distribución y, en redes grandes, puede interconectar múltiples edificios o campus.

La capa intermedia es la de Distribución (Distribution Layer), tiene las siguientes funciones:

- Implementa políticas de red.
- Realiza enrutamiento entre VLANs.
- Define dominios de broadcast.
- Proporciona servicios de seguridad y filtrado.
- Gestiona la calidad de servicio (QoS).
- Su función principal es agrupar el tráfico proveniente de los dispositivos de la capa de acceso y dirigirlo de manera eficiente hacia la capa de núcleo. Además, esta capa implementa políticas de red, como control de acceso, filtrado de tráfico y enrutamiento entre VLANs (Virtual LANs).
- Ejemplo de dispositivos en la capa de distribución: Switches de capa 3 (Layer 3 switches) con capacidades de enrutamiento. Firewalls para aplicar políticas de seguridad.

Características de la Capa de Distribución:

- ***Agregación de tráfico:*** Consolida el tráfico de múltiples dispositivos de la capa de acceso antes de enviarlo al núcleo.
- ***Políticas de red:*** Aplica reglas de seguridad, calidad de servicio (QoS) y control de acceso.
- ***Enrutamiento:*** Realiza el enrutamiento entre VLANs y subredes.
- ***Resiliencia:*** Proporciona redundancia y equilibrio de carga para garantizar la disponibilidad de la red.

La capa de Acceso (Access Layer) tiene las siguientes características:

- Punto de conexión para dispositivos finales.
- Responsabilidades principales:
    - Controla el acceso de usuarios y dispositivos a la red.

    - Agrupa usuarios en segmentos de red.
    - Implementa seguridad de puerto.
    - Establece VLANs.
    - Aplica PoE (Power over Ethernet) cuando se requiere.
- Características de la Capa de Acceso:
    - ***Conectividad de usuarios:*** Proporciona puertos Ethernet o Wi-Fi para conectar dispositivos finales.
    - ***Segmentación:*** Divide el tráfico en VLANs para mejorar la seguridad y el rendimiento.
    - ***Control de acceso:*** Implementa políticas para restringir el acceso a la red.
    - ***Simplicidad:*** Está diseñada para ser fácil de implementar y gestionar.

Ejemplo de dispositivos en la capa de acceso: Switches de capa 2 (Layer 2 switches). Puntos de acceso inalámbrico (Wireless Access Points, WAPs).

Ventajas del Modelo de Red Jerárquica

El modelo de red jerárquica ofrece varias ventajas clave:

- ***Escalabilidad:*** Permite agregar nuevos dispositivos o segmentos de red sin afectar el diseño general.
- ***Facilidad de gestión:*** Cada capa tiene responsabilidades claras, lo que simplifica la administración y la resolución de problemas.
- ***Rendimiento optimizado:*** La separación de funciones reduce la congestión y mejora la eficiencia del tráfico.
- ***Seguridad:*** Las políticas de red pueden implementarse de manera centralizada en la capa de distribución.
- ***Redundancia y resiliencia:*** La estructura jerárquica permite la implementación de redundancia en cada capa, mejorando la disponibilidad de la red.

Desafíos del Modelo de Red Jerárquica

A pesar de sus ventajas, el modelo de red jerárquica también presenta algunos desafíos:

- ***Costo:*** La implementación de múltiples capas y dispositivos especializados puede ser costosa.
- ***Complejidad inicial:*** El diseño y la configuración de una red jerárquica requieren planificación y conocimientos adecuados de la persona que está a cargo de la red.
- ***Rigidez:*** En algunos casos, la estructura jerárquica puede limitar la flexibilidad para adaptarse a cambios drásticos en los requisitos de la red.

6.3. Redes de Área Local Virtual (VLAN)

La administración y estructuración de las redes contemporáneas ha experimentado una transformación radical gracias a la tecnología VLAN. Este avance tecnológico permite dividir una red física en múltiples segmentos lógicos independientes, superando las limitaciones de las configuraciones de red tradicionales. El desarrollo de las VLAN fue impulsado principalmente por la demanda de mayor adap-

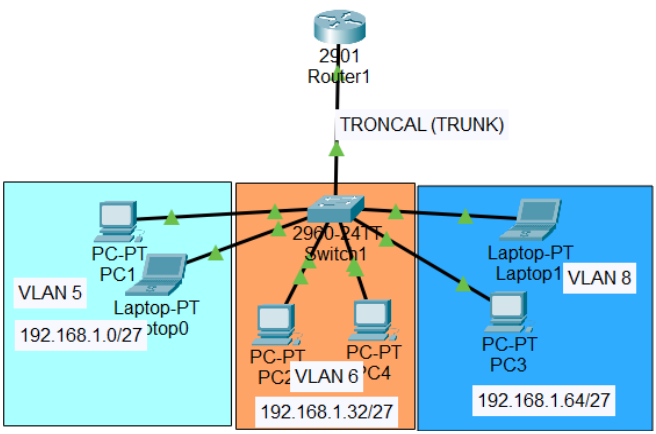
tabilidad y protección en los entornos de red corporativos, donde la disposición física de los equipos frecuentemente no coincide con las necesidades operativas de la empresa.

El dinamismo del sector empresarial moderno exige soluciones de red versátiles y eficaces, un requisito que las VLAN satisfacen perfectamente. Al posibilitar la creación de redes lógicas independientes sobre una única infraestructura física, esta tecnología mejora significativamente tanto la administración de los recursos como el desempeño general de la red. Esta capacidad de crear divisiones virtuales resulta particularmente beneficiosa en situaciones donde el control del flujo de datos y la ciberseguridad son aspectos críticos. Por ejemplo, se puede dividir en VLANs dependiendo de los departamentos, oficinas, áreas y se les da seguridad dependiendo de los datos o información que maneje.

Desde sus inicios, la tecnología VLAN ha experimentado constantes mejoras y actualizaciones para adaptarse a los requerimientos cada vez más exigentes de la conectividad moderna. En el presente, las VLAN han trascendido su función original de segregación de tráfico de red, convirtiéndose en componentes esenciales para la implementación de estrategias de seguridad, la maximización del rendimiento y la distribución efectiva de los recursos de red.

Fundamentos de las VLAN

Dentro de la arquitectura del modelo OSI, específicamente en su segunda capa (enlace de datos), encontramos la operatividad de las VLAN. Esta tecnología permite una notable innovación: transformar un único switch físico en múltiples unidades lógicas independientes. Gracias a esta funcionalidad, los profesionales encargados de la gestión de redes pueden establecer zonas de broadcast independientes en una misma estructura física, logrando una segmentación que tradicionalmente requería inversiones significativas en hardware como switches físicos adicionales o enrutadores.



En la figura anterior se puede ver que existen 3 VLAN que salen de un mismo switch, cada una de ellas tiene diferentes IP, máscara y Gateway que van acorde a las necesidades. Para que se pueda pasar datos entre subredes es necesario conectarse a un router mediante un puerto troncal; si no se hace este paso se podrá pasar información solo entre los dispositivos de cada VLAN, pero no entre todas.

El protocolo IEEE 802.1Q constituye una parte importante para el funcionamiento de las VLAN, estableciendo un método para la identificación de tramas. Este protocolo especifica las modificacio-

nes necesarias en las tramas Ethernet, incorporando identificadores que señalan la pertenencia a una VLAN específica. Durante el procesamiento de datos, cuando una trama alcanza un switch habilitado con tecnología VLAN, el equipo analiza estos identificadores para determinar su VLAN correspondiente y aplica el conjunto de políticas y reglas previamente definidas para dicha red virtual.

La gestión eficiente del tráfico en las VLAN se logra mediante sofisticadas tablas de correspondencia implementadas en los switches compatibles. Estas tablas establecen la relación entre los puertos físicos del dispositivo y las diferentes VLAN configuradas en el sistema. Este mecanismo permite una toma de decisiones ágil y precisa sobre el manejo de cada trama recibida: ya sea dirigiéndola exclusivamente hacia puertos asociados a la misma VLAN, o preservando la información de etiquetado en los enlaces troncales para su posterior procesamiento en otros switches de la infraestructura.

6.3.1. Beneficios de las VLAN

Utilizar las VLANs en las redes de datos empresariales puede incluir los siguientes beneficios:

- Fortalecimiento de la Protección en Red. La arquitectura VLAN incorpora capas adicionales de protección mediante la creación de perímetros virtuales entre distintos sectores de usuarios y recursos informáticos. Esta segmentación virtual no solo minimiza las posibilidades de intrusiones no deseadas, sino que también facilita la aplicación de protocolos de seguridad adaptados a cada sector. Un aspecto fundamental de esta protección radica en que la comunicación entre VLANs distintas requiere obligatoriamente la intervención de dispositivos de la capa 3 (router o switch de nivel de red), permitiendo así un control minucioso y adecuado del flujo de información entre los diferentes segmentos virtuales.
- Maximización de la eficiencia operativa. El diseño basado en VLANs revoluciona el rendimiento de las redes al establecer límites efectivos para los dominios de broadcast. A diferencia de las configuraciones tradicionales, donde las transmisiones broadcast saturaban toda la infraestructura, la tecnología VLAN confina estas comunicaciones dentro de segmentos específicos.
- Adaptabilidad y capacidad de crecimiento. La versatilidad destaca como uno de los atributos más valiosos de la tecnología VLAN. Los especialistas en redes pueden estructurar las conexiones basándose en criterios operativos y funcionales, superando las restricciones físicas tradicionales. Esta característica facilita la adaptación dinámica de la infraestructura de red ante cambios organizacionales, sin requerir modificaciones en el hardware existente. La capacidad de crear nuevas VLANs o ajustar las configuraciones actuales según la evolución de las necesidades empresariales demuestra la notable escalabilidad de esta solución.
- Optimización de la Inversión. La adopción de VLANs representa una estrategia efectiva para la optimización de recursos financieros en el ámbito de las redes empresariales. Al eliminar la necesidad de adquirir equipamiento adicional para la segmentación de red, se reduce significativamente la inversión inicial en infraestructura. Adicionalmente, la gestión centralizada que permite esta tecnología disminuye considerablemente los gastos operativos relacionados con el mantenimiento y la administración de la red.

6.3.2. Tipos de VLAN

VLAN de Datos: Fundamentos y Aplicaciones en Redes Modernas

Las VLAN de Datos constituyen un componente esencial en la arquitectura de redes contemporáneas, representando el tipo más común y fundamental de red virtual. Estas estructuras lógicas se diseñan específicamente para gestionar el tráfico regular de usuarios finales, estableciendo un entorno controlado para la transmisión de información cotidiana en entornos empresariales.

La VLAN de Datos se distingue por varios atributos específicos:

a. Propósito Principal
- Gestión del tráfico cotidiano de usuarios
- Transmisión de información empresarial regular
- Soporte para aplicaciones comerciales estándar
- Manejo de comunicaciones departamentales

b. Estructura Operativa
- Configuración como VLAN predeterminada en muchos casos
- Separación lógica del tráfico administrativo y especial
- Priorización adaptada a necesidades comerciales
- Gestión eficiente del ancho de banda asignado

Implementación Estratégica

La configuración de VLAN de Datos requiere una planificación cuidadosa que considere:

a. Aspectos Organizacionales
- Distribución departamental de la empresa
- Patrones de comunicación entre grupos
- Requisitos específicos de cada área
- Proyecciones de crecimiento futuro

b. Consideraciones Técnicas
- Capacidad de los switches disponibles
- Ancho de banda necesario
- Políticas de calidad de servicio (QoS)
- Requisitos de seguridad específicos

Beneficios Específicos

La implementación de VLAN de Datos aporta ventajas significativas:

1. Optimización Operativa
- Mejora en la gestión del tráfico regular
- Reducción de la congestión en la red
- Mayor eficiencia en las comunicaciones diarias
- Simplificación de la administración de recursos

2. Seguridad Mejorada
   - Aislamiento efectivo del tráfico entre departamentos
   - Control preciso sobre los accesos a recursos
   - Protección reforzada de datos sensibles
   - Monitoreo simplificado de actividades
3. Flexibilidad Administrativa
   - Adaptación ágil a cambios organizacionales
   - Gestión simplificada de recursos de red
   - Facilidad para implementar modificaciones
   - Escalabilidad mejorada

Mejores Prácticas de Configuración

Para optimizar el funcionamiento de las VLAN de Datos, se recomienda:

1 Planificación Inicial
   - Análisis detallado de necesidades departamentales
   - Documentación exhaustiva de la estructura
   - Definición clara de políticas de acceso
   - Establecimiento de protocolos de gestión
2. Implementación Técnica
   - Configuración precisa de puertos y enlaces
   - Establecimiento de prioridades de tráfico
   - Definición de políticas de seguridad
   - Documentación detallada de la configuración

Consideraciones de Mantenimiento

El mantenimiento efectivo de las VLAN de Datos requiere:

1. Monitoreo Continuo
   - Supervisión del rendimiento
   - Análisis de patrones de tráfico
   - Detección temprana de problemas
   - Ajustes proactivos de configuración
2. Gestión Activa
   - Actualización regular de políticas
   - Optimización de recursos asignados
   - Adaptación a nuevas necesidades
   - Mantenimiento de la documentación

Integración con otras VLAN

La interacción con otros tipos de VLAN debe considerar:

1. Aspectos de Comunicación
   - Políticas de enrutamiento entre VLANs

- Gestión de permisos de acceso
- Control de tráfico interdepartamental
- Priorización de servicios críticos

2. Aspectos de Seguridad
   - Establecimiento de barreras lógicas
   - Control de acceso entre segmentos
   - Monitoreo de comunicaciones inter-VLAN
   - Implementación de políticas de filtrado

Las VLAN de Datos representan un componente fundamental en la arquitectura de redes empresariales modernas. Su implementación adecuada no solo mejora la eficiencia operativa y la seguridad, sino que también proporciona la flexibilidad necesaria para adaptarse a las cambiantes necesidades organizacionales. La planificación cuidadosa, junto con una gestión continua y efectiva, garantiza que estas redes virtuales cumplan su función como base de las comunicaciones empresariales cotidianas.

VLAN de Voz: Arquitectura Especializada para Comunicaciones de Telefonía IP

Las VLAN de Voz representan una implementación especializada dentro de las redes virtuales, diseñada específicamente para gestionar y optimizar el tráfico de telefonía IP. Esta segmentación dedicada resulta fundamental para garantizar la calidad y confiabilidad de las comunicaciones de voz en entornos empresariales modernos.

Características distintivas:

1. Priorización del Tráfico
   - Gestión preferencial de paquetes de voz
   - Asignación garantizada de ancho de banda
   - Reducción efectiva de la latencia
   - Control optimizado de la fluctuación (jitter)
2. Configuración Especializada
   - Etiquetado específico de tramas de voz
   - Implementación de QoS (Calidad de Servicio) dedicada
   - Separación lógica del tráfico de datos
   - Asignación de prioridades en switches

Beneficios Fundamentales

La implementación de VLAN de Voz ofrece ventajas significativas:

1. Calidad de Servicio Mejorada
   - Minimización de interrupciones en llamadas
   - Reducción de eco y distorsión
   - Claridad optimizada en comunicaciones
   - Estabilidad en conexiones de voz
2. Gestión Eficiente
   - Administración simplificada de recursos

- Monitoreo específico del tráfico de voz
- Control preciso de la capacidad de red
- Resolución ágil de problemas

3. Seguridad Reforzada
   - Aislamiento del tráfico de voz
   - Protección contra interferencias
   - Control de acceso específico
   - Encriptación dedicada

Implementación Técnica

La configuración de VLAN de Voz requiere consideraciones específicas:

1. Planificación Inicial
   - Evaluación de necesidades de telefonía
   - Dimensionamiento de capacidad
   - Análisis de infraestructura existente
   - Definición de políticas de QoS
2. Configuración de Equipamiento
   - Programación de switches compatibles
   - Configuración de teléfonos IP
   - Establecimiento de enlaces troncales
   - Implementación de políticas de priorización

Consideraciones de Diseño

Aspectos críticos para una implementación exitosa:

1. Infraestructura
   - Switches con soporte para QoS
   - Capacidad adecuada de procesamiento
   - Enlaces de alta velocidad
   - Redundancia en conexiones críticas
2. Políticas de Red
   - Definición de prioridades de tráfico
   - Establecimiento de anchos de banda garantizados
   - Configuración de VLANs auxiliares
   - Protocolos de seguridad específicos

Optimización del Rendimiento

Estrategias para maximizar la eficiencia:

1. Monitoreo Continuo
   - Análisis de calidad de llamadas
   - Medición de latencia y jitter
   - Evaluación de uso de ancho de banda
   - Detección temprana de problemas

2. Ajustes Proactivos
    - Optimización de configuraciones
    - Actualización de políticas QoS
    - Balanceo de cargas
    - Mejoras en seguridad

Integración con Sistemas Existentes

Aspectos clave para la interoperabilidad:

1. Compatibilidad
    - Coordinación con otras VLANs
    - Integración con sistemas de datos
    - Conexión con infraestructura legacy
    - Adaptación a estándares existentes
2. Escalabilidad
    - Planificación de crecimiento
    - Adaptabilidad a nuevas tecnologías
    - Flexibilidad en configuraciones
    - Capacidad de expansión

Recomendaciones para una gestión efectiva:

1. Documentación
    - Registro detallado de configuraciones
    - Mapeo de recursos asignados
    - Procedimientos de mantenimiento
    - Protocolos de resolución de problemas
2. Mantenimiento Preventivo
    - Actualizaciones regulares de firmware
    - Pruebas periódicas de calidad
    - Verificación de seguridad
    - Optimización continua

Consideraciones de Seguridad

Aspectos críticos para la protección:

1. Control de Acceso
    - Autenticación de dispositivos
    - Restricción de conexiones no autorizadas
    - Monitoreo de actividades sospechosas
    - Políticas de seguridad específicas
2. Protección de Datos
    - Encriptación de comunicaciones
    - Segmentación efectiva del tráfico

- Prevención de interceptaciones
- Auditorías regulares

Las VLAN de Voz constituyen un componente esencial en las comunicaciones empresariales modernas, proporcionando la base necesaria para servicios de telefonía IP confiables y de alta calidad. Su implementación adecuada requiere una planificación cuidadosa, considerando aspectos técnicos, operativos y de seguridad. La atención a los detalles en la configuración, junto con un mantenimiento proactivo, garantiza un servicio de comunicaciones de voz eficiente y confiable en entornos empresariales.

VLAN Nativa: Fundamentos y Aplicaciones en Enlaces Troncales

La VLAN nativa es particularmente importante para mantener la compatibilidad con dispositivos que no soportan el etiquetado 802.1Q. Sin embargo, por razones de seguridad, muchos administradores optan por cambiar la VLAN nativa de su valor predeterminado (VLAN 1) y limitar su uso para reducir posibles vulnerabilidades.

También representa un concepto fundamental en la arquitectura de redes conmutadas, específicamente en la configuración de enlaces troncales. Esta VLAN especial cumple una función única en el manejo de tramas sin etiquetar, estableciendo un mecanismo esencial para la compatibilidad y el funcionamiento eficiente de las conexiones troncales.

Características Fundamentales

1. Definición Técnica
   - VLAN predeterminada para tramas sin etiquetas
   - Componente esencial en enlaces troncales
   - Procesamiento especial de tramas IEEE 802.1Q
   - Identificador único en cada puerto troncal
2. Comportamiento Distintivo
   - Transmisión de tramas sin etiquetas
   - Recepción de tráfico no etiquetado
   - Procesamiento automático de frames
   - Gestión especial en interfaces troncales

Funcionalidad Principal

La VLAN Nativa opera bajo principios específicos:

1. Gestión de Tramas
   - Procesamiento de frames sin etiqueta 802.1Q
   - Asignación automática a la VLAN predeterminada
   - Manejo especial en puertos troncales
   - Preservación de compatibilidad con dispositivos legacy
2. Operación en Enlaces Troncales
   - Facilitación de comunicaciones entre switches

- Mantenimiento de compatibilidad entre dispositivos
- Gestión eficiente del tráfico no etiquetado
- Soporte para equipos sin capacidad de etiquetado

Consideraciones de Implementación

Aspectos críticos para una configuración adecuada:

1. Planificación
   - Selección apropiada del ID de VLAN
   - Consistencia en toda la red
   - Documentación detallada
   - Evaluación de requisitos de seguridad
2. Configuración Técnica
   - Asignación de VLAN ID consistente
   - Verificación de compatibilidad
   - Establecimiento de políticas de seguridad
   - Pruebas de conectividad

Mejores Prácticas de Seguridad

Recomendaciones para una implementación segura:

1. Protección Básica
   - Cambio de VLAN nativa predeterminada
   - Monitoreo de tráfico no etiquetado
   - Implementación de controles de acceso
   - Revisión regular de configuraciones
2. Medidas Preventivas
   - Deshabilitación de puertos no utilizados
   - Configuración de trunk permitidos
   - Documentación de cambios
   - Auditorías periódicas

Consideraciones de Diseño

Aspectos importantes para la arquitectura de red:

1. Estructura de Red
   - Planificación de enlaces troncales
   - Distribución de VLANs
   - Topología de red
   - Requisitos de rendimiento
2. Compatibilidad
   - Verificación de soporte de dispositivos
   - Evaluación de equipos legacy

- Pruebas de interoperabilidad
- Planificación de actualizaciones

Resolución de Problemas Comunes

Estrategias para abordar desafíos típicos:

1. Diagnóstico
   - Verificación de configuraciones
   - Análisis de tráfico
   - Pruebas de conectividad
   - Identificación de inconsistencias
2. Soluciones
   - Corrección de configuraciones erróneas
   - Ajuste de parámetros
   - Actualización de firmware
   - Optimización de rendimiento

Optimización del Rendimiento

Estrategias para mejorar la eficiencia:

1. Monitoreo
   - Seguimiento del tráfico
   - Análisis de patrones
   - Detección de anomalías
   - Evaluación de rendimiento
2. Ajustes
   - Optimización de configuraciones
   - Balanceo de carga
   - Mejoras de seguridad
   - Actualizaciones proactivas

Integración con Otras VLANs

Consideraciones para la interoperabilidad:

1. Comunicación
   - Configuración de enlaces troncales
   - Gestión de permisos
   - Control de tráfico
   - Políticas de ruteo
2. Gestión
   - Administración centralizada
   - Monitoreo integrado
   - Control de acceso
   - Documentación unificada

La VLAN Nativa constituye un elemento crítico en la infraestructura de red moderna, especialmente en la configuración y operación de enlaces troncales. Su correcta implementación requiere una comprensión profunda de sus características y funcionalidades, así como una planificación cuidadosa y atención a los detalles de seguridad. La gestión efectiva de la VLAN Nativa contribuye significativamente a la estabilidad y eficiencia de la red, facilitando la comunicación entre dispositivos y manteniendo la compatibilidad con equipos diversos.

VLAN de Administración: Pilar Fundamental en la Gestión de Redes

La VLAN de Administración representa una implementación especializada dentro de las redes virtuales, diseñada específicamente para la gestión y supervisión de dispositivos de infraestructura de red. Esta segregación virtual cumple un papel crucial en la administración segura y eficiente de los recursos de red.

Fundamentos Esenciales

1. Definición y Propósito
   - Canal dedicado para gestión de red
   - Separación del tráfico administrativo
   - Control centralizado de dispositivos
   - Acceso privilegiado a equipos
2. Componentes Principales
   - Interfaces de gestión dedicadas
   - Direccionamiento IP específico
   - Protocolos de administración
   - Herramientas de monitoreo

Arquitectura de Seguridad

Elementos críticos para la protección:

1. Controles de Acceso
   - Autenticación multinivel
   - Restricciones de IP
   - Políticas de usuario
   - Cifrado de comunicaciones
2. Aislamiento
   - Segregación lógica
   - Filtrado de tráfico
   - Protección perimetral
   - Control de puertos

Configuración Básica

Aspectos fundamentales de implementación:

1. Preparación
   - Asignación de VLAN ID
   - Planificación de direcciones

- Definición de roles
- Documentación inicial

2. Implementación
   - Configuración de switches
   - Establecimiento de accesos
   - Pruebas de conectividad
   - Verificación de seguridad

Gestión Operativa

Elementos clave para la operación:

1. Tareas Administrativas
   - Configuración remota
   - Actualizaciones de sistema
   - Monitoreo de estado
   - Resolución de problemas
2. Herramientas de Gestión
   - Consolas de administración
   - Software de monitoreo
   - Sistemas de alertas
   - Registros de actividad

Consideraciones de Diseño

Aspectos críticos para la planificación:

1. Estructura
   - Topología de red
   - Puntos de acceso
   - Redundancia
   - Escalabilidad
2. Rendimiento
   - Ancho de banda reservado
   - Priorización de tráfico
   - Latencia
   - Disponibilidad

Mejores Prácticas

Recomendaciones fundamentales:

1. Seguridad
   - Cambio regular de credenciales
   - Auditorías periódicas
   - Actualizaciones de seguridad
   - Monitoreo continuo

2. Mantenimiento
   - Respaldos de configuración
   - Revisiones programadas
   - Documentación actualizada
   - Pruebas regulares

Resolución de Problemas

Estrategias de troubleshooting:

1. Diagnóstico
   - Verificación de conectividad
   - Análisis de logs
   - Pruebas de acceso
   - Revisión de configuraciones
2. Soluciones
   - Corrección de errores
   - Ajustes de configuración
   - Optimización de recursos
   - Documentación de incidentes

Monitoreo y Control

Aspectos de supervisión:

1. Supervisión
   - Métricas de rendimiento
   - Estado de dispositivos
   - Patrones de tráfico
   - Alertas automáticas
2. Control
   - Gestión de cambios
   - Accesos administrativos
   - Políticas de uso
   - Registros de actividad

Integración de Sistemas

Consideraciones de interoperabilidad:

a. Compatibilidad
   - Protocolos estándar
   - Interfaces comunes
   - Herramientas integradas
   - Soporte multi-vendor

b. Conectividad
   - Enlaces redundantes

- Rutas alternativas
- Backup de conexiones
- Failover automático

Documentación Técnica

Elementos esenciales:

a. Registros
- Inventario de equipos
- Configuraciones base
- Procedimientos operativos
- Planes de contingencia

b. Políticas
- Normas de acceso
- Protocolos de seguridad
- Procedimientos de cambio
- Guías de operación

Evolución y Crecimiento

Planificación futura:

a. Escalabilidad
- Capacidad de expansión
- Adaptabilidad
- Flexibilidad
- Actualizaciones

b. Innovación
- Nuevas tecnologías
- Mejoras de seguridad
- Optimizaciones
- Tendencias emergentes

La VLAN de Administración constituye un elemento crítico en la infraestructura de red moderna, proporcionando un entorno seguro y controlado para la gestión de dispositivos. Su implementación exitosa requiere una planificación detallada, considerando aspectos de seguridad, rendimiento y mantenimiento. La atención a estos detalles asegura una administración eficiente y segura de la red empresarial."

VLAN Dinámica: Asignación Inteligente en Redes Modernas

Las VLAN dinámicas permiten la asignación automática de dispositivos a VLAN específicas basándose en criterios como la dirección MAC, el protocolo utilizado o incluso la ubicación física del dispositivo. Esta flexibilidad en la asignación de VLAN facilita la gestión de redes grandes y reduce la carga administrativa asociada con la configuración manual de VLAN.

Fundamentos Principales

a. Concepto Base
- Asignación automática de VLAN
- Criterios dinámicos de membresía
- Gestión flexible de usuarios
- Adaptabilidad en tiempo real

b. Métodos de Asignación
- Por dirección MAC
- Por usuario/contraseña
- Por puerto
- Por protocolo

Mecanismos de Funcionamiento

Aspectos operativos clave:

a. Proceso de Asignación
- Detección de dispositivo
- Evaluación de criterios
- Asignación automática
- Verificación de membresía

b. Gestión de Membresía
- Actualización dinámica
- Seguimiento de cambios
- Control de acceso
- Monitoreo continuo

Implementación Técnica

Elementos fundamentales:

a. Configuración Inicial
- Definición de políticas
- Establecimiento de criterios
- Configuración de servidores
- Preparación de bases de datos

b. Infraestructura Necesaria
- Switches compatibles
- Servidores VMPS/RADIUS
- Bases de datos de usuarios
- Sistemas de autenticación

Ventajas Operativas

Beneficios principales:

a. Eficiencia Administrativa

- Reducción de tareas manuales
- Gestión centralizada
- Respuesta rápida a cambios
- Optimización de recursos

b. Flexibilidad

- Adaptación automática
- Movilidad de usuarios
- Escalabilidad mejorada
- Gestión simplificada

Consideraciones de Seguridad

Aspectos críticos:

1. Protección
   - Control de acceso
   - Monitoreo de asignaciones
   - Auditoría de cambios
   - Prevención de ataques
2. Políticas
   - Reglas de asignación
   - Restricciones de acceso
   - Verificación de identidad
   - Control de membresía

Gestión y Mantenimiento

Tareas esenciales:

1. Administración
   - Monitoreo de asignaciones
   - Actualización de políticas
   - Gestión de excepciones
   - Resolución de conflictos
2. Supervisión
   - Control de estado
   - Registro de cambios
   - Análisis de patrones
   - Detección de anomalías

Resolución de Problemas

Estrategias de solución:

a. Diagnóstico

- Verificación de asignaciones
- Análisis de logs
- Pruebas de conectividad
- Revisión de políticas

b. Corrección
- Ajuste de configuraciones
- Actualización de criterios
- Resolución de conflictos
- Optimización de reglas

Optimización del Sistema

Mejoras continuas:

a. Rendimiento
- Ajuste de parámetros
- Optimización de recursos
- Balanceo de carga
- Eficiencia operativa

b. Escalabilidad
- Planificación de crecimiento
- Adaptación a cambios
- Expansión de capacidades
- Actualización de sistemas

Integración con Sistemas Existentes

Consideraciones de compatibilidad:

a. Interoperabilidad
- Compatibilidad de protocolos
- Integración de servicios
- Sincronización de datos
- Gestión unificada

b. Migración
- Planificación de transición
- Compatibilidad retroactiva
- Actualización gradual
- Preservación de servicios

Documentación y Políticas

Aspectos administrativos:

a. Documentación
- Políticas de asignación
- Procedimientos operativos
- Registro de cambios
- Guías de troubleshooting

b. Normativas
- Estándares de configuración
- Políticas de seguridad
- Procedimientos de cambio

- Protocolos de gestión

Tendencias y Evolución

Perspectivas futuras:

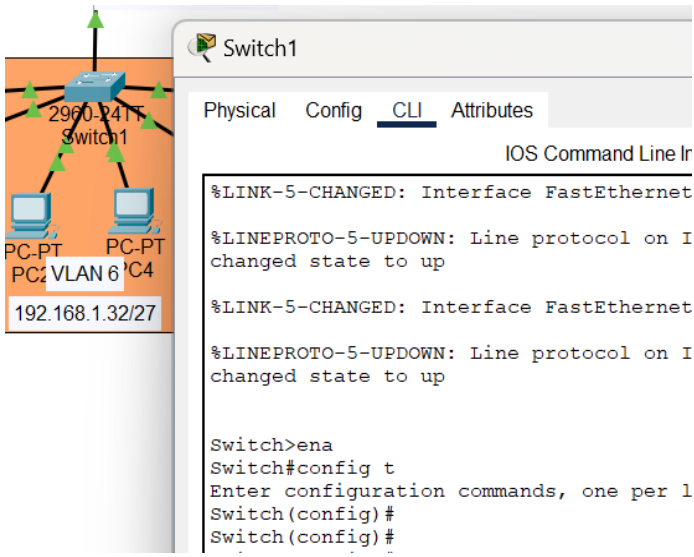
a. Innovaciones
- Nuevas tecnologías
- Automatización avanzada
- Inteligencia artificial
- Machine learning

b. Adaptación
- Requisitos emergentes
- Nuevos estándares
- Tecnologías futuras
- Mejoras de seguridad

La VLAN Dinámica representa una solución avanzada para la gestión moderna de redes, ofreciendo flexibilidad, eficiencia y automatización en la asignación de recursos de red. Su implementación exitosa requiere una planificación cuidadosa, considerando aspectos de seguridad, rendimiento y mantenimiento. La atención a estos detalles garantiza una operación eficiente y adaptable de la infraestructura de red.

6.3.3. Configuración de VLAN en Cisco Packet Tracer
Creación de VLAN Básica

- Ingresamos al Simulador de CISCO PACKET TRACER.
- Elegimos los elementos adecuados para la red.
- Damos clic izquierdo en el switch e ingresamos a los CLI.



Acceder al modo de configuración global
Switch>enable
Switch#configure terminal

Crear una VLAN y asignarle un nombre
Switch(config)#vlan 10
Switch(config-vlan)#name Administracion
Switch(config-vlan)#exit

Crear VLAN adicionales
Switch(config)#vlan 20
Switch(config-vlan)#name Ventas
Switch(config-vlan)#exit

Switch(config)#vlan 30
Switch(config-vlan)#name Produccion
Switch(config-vlan)#exit

Asignar puertos a las VLAN
Switch(config)#interface fast Ethernet 0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#exit

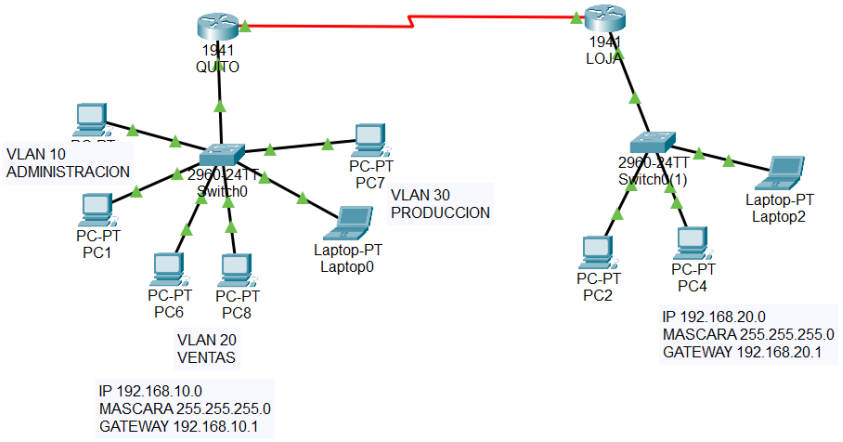
Configuración de Enlaces Troncales (Trunk)
Configurar puerto trunk
Switch(config)#interface gigabitEthernet 0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan all
Switch(config-if) #exit

Verificar configuración de trunk
Switch#show interfaces trunk

Configuración de VLAN de Voz
Configurar VLAN de voz
Switch(config)#vlan 100
Switch(config-vlan)#name VoIP
Switch(config-vlan)#exit

Configurar puerto para voz y datos
Switch(config)#interface fastEthernet 0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
Switch(config-if)#switchport voice vlan 100
Switch(config-if)#exit

6.3.4. Ejemplo práctico de implementación



Escenario: Empresa con tres departamentos y una sucursal en otra ciudad

Consideremos una empresa con los siguientes departamentos:

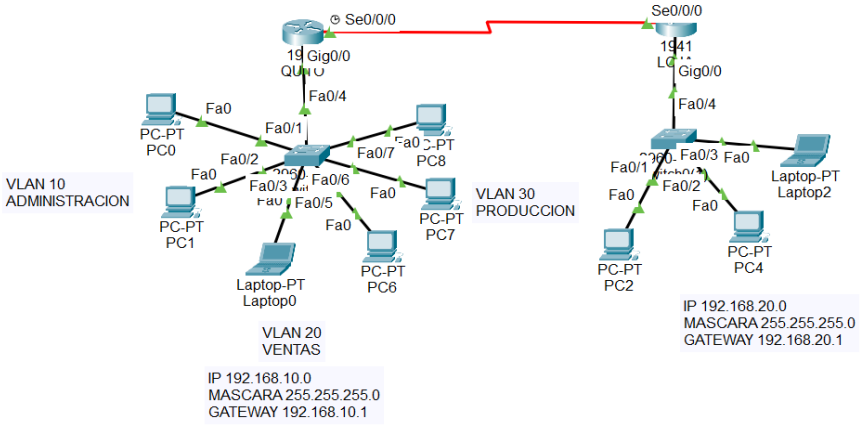
- Administración (VLAN 10)
- Ventas (VLAN 20)
- Producción (VLAN 30)

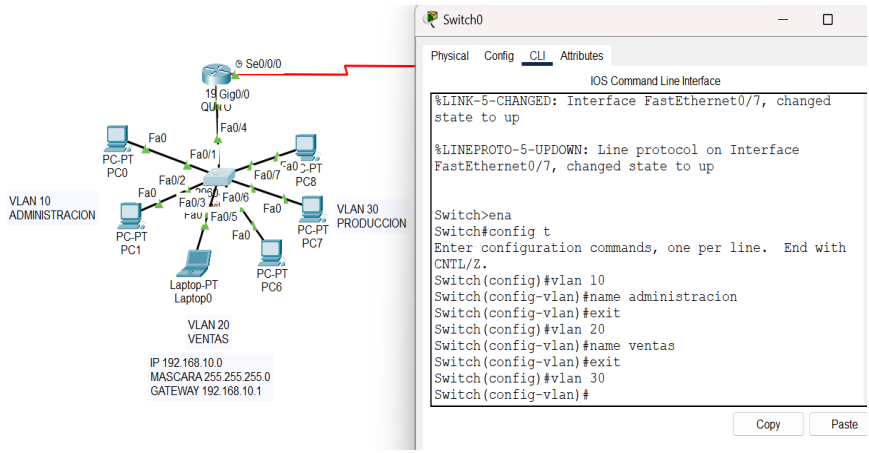
Topología de Red

- 2 Switches Cisco 2960
- 6 PCs (2 por departamento)
- 1 enlace troncal entre switches
- 1 router

Configuración Completa

Primero se da un clic sobre el switch en que se va a trabajar y luego se ingresa a la pestaña de CLI en donde se va a colocar todos los comandos que se describen a continuación. Se debe tomar en cuenta que las conexiones de las computadoras al switch deben estar en forma ordenada para que no exista ningún error el momento de correr el simulador.





Switch1>enable

Switch1#configure terminal

Crear VLANs

Switch1(config)#vlan 10

Switch1(config-vlan)#name Administracion

Switch1(config-vlan)#exit

Switch1(config)#vlan 20

Switch1(config-vlan)#name Ventas

```
Switch1(config-vlan)#exit
Switch1(config)#vlan 30
Switch1(config-vlan)#name Produccion
Switch1(config-vlan)#exit

! Configurar puertos de acceso
Switch1(config)#interface range fa0/1-2
Switch1(config-if-range)#switchport mode access
Switch1(config-if-range)#switchport access vlan 10
Switch1(config-if-range)#exit

Switch1(config)#interface range fa0/3-4
Switch1(config-if-range)#switchport mode access
Switch1(config-if-range)#switchport access vlan 20
Switch1(config-if-range)#exit

Switch1(config)#interface gi0/1
Switch1(config-if)#switchport mode trunk
Switch1(config-if)#exit

! Switch2 (configuración similar)
Switch2>enable
Switch2#configure terminal
```

```
! Crear VLANs idénticas
Switch2(config)#vlan 10
Switch2(config-vlan)#name Administracion
Switch2(config-vlan)#exit
Switch2(config)#vlan 20
Switch2(config-vlan)#name Ventas
Switch2(config-vlan)#exit
Switch2(config)#vlan 30
Switch2(config-vlan)#name Produccion
Switch2(config-vlan)#exit

! Configurar puertos de acceso
Switch2(config)#interface range fa0/1-2
Switch2(config-if-range)#switchport mode access
Switch2(config-if-range)#switchport access vlan 30
Switch2(config-if-range)#exit

! Configurar enlace troncal
Switch2(config)#interface gi0/1
Switch2(config-if)#switchport mode trunk
Switch2(config-if)#exit
```

Verificación de Configuración

cisco

Copiar

! Comandos de verificación

Switch#show vlan brief

Switch#show interfaces trunk

Switch#show running-config

Seguridad en VLAN
VLAN Hopping Prevention

cisco

Copiar

! Deshabilitar DTP

Switch(config-if)#switchport nonegotiate

! Establecer puertos no utilizados en VLAN no usada

Switch(config)#vlan 999

Switch(config-vlan)#name Unused

Switch(config-vlan)#exit

Switch(config)#interface range fa0/5-24

Switch(config-if-range)#switchport mode access

Switch(config-if-range)#switchport access vlan 999

Switch(config-if-range)#shutdown

Private VLAN

cisco

Copiar

! Configurar Private VLAN

Switch(config)#vlan 100

Switch(config-vlan)#private-vlan primary

Switch(config-vlan)#exit

Switch(config)#vlan 101

Switch(config-vlan)#private-vlan isolated

Switch(config-vlan)#exit

Switch(config)#vlan 100

Switch(config-vlan)#private-vlan association 101

Inter-VLAN Routing Router-on-a-Stick

cisco

Copiar

! Configuración del router

Router>enable

Router#configure terminal

! Configurar subinterfaces

Router(config)#interface gigabitEthernet 0/0.10

```
Router(config-subif)#encapsulation dot1q 10
Router(config-subif)#ip address 192.168.10.1 255.255.255.0
Router(config-subif)#exit

Router(config)#interface gigabitEthernet 0/0.20
Router(config-subif)#encapsulation dot1q 20
Router(config-subif)#ip address 192.168.20.1 255.255.255.0
Router(config-subif)#exit

Router(config)#interface gigabitEthernet 0/0.30
Router(config-subif)#encapsulation dot1q 30
Router(config-subif)#ip address 192.168.30.1 255.255.255.0
Router(config-subif)#exit

! Activar interfaz física
Router(config)#interface gigabitEthernet 0/0
Router(config-if)#no shutdown
```

Troubleshooting de VLAN

Comandos de Diagnóstico

```
! Verificar estado de VLANs
Switch#show vlan
Switch#show vlan brief
```

```
! Verificar configuración de puertos
Switch#show interfaces status
Switch#show interfaces switchport

! Verificar enlaces troncales
Switch#show interfaces trunk

! Verificar spanning-tree
Switch#show spanning-tree vlan 10
```

Problemas Comunes y Soluciones

a. Conectividad entre VLANs

```
! Verificar configuración de router
Router#show ip interface brief
Router#show running-config interface gigabitEthernet 0/0

! Verificar enrutamiento
Router#show ip route
```

b. Problemas de Trunk

```
! Verificar modo de puerto
Switch#show interfaces gi0/1 switchport

! Verificar VLANs permitidas
Switch(config)#interface gi0/1
Switch(config-if)#switchport trunk allowed vlan all
```

Router Loja

```
Router>ena

Router#config t

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#int gi0/0

Router(config-if)#no shutdown

Router(config-if)#ip add 192.168.20.1 255.255.255.0

Router(config-if)#exit

Router(config)#int se0/0/0

Router(config-if)#no shutdown

Router(config-if)#ip add 10.0.0.1 255.255.255.0

Router(config-if)#exit

Router(config)#router rip

Router(config-router)#network 192.168.20.0

Router(config-router)#network 192.168.10.0

Router(config-router)#network 10.0.0.0

Router(config-router)#exit

Router(config)#exit

Router#

%SYS-5-CONFIG_I: Configured from console by console


Router#copy run start

Destination filename [startup-config]?

Building configuration...
```

[OK]

Router#

Router Quito

Router>ena

Router#config t

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#int gi0/0

Router(config-if)#no shutdown

Router(config-if)#ip add 192.168.10.1 255.255.255.0

Router(config-if)#exit

Router(config)#int se0/0/0

Router(config-if)#no shutdown

Router(config-if)#ip add 10.0.0.2 255.255.255.0

Router(config-if)#exit

Router(config)#router rip

Router(config-router)#network 192.168.10.0

Router(config-router)#network 192.168.20.0

Router(config-router)#network 10.0.0.0

Router(config-router)#exit

Router(config)#exit

Router#

%SYS-5-CONFIG_I: Configured from console by console

Router#copy run start

Destination filename [startup-config]?

Building configuration...

[OK]

Router#

Observación: Para que la práctica salga bien es necesario que todos los dispositivos estén colocados igual que en la topología, ya que si se cambia de interfaces también se deberán cambiar en las líneas de código, caso contrario no correrá la simulación.

Como se puede ver las VLAN son una herramienta fundamental en el diseño y administración de redes modernas. Su implementación correcta mejora significativamente la seguridad, el rendimiento y la flexibilidad de la red. Además, en la parte económica disminuye los costos, tomando en cuenta que con un mismo dispositivo (switch) se puede hacer varias subredes.

La práctica continua en entornos de simulación como Cisco Packet Tracer es esencial para dominar estas configuraciones y estar preparado para implementaciones en entornos de producción. La combinación de conocimiento teórico y habilidades prácticas garantiza una gestión exitosa de redes empresariales modernas. No es necesario aprender de memoria los CLI, ya que con el símbolo "?" se puede obtener todos los comandos que se van a utilizar en la red, lo importante es conocer la forma, aplicaicón y utilización de estos.

6.4. ACL (Listas de Control de Acceso) en Redes

Las Listas de Control de Acceso (ACL) son conjuntos secuenciales de declaraciones de permiso o denegación que se aplican a direcciones IP o protocolos de nivel superior. Funcionan como un filtro de tráfico de red, evaluando los paquetes según las condiciones establecidas y decidiendo si permitir o denegar su paso.

6.4.1. Tipos de ACL
ACL Estándar

Las Listas de Control de Acceso (ACL) estándar representan un mecanismo fundamental en la gestión de redes que actúa como un filtro selectivo del tráfico de red. Su principal característica distintiva radica en que únicamente evalúan la dirección IP de origen de los paquetes que atraviesan la red, lo que las convierte en una herramienta relativamente sencilla pero efectiva para el control básico del tráfico.

Cuando se habla de la implementación de ACL estándar, es importante mencionar que operan exclusivamente en la capa 3 del modelo OSI, también conocida como la capa de red. Esta característica las distingue de sus contrapartes más complejas, las ACL extendidas, ya que su alcance se limita a examinar únicamente el origen del tráfico, sin considerar otros parámetros como puertos o protocolos.

En el contexto de la numeración, las ACL estándar se identifican mediante un rango específico de números que abarca desde el 1 hasta el 99, y se extiende adicionalmente desde el 1300 hasta el 1999. Esta nomenclatura numérica facilita su organización y gestión dentro de la configuración de los dispositivos de red, permitiendo una identificación rápida y eficiente de las diferentes políticas de acceso implementadas.

Un aspecto crucial en la implementación de las ACL estándar es su ubicación estratégica en la red. La práctica recomendada sugiere colocarlas lo más cerca posible del destino del tráfico. Esta recomendación se fundamenta en la necesidad de evitar el filtrado innecesario de tráfico en puntos intermedios de la red, lo que podría afectar negativamente el rendimiento general del sistema.

El funcionamiento de una ACL estándar sigue un proceso secuencial y lógico. Cuando un paquete llega al dispositivo de red, la ACL examina la dirección IP de origen y la compara con las reglas establecidas en orden descendente. Este proceso continúa hasta encontrar una coincidencia o hasta llegar al final de la lista, donde existe una regla implícita que deniega todo el tráfico no especificado anteriormente.

La flexibilidad de las ACL estándar se manifiesta en su capacidad para trabajar con máscaras wildcard, que permiten definir rangos de direcciones IP de manera eficiente. Estas máscaras funcionan de manera inversa a las máscaras de subred tradicionales, donde un bit en 0 indica que debe haber una coincidencia exacta, mientras que un bit en 1 permite cualquier valor en esa posición.

En el ámbito de la seguridad de red, las ACL estándar desempeñan un papel fundamental como primera línea de defensa. Aunque su funcionalidad puede parecer limitada en comparación con las ACL extendidas, su simplicidad las hace ideales para implementar políticas de seguridad básicas y efectivas, especialmente en situaciones donde solo se necesita controlar el acceso basado en el origen del tráfico.

El mantenimiento y la gestión de las ACL estándar forman parte integral de la administración de red. Es importante realizar revisiones periódicas de las reglas implementadas, eliminar aquellas que ya no sean necesarias y actualizar las existentes según evolucionen las necesidades de la red. Esta práctica ayuda a mantener un entorno de red eficiente y seguro.

La documentación adecuada de las ACL estándar es crucial para su gestión efectiva a largo plazo. Cada regla debe estar bien documentada, incluyendo su propósito, fecha de implementación y cualquier consideración especial. Esto facilita la resolución de problemas y permite que otros administradores de red comprendan y mantengan las políticas de acceso implementadas.

ACL Extendida

Las Listas de Control de Acceso Extendidas representan una evolución significativa en el control del tráfico de red, ofreciendo un nivel de granularidad y precisión considerablemente superior a sus contrapartes estándar. Estas herramientas avanzadas de filtrado operan simultáneamente en las capas 3 y 4 del modelo OSI, permitiendo un control más detallado y específico sobre el flujo de datos en la red.

A diferencia de las ACL estándar, las ACL extendidas pueden examinar múltiples parámetros dentro de los paquetes de red. Esta capacidad incluye la evaluación tanto de direcciones IP de origen como de destino, la identificación de protocolos específicos (como TCP, UDP o ICMP), y el análisis de números de puerto, proporcionando así un control extraordinariamente preciso sobre el tráfico de red.

En el esquema de numeración de Cisco, las ACL extendidas se identifican mediante números que van desde 100 hasta 199, y se complementan con un rango adicional que abarca desde 2000 hasta 2699. Esta nomenclatura específica facilita su identificación y gestión en entornos de red complejos, permitiendo una organización más estructurada de las políticas de seguridad.

La implementación estratégica de las ACL extendidas sigue un principio fundamental: deben colocarse lo más cerca posible del origen del tráfico. Esta ubicación estratégica permite filtrar el tráfico no deseado en su punto de origen, optimizando así el uso de recursos de red y mejorando la eficiencia general del sistema.

Las ACL extendidas destacan por su capacidad para implementar controles basados en tiempo, permitiendo la creación de políticas de acceso que varían según horarios específicos. Esta funcionalidad resulta particularmente útil en entornos empresariales donde se requiere un control diferenciado del acceso durante y fuera del horario laboral.

En el ámbito de la seguridad de red, las ACL extendidas juegan un papel crucial en la implementación de políticas de seguridad detalladas. Su capacidad para filtrar tráfico basándose en múltiples criterios las convierte en una herramienta esencial para proteger recursos críticos y prevenir accesos no autorizados.

La configuración de ACL extendidas requiere un conocimiento profundo de los protocolos de red y una comprensión clara de los requisitos de seguridad específicos de la organización. Cada regla debe diseñarse cuidadosamente para equilibrar la seguridad con la funcionalidad, asegurando que las políticas implementadas no obstaculicen las operaciones comerciales legítimas.

El mantenimiento efectivo de las ACL extendidas demanda una atención constante y una revisión periódica. Las reglas deben actualizarse regularmente para reflejar cambios en la infraestructura de red, nuevos requisitos de seguridad y amenazas emergentes. Esta gestión continua es fundamental para mantener un entorno de red seguro y eficiente. También ofrecen capacidades avanzadas de logging y monitoreo, permitiendo un seguimiento detallado del tráfico que coincide con reglas específicas.

La optimización del rendimiento es un aspecto crítico en la implementación de ACL extendidas. Las reglas deben organizarse de manera eficiente, colocando las coincidencias más frecuentes al principio de la lista para minimizar el tiempo de procesamiento y maximizar el rendimiento de la red.

En entornos empresariales modernos, las ACL extendidas se integran frecuentemente con otras tecnologías de seguridad, como sistemas de detección de intrusiones y firewalls, formando parte de una estrategia de seguridad en capas. Esta integración permite una protección más robusta y completa de los recursos de red.

La flexibilidad de las ACL extendidas se evidencia en su capacidad para adaptarse a diversos escenarios de implementación, desde la segmentación de redes corporativas hasta la protección de

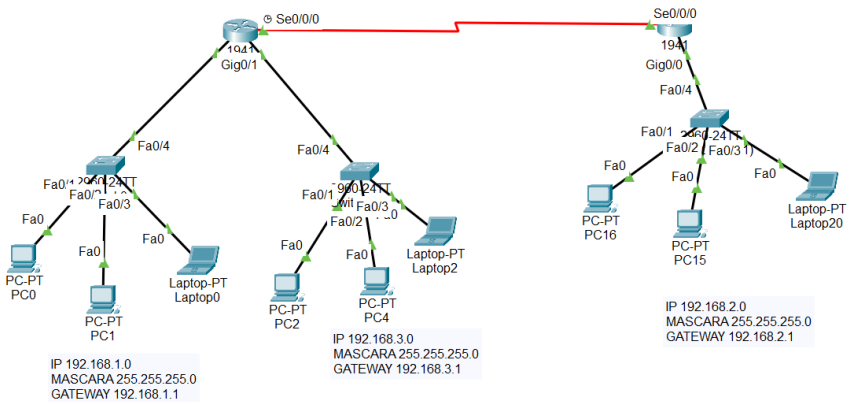
servicios específicos. Esta versatilidad las convierte en una herramienta indispensable en el arsenal de cualquier administrador de red.

6.4.2. Práctica en Cisco Packet Tracer
Escenario de Práctica

Vamos a crear una red con las siguientes características:

- 3 redes diferentes
- Control de acceso entre redes
- Restricciones de servicios específicos

Topología



Configuración Paso a Paso

1. Configuración Básica de Routers

! Router 1

```
enable
configure terminal
hostname R1

! Configuración de interfaces
interface GigabitEthernet0/0
ip address 192.168.1.1 255.255.255.0
no shutdown
```

```
interface GigabitEthernet0/1
ip address 192.168.3.1 255.255.255.0
no shutdown
interface Serial0/0/0
ip address 10.0.0.1 255.255.255.252
no shutdown
```

! Router 2

```
enable
configure terminal
hostname R2

interface GigabitEthernet0/0
ip address 192.168.2.1 255.255.255.0
no shutdown

interface Serial0/0/0
ip address 10.0.0.2 255.255.255.252
no shutdown
```

2. Configuración de ACL Estándar

```
! En Router 1
! Permitir acceso desde Red A a Red B
access-list 10 permit 192.168.1.0 0.0.0.255
access-list 10 deny any

! Aplicar ACL a la interfaz
interface Serial0/0/0
ip access-group 10 out
```

3. Configuración de ACL Extendida

```
! En Router 1

! Permitir solo HTTP y DNS desde Red C a Red B

access-list 100 permit tcp 192.168.3.0 0.0.0.255 192.168.2.0 0.0.0.255 eq 80

access-list 100 permit udp 192.168.3.0 0.0.0.255 192.168.2.0 0.0.0.255 eq 53

access-list 100 deny ip any any


! Aplicar ACL a la interfaz

interface GigabitEthernet0/1

ip access-group 100 in
```

4. Verificación de Configuración

```
! Comandos de verificación

show access-lists

show ip interface

show running-config | include access-list
```

Ejemplos de ACL Avanzadas

1. ACL con Control de Tiempo

```
! Permitir acceso web solo en horario laboral

time-range HORARIO_LABORAL

 periodic weekdays 8:00 to 18:00


access-list 101 permit tcp any any eq 80 time-range HORARIO_LABORAL
```

2. ACL con Control de Protocolos Específicos

```
! Control de protocolos comunes

access-list 102 permit tcp any any eq 80  ! HTTP

access-list 102 permit tcp any any eq 443 ! HTTPS

access-list 102 permit tcp any any eq 25  ! SMTP

access-list 102 deny tcp any any range 135 139 ! Bloquear NetBIOS


! Comandos útiles para monitoreo

show access-lists

show ip access-lists

show logging
```

Resolución de Problemas Comunes

- ***Problemas de Conectividad:***
    - Verificar orden de las reglas
    - Comprobar dirección de aplicación (in/out)
    - Revisar wildcard masks
- ***Rendimiento:***
    - Optimizar orden de reglas
    - Eliminar reglas redundantes
    - Usar ACL nombradas cuando sea posible
- ***Comandos de Diagnóstico:***
    - debug ip packet detail access-list
    - show ip interface | include access list
    - show access-lists [número/nombre]

Consideraciones de Seguridad

1. Backup y Documentación:

```
cisco

Copiar

! Guardar configuración
```

```
copy running-config startup-config

! Exportar a TFTP

copy running-config tftp
```

2. Actualizaciones:

```
Planificar ventanas de mantenimiento

Probar cambios en laboratorio

Mantener procedimiento de rollback
```

Tabla comparativa entre ACL estándar y ACL extendido

Característica	*ACL Estándar*	*ACL Extendida*
Rango de Números	1-99 y 1300-1999	100-199 y 2000-2699
Capas OSI	Solo Capa 3 (Red)	Capa 3 (Red) y Capa 4 (Transporte)
Criterios de Filtrado	Solo dirección IP origen	- Dirección IP origen - Dirección IP destino - Protocolos - Puertos origen - Puertos destino
Complejidad	Simple	Compleja
Ubicación Recomendada	Cerca del destino	Cerca del origen
Recursos de Procesamiento	Bajo consumo	Mayor consumo
Nivel de Control	Básico	Granular
Flexibilidad	Limitada	Alta
Casos de Uso	Control básico de acceso Filtrado simple de tráfico Restricciones por origen	Control detallado de servicios Filtrado por aplicación Políticas de seguridad complejas
Sintaxis de Configuración	Simple y directa	Más extensa y detallada

Característica	*ACL Estándar*	*ACL Extendida*
Tiempo de Configuración	Rápido	Requiere más tiempo
Mantenimiento	Fácil	Más complejo
Troubleshooting	Simple	Complejo
Control de Protocolos	No disponible	Disponible
Control de Puertos	No disponible	Disponible
Wildcards	Solo para IP origen	Para IP origen y destino
Impacto en Performance	Mínimo	Moderado
Logging	Básico	Detallado
Verificación	Simple	Requiere más verificaciones
Documentación Necesaria	Básica	Extensa

Cuestionario de refuerzo para medir conocimientos de ACL

Responder las siguientes preguntas de opción múltiple

1. ¿Qué significa ACL en el contexto de redes de datos?
    a) Access Control List
    b) Automatic Control Layer
    c) Access Control Layer
    d) Advanced Control List
2. ¿Cuál es la función principal de una ACL?
    a) Aumentar la velocidad de la red
    b) Filtrar tráfico de red
    c) Mejorar la calidad de servicio
    d) Monitorear el uso de ancho de banda
3. ¿En qué dispositivos se pueden implementar ACLs?
    a) Solo en routers
    b) Solo en switches
    c) En routers y switches
    d) En servidores únicamente
4. ¿Cuál de las siguientes es una ventaja de utilizar ACLs?
    a) Reducción de costos de hardware
    b) Mejora en el rendimiento de la red
    c) Simplificación del diseño de la red
    d) Aumento de la complejidad de la red
5. ¿Qué tipo de ACL permite el filtrado de tráfico basado en direcciones IP de origen y destino?
    a) ACL estándar
    b) ACL extendida
    c) ACL dinámica
    d) ACL de ruta

Llenado de forma adecuada la frase

6. Complete la frase: Las ACLs se utilizan principalmente para _____ el tráfico no deseado en una red.
7. Las ACLs pueden ser clasificadas en dos tipos principales: _____ y _____.
8. El comando para crear una ACL estándar en un router Cisco es _____.
9. Una ACL extendida puede filtrar tráfico basado en protocolos como _____ y _____.
10. El número de una ACL estándar en un router Cisco puede estar entre _____ y _____.

Verdadero/Falso

11. Las ACLs solo pueden ser aplicadas a interfaces de entrada.
    a) Verdadero
    b) Falso
12. Una ACL estándar puede filtrar tráfico basado solo en la dirección IP de origen.
    a) Verdadero
    b) Falso
13. Las ACLs pueden afectar el rendimiento de la red si no se configuran adecuadamente.
    a) Verdadero
    b) Falso
14. Las ACLs no pueden ser utilizadas en conexiones VPN.
    a) Verdadero
    b) Falso
15. Las ACLs pueden ser utilizadas para permitir o denegar el acceso a ciertos servicios en la red.
    a) Verdadero
    b) Falso

16. ¿Qué protocolo se utiliza comúnmente para la gestión de ACLs en dispositivos Cisco?
    a) SNMP
    b) HTTP
    c) Telnet
    d) FTP
17. ¿Cuál de las siguientes afirmaciones sobre ACLs es correcta?
    a) Las ACLs se procesan en orden secuencial.
    b) Las ACLs se aplican solo a tráfico interno.
    c) Las ACLs no pueden ser modificadas una vez creadas.
    d) Las ACLs son irrelevantes para la seguridad de la red.
18. ¿Qué acción realiza una ACL si no encuentra una coincidencia en las reglas definidas?
    a) Permite el tráfico automáticamente
    b) Bloquea el tráfico automáticamente
    c) Genera una alerta
    d) Ignora el tráfico
19. ¿Cuál es el rango de números para las ACLs extendidas en un router Cisco?
    a) 1-99
    b) 100-199
    c) 200-299
    d) 300-399
20. ¿Qué tipo de tráfico puede ser filtrado por una ACL extendida?
    a) Solo tráfico HTTP
    b) Tráfico de cualquier protocolo
    c) Solo tráfico de correo electrónico
    d) Solo tráfico de video

6.5. NAT

La Traducción de Direcciones de Red (NAT, por sus siglas en inglés) es una técnica fundamental en la administración de redes que permite la modificación de las direcciones IP en los encabezados de los paquetes mientras atraviesan un dispositivo de red. Esta técnica se utiliza principalmente para permitir que múltiples dispositivos, dentro de una red local, compartan una única dirección IP pública para acceder a Internet. La NAT juega un papel crucial en la conservación de direcciones IP y en la mejora de la seguridad de la red.

El funcionamiento de NAT se basa en la modificación de las direcciones IP en los paquetes de datos. Cuando un dispositivo en la red interna envía un paquete a Internet, el router que implementa NAT realiza las siguientes acciones:

a) ***Identificación de la dirección IP interna:*** El router identifica la dirección IP privada del dispositivo que está enviando el paquete.

b) ***Sustitución de la dirección IP:*** El router reemplaza la dirección IP privada con su propia dirección IP pública en el encabezado del paquete.

c) ***Registro de la conexión:*** El router guarda una entrada en una tabla de traducción que vincula la dirección IP privada con la dirección IP pública y el número de puerto utilizado.

d) ***Envío del paquete:*** El paquete modificado se envía a su destino en Internet.

Cuando el paquete de respuesta regresa al router, este utiliza la tabla de traducción para revertir el proceso, cambiando la dirección IP pública de vuelta a la dirección IP privada correspondiente y enviando el paquete al dispositivo correcto en la red interna.

6.5.1. Tipos de NAT

Existen varios tipos de NAT, cada uno con características y aplicaciones específicas:

a) ***NAT Estático:***

- Asocia una dirección IP pública específica a una dirección IP privada fija.
- Ideal para servidores que necesitan ser accesibles desde el exterior, como servidores web, servidores FTP o servidores de correo electrónico.
- Ejemplo: Un servidor web con la dirección IP privada 192.168.1.10 puede ser accesible desde Internet a través de la dirección IP pública 203.0.113.10.

b) ***NAT Dinámico:***

- Utiliza un grupo de direcciones IP públicas y asigna una de ellas a una dirección IP privada cuando es necesario.
- A diferencia del NAT estático, no hay una asignación fija, lo que permite una mejor utilización de las direcciones IP públicas.

- Ejemplo: Si hay tres direcciones IP públicas disponibles, el router puede asignar una de ellas a cualquier dispositivo interno que necesite acceso a Internet.

c) PAT (Traducción de Dirección de Puerto):

- También conocido como NAT sobrecargado, permite que múltiples dispositivos en una red local compartan una única dirección IP pública utilizando diferentes números de puerto.

- Es el tipo más común de NAT en entornos domésticos y pequeñas empresas, ya que maximiza el uso de direcciones IP.

- Ejemplo: Dos dispositivos internos con direcciones IP 192.168.1.2 y 192.168.1.3 pueden acceder a Internet usando la misma dirección IP pública (203.0.113.10) pero con diferentes números de puerto.

La implementación de NAT ofrece diversas ventajas que son esenciales para la administración de redes:

- ***Conservación de direcciones IP:*** Permite que una red interna utilice direcciones privadas, lo que ayuda a conservar el espacio de direcciones públicas. Esto es especialmente importante dado el agotamiento de direcciones IPv4.

- ***Seguridad:*** Al ocultar las direcciones IP internas de los dispositivos, se reduce la exposición a ataques externos. Los dispositivos de la red interna no son directamente accesibles desde Internet, lo que añade una capa de protección.

- ***Flexibilidad en la reestructuración de la red:*** La NAT permite cambiar las direcciones IP internas sin necesidad de modificar la configuración de las direcciones IP públicas, lo que facilita la reestructuración de la red.

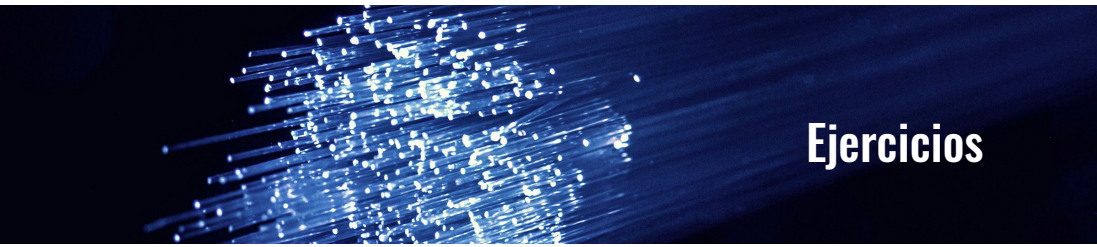
- ***Facilidad de implementación:*** NAT se puede implementar en la mayoría de los routers y dispositivos de red, lo que lo hace accesible y fácil de configurar.

A pesar de sus ventajas, NAT también presenta algunas desventajas:

- ***Complejidad en la configuración:*** La configuración de NAT puede ser compleja, especialmente en entornos que utilizan múltiples tipos de NAT o donde se requieren configuraciones avanzadas.

- ***Problemas de rendimiento:*** La traducción de direcciones puede introducir latencia en la red, especialmente si el router está manejando un gran volumen de tráfico.

- ***Problemas con ciertos protocolos:*** Algunos protocolos, como SIP (Protocolo de Inicio de Sesión) y FTP (Protocolo de Transferencia de Archivos), pueden tener dificultades para funcionar correctamente a través de NAT debido a la forma en que manejan las conexiones y las direcciones IP.



Ejercicios

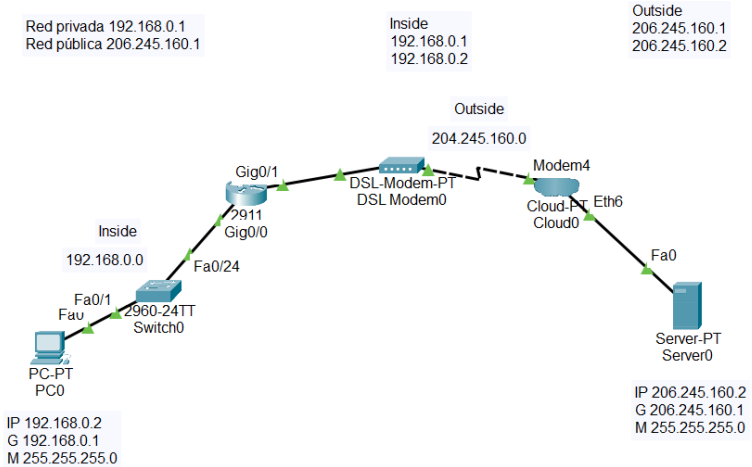
6.5.2 Ejercicio Práctico en Cisco Packet Tracer

A continuación, se presenta un ejercicio detallado para implementar NAT en Cisco Packet Tracer, que permitirá comprender mejor su funcionamiento.

Objetivo

Configurar NAT para permitir que los dispositivos de una red interna accedan a Internet utilizando una única dirección IP pública.

Topología



Pasos por seguir:

La red conecta una ***PC en red privada*** con un ***servidor en red pública*** a través de un router con NAT, un módem DSL y una nube simulada (tomar en cuenta que los dispositivos de su topología estén conectados de forma idéntica al del ejercicio, caso contrario no funcionará la simulación).

Dispositivo	*Interfaz*	*IP*	*Rol*
PC0	Fa0	192.168.0.2 / 24	Cliente LAN
Switch0	—	—	Conmutador LAN
Router 2911	Gig0/0	192.168.0.1 / 24	Gateway Inside
Router 2911	Gig0/1	204.245.160.x	Enlace WAN
DSL Modem0	—	—	Puente DSL
Cloud0	—	—	Simulación WAN
Server0	Fa0	206.245.160.2 / 24	Servidor público

PASO 1: Agregar Dispositivos al Área de Trabajo

Coloca los siguientes dispositivos desde el panel inferior del simulador de Cisco Packet Tracer:

- ***1x PC-PT*** →PC0
- ***1x Switch 2960-24TT*** → Switch0
- ***1x Router 2911*** → Router0
- ***1x DSL-Modem-PT*** →DSL Modem0
- ***1x Cloud-PT*** → Cloud0
- ***1x Server-PT*** →Server0

PASO 2 — Conectar los Dispositivos

Usa los cables correctos desde ***Connections*** (rayo):

Origen	*Puerto*	*Destino*	*Puerto*	*Cable*
PC0	Fa0	Switch0	Fa0/1	Cobre directo
Switch0	Fa0/24	Router 2911	Gig0/0	Cobre directo
Router 2911	Gig0/1	DSL Modem0	Puerto DSL	Serial / Telefónico
DSL Modem0	Eth	Cloud0	Modem4	Cobre directo
Cloud0	Eth6	Server0	Fa0	Cobre directo

Para el enlace ***Router → DSL Modem,*** usa cable telefónico (Phone). Para ***DSL Modem → Cloud***, usa cobre directo.

PASO 3 — Configurar la PC0

Clic en ***PC0 → Desktop → IP Configuration:***

IP Address: 192.168.0.2

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.0.1

PASO 4 — Configurar el Server0

Clic en ***Server0 → Desktop → IP Configuration:***

IP Address: 206.245.160.2

Subnet Mask: 255.255.255.0

Default Gateway: 206.245.160.1

PASO 5 — Configurar el Router 2911

Clic en ***Router → CLI*** y escribe:

```
enable
configure terminal

! --- Interfaz LAN (Inside) ---
interface GigabitEthernet0/0
 ip address 192.168.0.1 255.255.255.0
 ip nat inside
 no shutdown
```

```
! --- Interfaz WAN (Outside) ---
interface GigabitEthernet0/1
 ip address 204.245.160.1 255.255.255.0
 ip nat outside
 no shutdown

! --- Ruta estática hacia la red pública ---
ip route 0.0.0.0 0.0.0.0 204.245.160.2

! --- Configurar NAT (PAT / Overload) ---
access-list 1 permit 192.168.0.0 0.0.0.255
ip nat inside source list 1 interface GigabitEthernet0/1 overload
end
write memory
```

PASO 6 — Configurar la Nube (Cloud0)

Clic en ***Cloud0 → Config → DSL:***

- Verifica que el ***Modem4*** esté vinculado al puerto ***Eth6***
- Esto simula el enlace entre el módem DSL y la red pública

En Packet Tracer, la nube actúa como ***puente transparente*** entre el módem y el servidor.

PASO 7 — Configurar el DSL Modem0

Clic en ***DSL Modem0 → Config:***

- Puerto ***Ethernet*** conectado al Router (Gig0/1)
- Puerto ***DSL*** conectado hacia la nube

- No requiere IP — actúa como ***bridge/puente***

PASO 8 — Verificar Conectividad

Desde ***PC0 → Desktop → Command Prompt:***

Copiar

Prueba al gateway local

ping 192.168.0.1

Prueba al servidor público

ping 206.245.160.2

Verificar traducción NAT en el router

Desde el ***Router CLI:***

Copiar

show ip nat translations

show ip route

show interfaces

Resultado Esperado

Prueba	*Resultado*
PC0 → Gateway (192.168.0.1)	Exitoso
PC0 → Server0 (206.245.160.2)	Exitoso con NAT
show ip nat translations	Muestra traducción 192.168.0.2 → 204.245.160.1

Clave del ejercicio: el Router 2911 hace ***NAT con sobrecarga (PAT)***, traduciendo la IP privada 192.168.0.2 a la IP pública 204.245.160.1 para que el servidor externo pueda responder correctamente.

La conclusión después de realizar la práctica seria que la NAT es una técnica esencial en la administración de redes modernas, permitiendo el acceso a Internet y mejorando la seguridad de la red. A través de la práctica con herramientas como Cisco Packet Tracer, los administradores de red pueden familiarizarse con su configuración y funcionamiento, lo que les permitirá gestionar mejor sus infraestructuras de red. La comprensión profunda de NAT es crucial para el diseño y la implementación de redes eficientes y seguras.

Quito - Ecuador | @isucentraltécnico.ec

www.istct.edu.ec

ISBN: 978-9942-53-155-1