Resumen Redes I

# Multiplexación

Multiplexar se denomina a la técnica de combinar 2 o más señales y transmitirlas a través de un único medio de transmisión.

La principal ventaja de utilizar esta técnica es que permite aprovechar mejor el ancho de banda de cada medio de transmisión, permitiendo que más señales viajen a través de él en simultáneo. De lo contrario, se debería realizar una conexión dedicada por cada par de dispositivos que se quiere conectar en la red, lo cual es ineficiente en términos de recursos (tanto económicos como en términos de ancho de banda).

## Demultiplexación

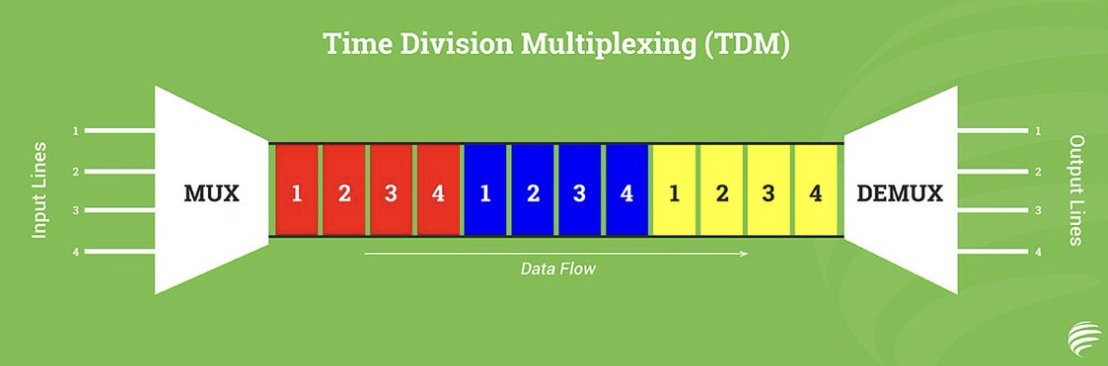
La demultiplexación es el proceso inverso a la multiplexación, en el cual se recupera cada una de las señales individuales transmitidas a través del único medio.

## TDM

Modulación por división de tiempo

Las señales múltiples son llevadas al mismo canal en espacios de tiempo alternados.

Se usa en enlaces SONET que solían ser uno de los pilares de las iniciativas WAN y de conectividad a Internet.

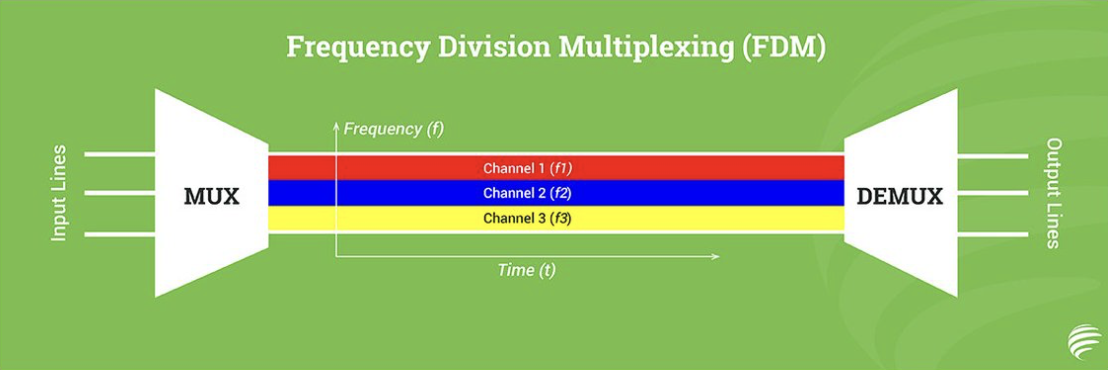


## FDM

Modulación por división de frecuencia

El ancho de banda en un enlace de comunicaciones se divide en subcanales de diferentes anchos de frecuencia, cada uno con una señal al mismo tiempo en paralelo.

La televisión por cable implementa FDM, donde envía múltiples canales a través de los mismos hilos del cable coaxial.

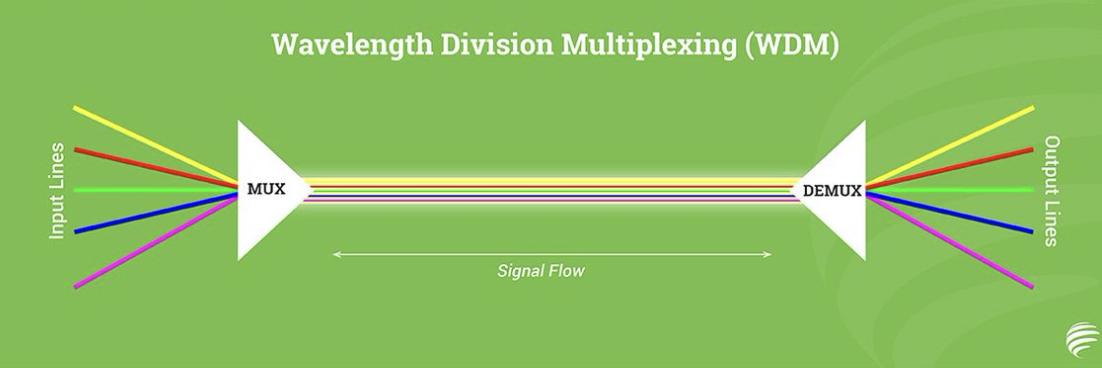


## WDM

Modulación por división de longitud de onda

Los datos de diferentes canales de comunicación se envían en ondas de luz de diferentes longitudes de onda, aunque se debe considerar que esto sólo se puede realizar en canales de **fibra óptica**.

Se utiliza en canales de fibra óptica para un mayor aprovechamiento del amplio ancho de banda que ofrece este medio de transmisión.



## DWDM

Modulación por división de longitud de onda densa

A través de una única fibra óptica se pueden transmitir hasta **128 longitudes** de onda diferentes.

Los canales se encuentran definidos dentro del rango **1530 – 1610 nm**, separados entre ellos por entre **0,8 nm** y **1,6 nm**.

Dependiendo de la separación entre las longitudes de onda, el sistema puede proveer una capacidad de entre **50 GHz** y **200 GHz.**

Los sistemas DWDM se utilizan principalmente en redes de transmisión de larga distancia donde se necesita una gran capacidad de transmisión de información.

## 

## Ejercicio de Ejemplo - Multiplexación

Un multiplexor TDM tiene 4 entradas, dos de ellas A y D de 9600 bps y las otras dos B y C de 4800 bps . Determine la velocidad de la puerta de salida y la distribución de los time slots de tiempo.

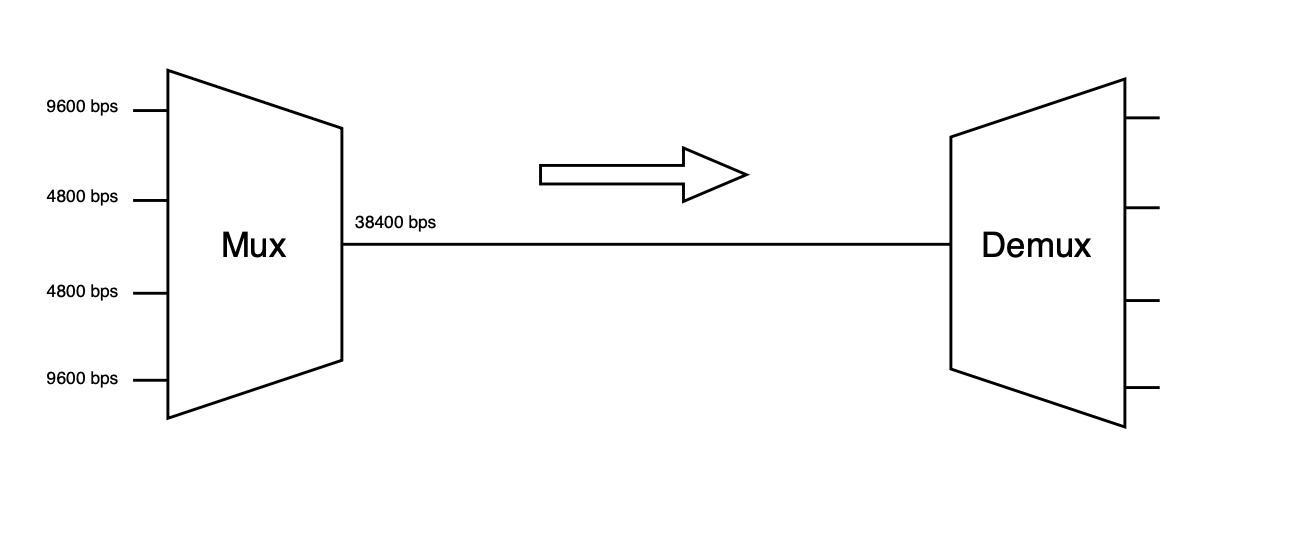
* ¿A qué velocidad deberá muestrear el multiplexor?

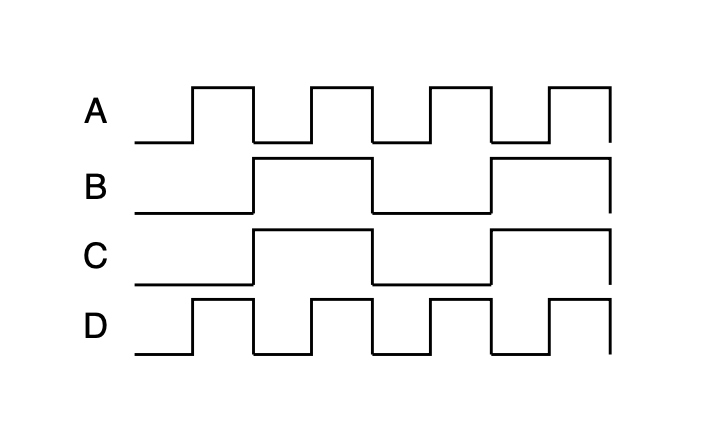
9600 bps

4 x 9600 bps ???

Deberá muestrear a 104.1664 x 10-6 segundos

* A - Dibuje el multiplexor y grafique en un diagrama de tiempos cada una de las entradas y la salida con al menos la información de 4 tramas.





* B - ¿Cuál es el tiempo en segundos de cada trama y de cada slot?

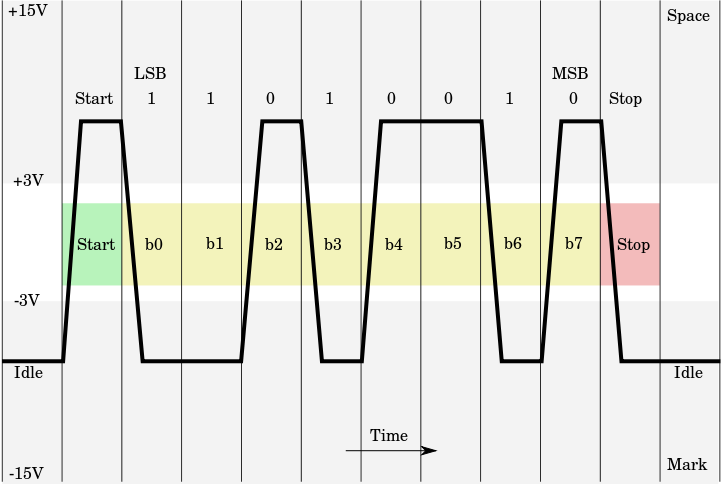
Time slot = 1 / (4 x 9600) = **26.0416 x 10-6 segundos**

Trama = 26,0416 x 10-6 x 4 = **104.1664 x 10-6 segundos**

# Transmisión asíncrona

La transmisión asíncrona es un método de comunicación de datos en el cual la transmisión de los datos no requiere una sincronización precisa entre el emisor y el receptor. Es decir, los datos se envían en bloques o carácteres individuales, cada uno con su propio inicio y fin, lo cual permite que el receptor pueda interpretar cada bloque independientemente del tiempo en que llegue.

## Trama RS-232



* **START BIT (Bit de inicio):** Indica el comienzo de la transmisión de un carácter. Representa un único bit de valor cero (nivel bajo).
* **DATA BITS (Bits de datos):** Generalmente se envían 5 a 8 bits de datos, dependiendo de la configuración. Los bits se transmiten en orden de menos significativo a más significativo (LSB a MSB).
* **PARITY BIT (Bit de paridad) (opcional):** Puede ser par (even), impar (odd), ninguno (none), marca (mark) o espacio (space). Se utiliza para la detección de errores simples en la transmisión de datos. Este bit es opcional y depende de la configuración de la comunicación.
* **STOP BITS (Bits de parada):** Generalmente se utiliza 1 o 2 bits de parada. Un bit de valor 1 (nivel alto). Indican el final de la transmisión de un carácter.

## Razones por las que no se utilizan velocidades más altas

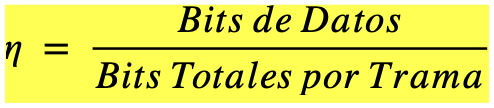
* Sobrecarga de Bits de Control
* Sincronización y Estabilidad del Reloj
* Tolerancia a Ruido y Errores
* Capacidades físicas del hardware

## Ventajas de una comunicación asíncrona

* El hardware es menos complejo y el software es más sencillo.
* Facilidad de re-sincronización. Inicio y parada independientes para cada carácter.
* Ideal para transmisiones de datos esporádicas.
* Uso eficiente de recursos, permitiendo modos de bajo consumo entre transmisiones.
* Menores costos de implementación.
* Compatibilidad con muchos dispositivos.
* Conexiones más simples porque utiliza menos pines.

## Rendimiento de una trama

El rendimiento de una trama en comunicaciones de datos se refiere a la eficiencia con la cual la información útil (los datos) es transmitida a través de un canal de comunicación. Es una medida que compara la cantidad de datos útiles con la cantidad total de bits transmitidos, incluyendo todos los bits de control y sobrecarga.



## Control de Flujo de datos

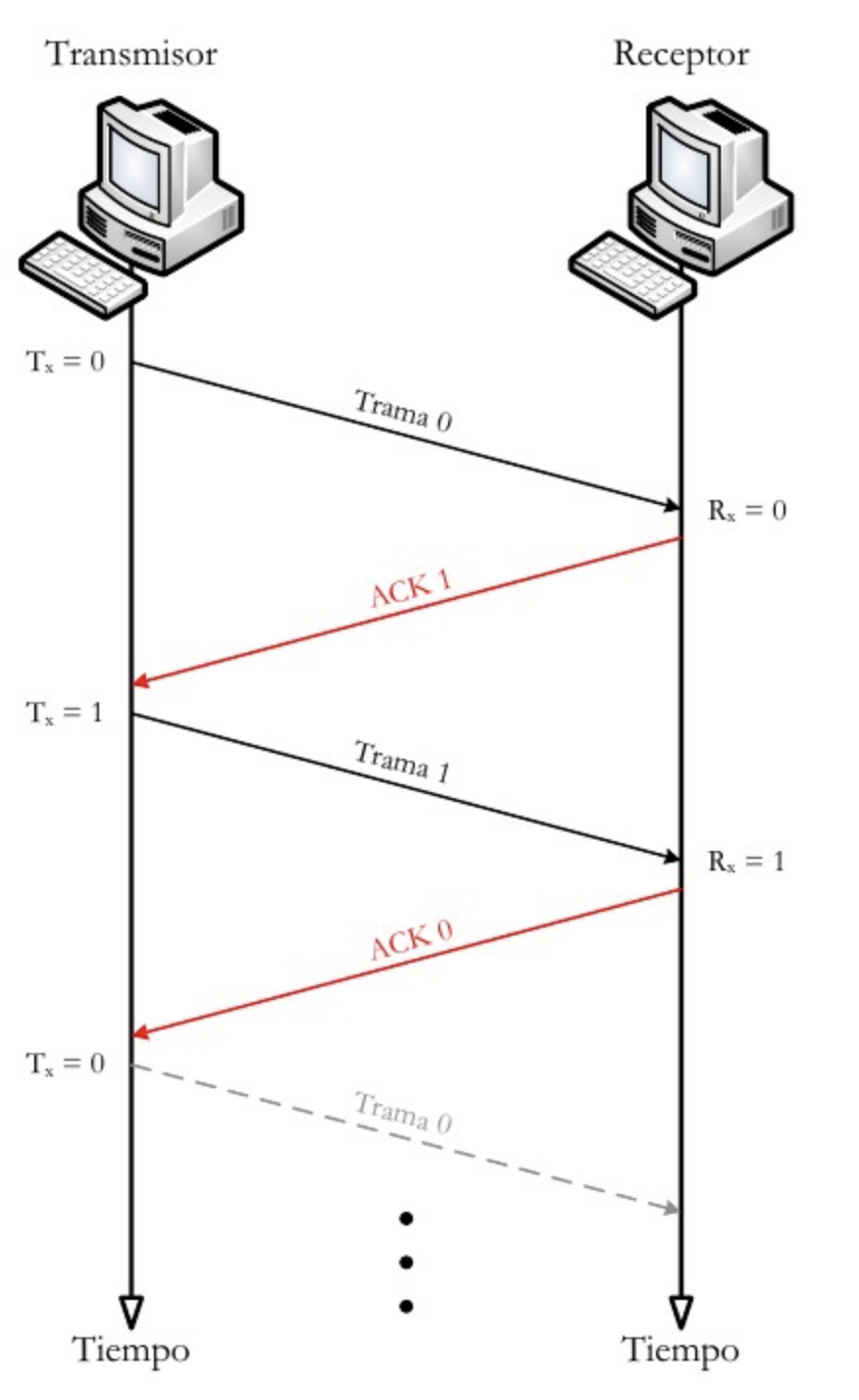
Si comenzamos a transmitir tramas a una velocidad mayor a la que el receptor puede

procesar, se pueden producir los siguientes problemas:

* **Desbordamiento del Buffer:** El receptor puede no ser capaz de almacenar todas las tramas entrantes, lo que resulta en la pérdida de datos.
* **Errores de Comunicación:** La comunicación se vuelve ineficaz debido a la pérdida de paquetes o la necesidad de transmitir los datos nuevamente

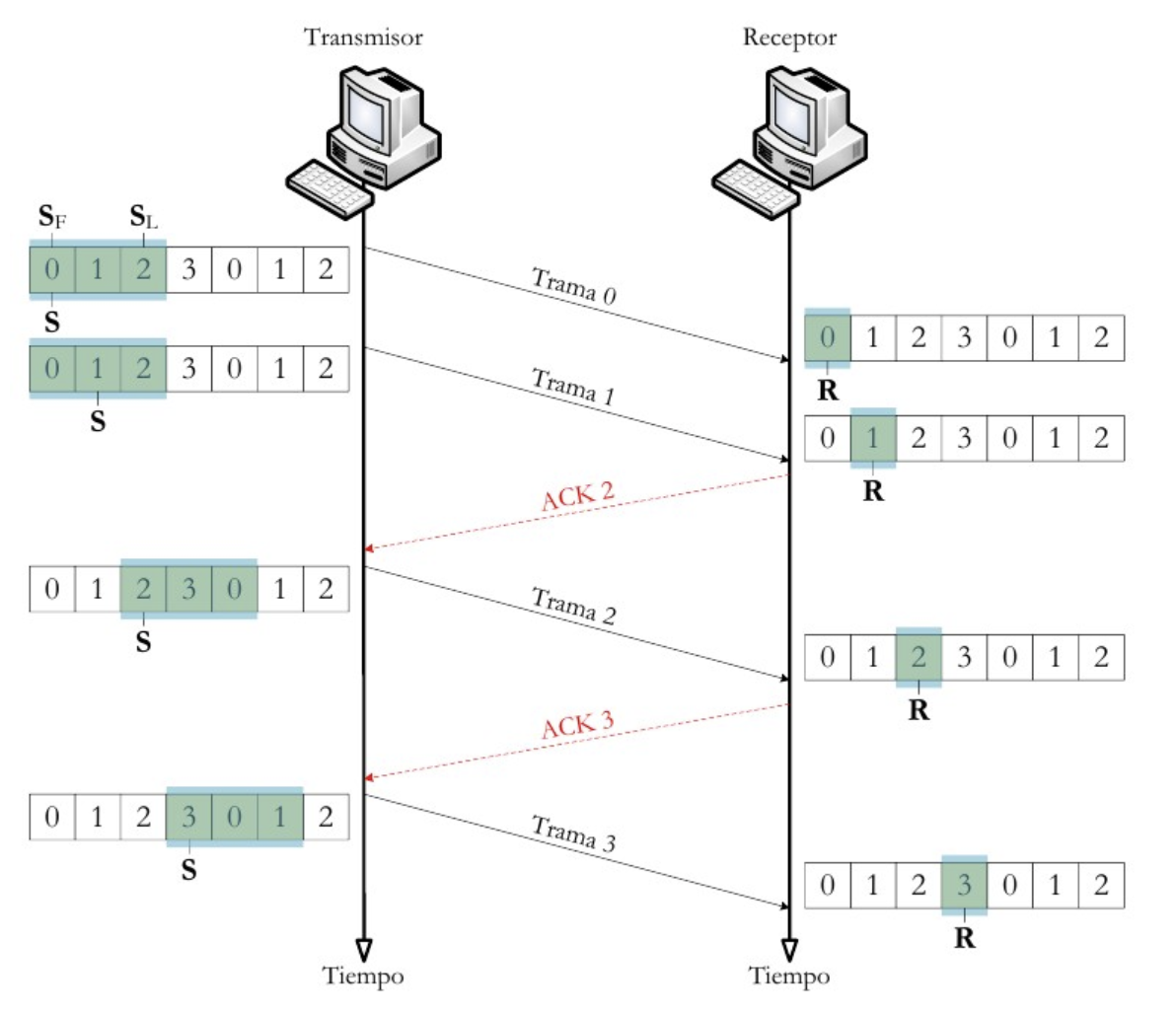
### Stop and Wait

* **Funcionamiento:**
* El transmisor envía una trama y luego espera a recibir un acuse de recibo (ACK) del receptor antes de enviar la siguiente trama.
* Si no recibe un ACK dentro de un tiempo específico (debido a que la trama o el ACK se perdió), reenvía la trama.
* **Ventajas:**
* Simple de implementar.
* Asegura que el receptor no sea sobrecargado ya que solo procesa una trama a la vez.
* **Desventajas:**
* Ineficiencia en el uso del canal, especialmente en canales de alta velocidad o alta latencia, ya que el transmisor está inactivo mientras espera el ACK.



### Sliding Window

* **Funcionamiento:**
* El transmisor puede enviar varias tramas antes de necesitar un ACK para la primera de ellas, dependiendo del tamaño de la ventana deslizante.
* El receptor puede enviar un ACK para varias tramas a la vez, lo que permite mayor eficiencia.
* El número de tramas que se pueden enviar sin recibir un ACK está limitado por el tamaño de la ventana.
* La ventana se “desliza” conforme se reciben ACKs, permitiendo el envío de nuevas tramas.
* **Ventajas:**
* Mayor eficiencia en el uso del canal, ya que permite la transmisión continua de tramas.
* Mejor uso de la capacidad del canal, especialmente en canales de alta latencia y alta velocidad.
* Reduce el tiempo de espera del transmisor y aumenta la tasa de transferencia de datos.
* **Desventajas:**
* Más complejo de implementar que el método Stop and Wait.
* Requiere más memoria y procesamiento para manejar la ventana deslizante y los buffers de datos.



## Detección de errores

### Control de Paridad

* **Funcionamiento:**
* En el método de paridad, se añade un bit de paridad a los datos que se transmiten. Este bit puede ser de paridad par o impar.
* Paridad par: El bit de paridad se ajusta de manera que el número total de bits 1 en la trama (incluyendo el bit de paridad) sea par.
* Paridad impar: El bit de paridad se ajusta de manera que el número total de bits 1 en la trama sea impar.
* Al recibir la trama, el receptor cuenta los bits 1 y verifica si coinciden con la paridad esperada.
* **Ventajas:**
* Simple y fácil de implementar.
* Requiere poco hardware adicional.
* **Desventajas:**
* No detecta todos los errores. Por ejemplo, si hay un número par de bits erróneos, el error no será detectado.
* Menor precisión en la detección de errores en comparación con CRC.

### CRC Cyclic Redundancy Check

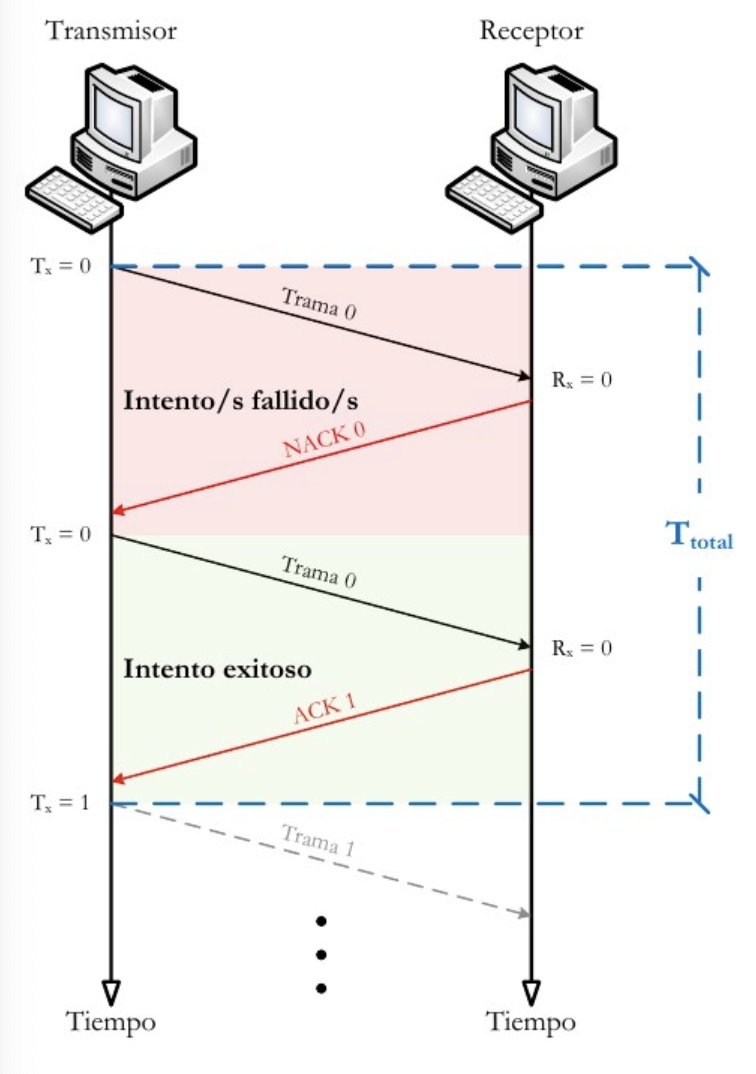
* **Funcionamiento:**
* CRC utiliza un algoritmo más complejo basado en la teoría de polinomios.
* Tanto el transmisor como el receptor comparten un polinomio generador predefinido.
* El transmisor realiza una división polinómica de los datos por el polinomio generador, y el residuo de esta división se añade al final de la trama como el FCS.
* Al recibir la trama, el receptor realiza la misma división polinómica y compara el residuo calculado con el FCS recibido.
* Si los residuos coinciden, se considera que la trama está libre de errores; de lo contrario, se detecta un error.
* **Ventajas:**
* Alta probabilidad de detección de errores, incluyendo errores de ráfaga.
* Detecta errores múltiples y la mayoría de los errores de mayor complejidad.
* **Desventajas:**
* Más complejo de implementar y requiere más procesamiento que el control de paridad.
* Requiere más bits adicionales (el tamaño del FCS es mayor que el bit de paridad).

Entre los dos métodos, CRC tiene una probabilidad mucho más alta de detectar errores en la trama en comparación con el Control de Paridad. Esto se debe a su capacidad de detectar múltiples bits erróneos y errores de ráfaga, a la complejidad de su algoritmo y al tamaño del campo de verificación.

## Manejo de errores

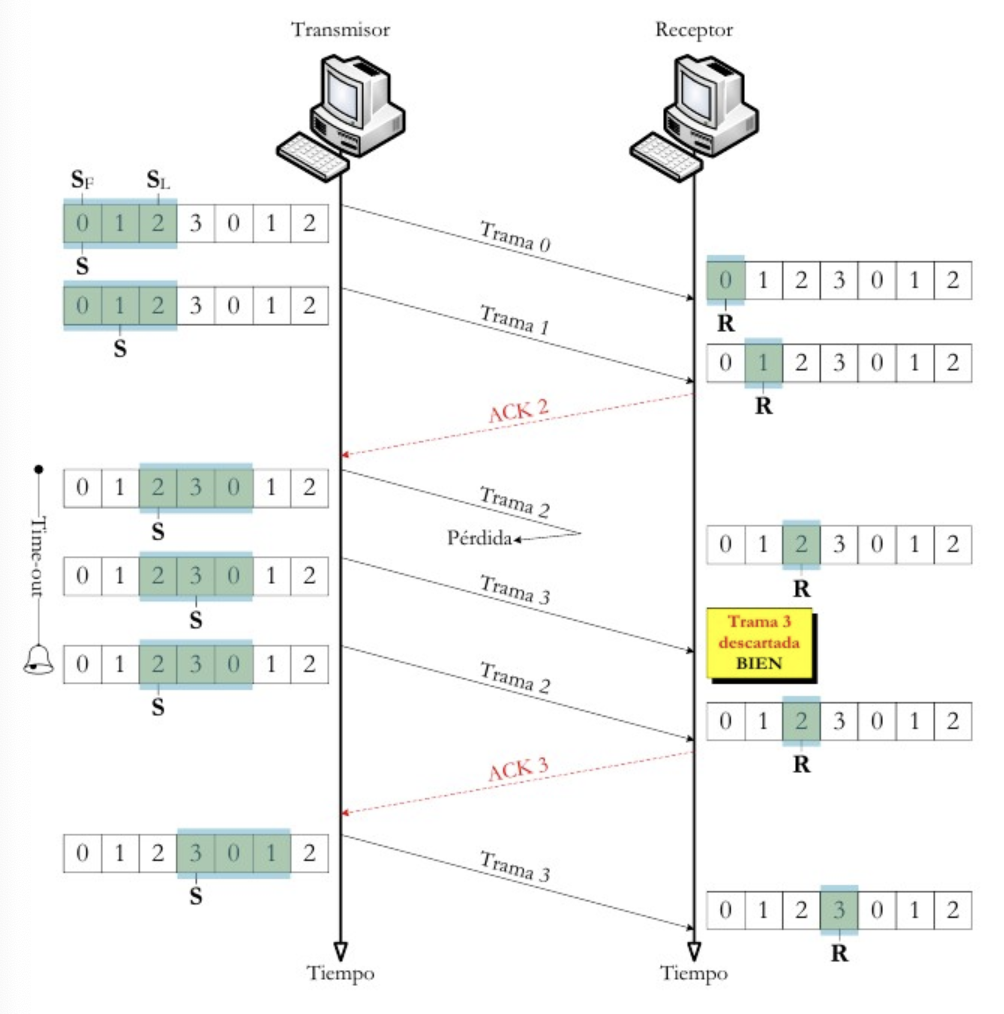
### ARQ Stop and Wait

* **Funcionamiento:**
* El transmisor envía una trama y espera un acuse de recibo (ACK) del receptor antes de enviar la siguiente trama.
* Si el receptor detecta un error en la trama recibida, envía un mensaje de no acuse de recibo (NACK).
* Si el transmisor recibe un NACK o no recibe un ACK dentro de un tiempo determinado, retransmite la trama.
* **Ventajas:**
* Simple de implementar y entender.
* Asegura que cada trama es correctamente recibida antes de enviar la siguiente.
* **Desventajas:**
* Ineficiente en términos de utilización del canal, ya que el transmisor pasa mucho tiempo esperando ACKs.
* Menor throughput en enlaces de alta latencia o alta velocidad.



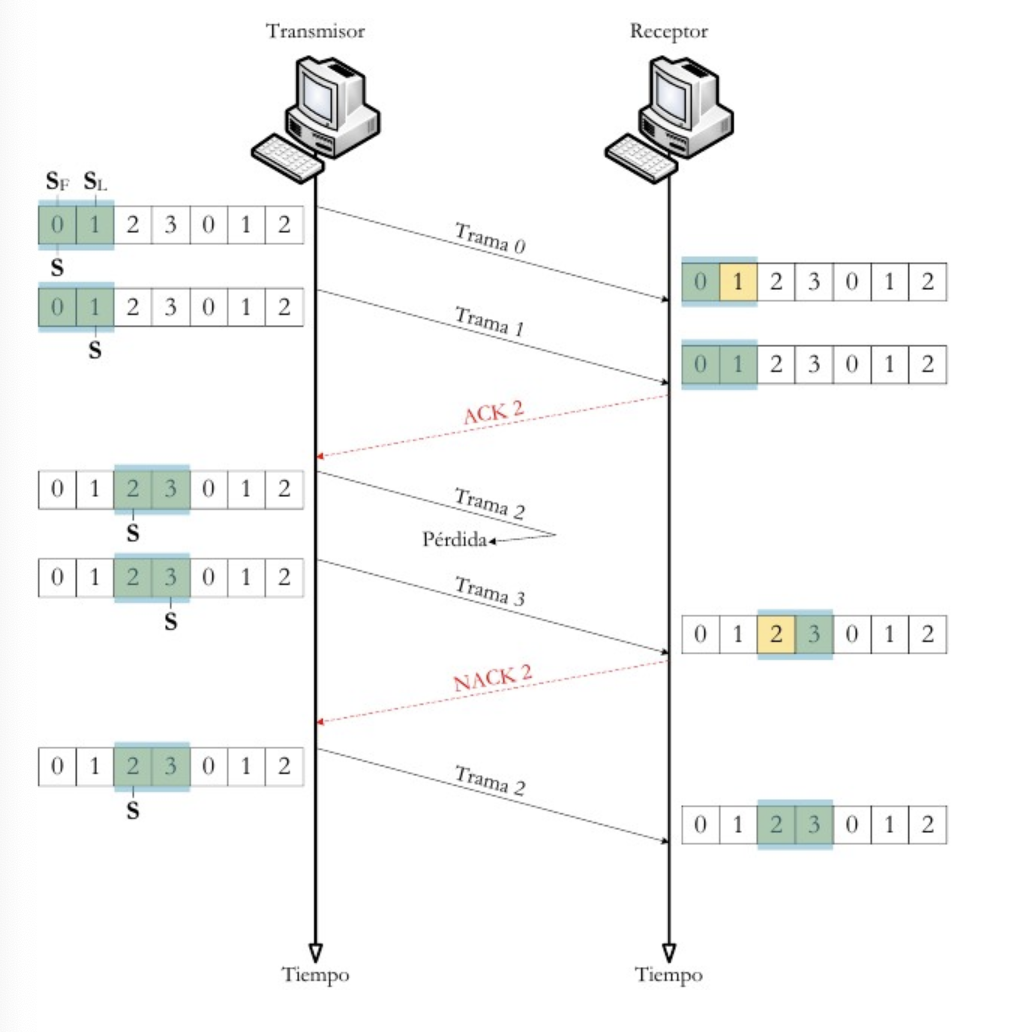
### ARQ Go Back to N

* **Funcionamiento:**
* El transmisor puede enviar varias tramas antes de recibir ACKs, hasta un número máximo de tramas (N), determinado por el tamaño de la ventana deslizante.
* El receptor envía ACKs para cada trama recibida sin errores.
* Si el receptor detecta una trama con error, descarta esa trama y todas las tramas siguientes hasta que reciba la trama correcta.
* El transmisor, al no recibir ACKs para las tramas con errores, retransmite desde la trama con error (y todas las subsiguientes).
* **Ventajas:**
* Mejor utilización del canal en comparación con Stop and Wait, ya que permite múltiples tramas en tránsito.
* Mayor throughput en enlaces de alta velocidad y alta latencia.
* **Desventajas:**
* Ineficiencia en términos de retransmisión, ya que puede retransmitir tramas correctamente recibidas (tramas posteriores a la que tenía error).



### ARQ Selective Reject

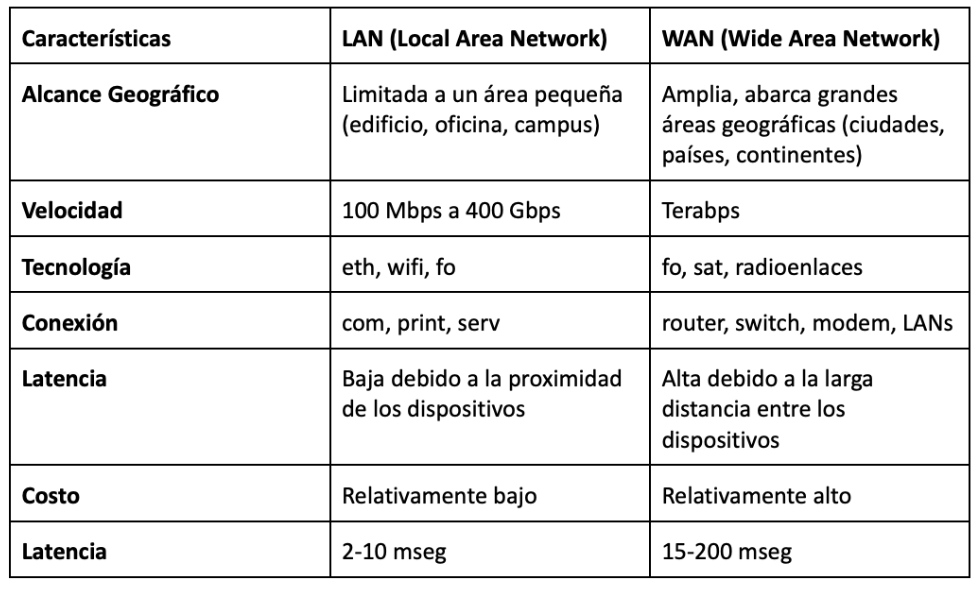
* **Funcionamiento:**
* Similar a Go-Back-N, pero más eficiente en la retransmisión.
* El transmisor puede enviar múltiples tramas antes de recibir ACKs, hasta un número máximo de tramas (N).
* El receptor envía ACKs individuales para cada trama correctamente recibida.
* Si el receptor detecta una trama con error, envía un NAK para esa trama específica.
* El transmisor retransmite únicamente las tramas para las cuales ha recibido NAKs.
* **Ventajas:**
* Mayor eficiencia en la utilización del canal, ya que sólo se retransmiten las tramas con errores.
* Mayor throughput y mejor manejo de errores en comparación con Go-Back-N.
* **Desventajas:**
* Más complejo de implementar debido a la necesidad de mantener un buffer y gestionar las tramas fuera de secuencia.
* Requiere más memoria y procesamiento en el receptor.



## Direccionamiento

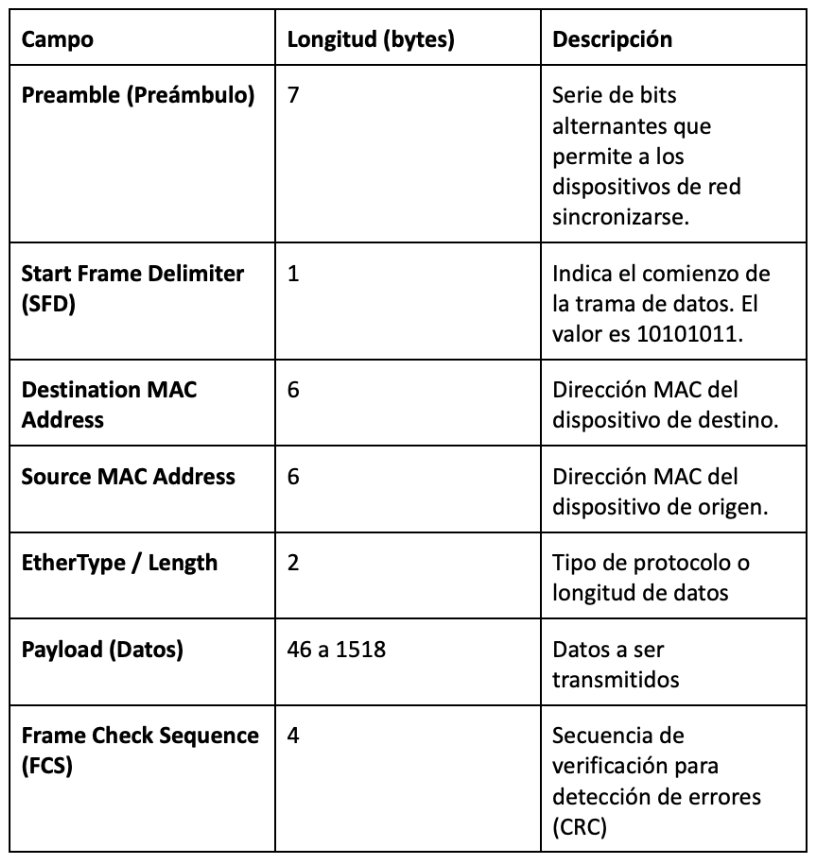
El direccionamiento para poder reconocer y saber quien envía y quien debe recibir la información que está en el medio compartido se realiza mediante la MAC Address.

## LAN y WAN



Velocidades LAN??

# Ethernet



## Control de flujo

El control de flujo en ethernet es descartar. No tiene un método para decirle al otro que mande más lento

## Control de acceso al medio

### Round Robin

* Es un método de control de flujo que asigna el uso del canal a cada dispositivo en turnos fijos.
* Funciona en un orden cíclico, donde cada dispositivo tiene una cantidad de tiempo predefinida para transmitir datos antes de pasar el control al siguiente dispositivo en la cola.
* Este método es justo, ya que cada dispositivo tiene igual oportunidad de acceso al canal.
* Simple y fácil de implementar.
* Garantiza un acceso equitativo al canal para todos los dispositivos.
* Puede ser ineficiente si algunos dispositivos no tienen datos para enviar durante su turno.
* El tiempo de espera puede ser alto si hay muchos dispositivos en la red.

### Reservation

* En el método de Reservation, los dispositivos reservan el canal antes de transmitir datos.
* Esto puede hacerse mediante una señal previa o una fase de reserva en la que los dispositivos indican su intención de usar el canal.
* Una vez que un dispositivo ha reservado el canal, tiene el derecho exclusivo de transmitir durante el tiempo reservado.
* Reduce las colisiones y asegura que los dispositivos con datos para transmitir puedan hacerlo de manera ordenada.
* Puede ser eficiente en redes con alta carga de tráfico y dispositivos que necesitan transmitir grandes cantidades de datos.
* Puede requerir una fase de reserva adicional, lo que añade un pequeño overhead.
* Los dispositivos deben esperar su turno de reserva, lo que puede introducir latencia.

### Contention

* En el método de Contention, los dispositivos compiten por el uso del canal.
* Los dispositivos intentan transmitir cuando el canal está libre, pero pueden ocurrir colisiones si dos o más dispositivos transmiten simultáneamente.
* Protocolos como CSMA/CD (Carrier Sense Multiple Access with Collision Detection) son ejemplos de métodos de contention.
* No requiere una fase de reserva previa, permitiendo un acceso más dinámico.
* Puede ser más eficiente en redes con baja carga de tráfico y pocos dispositivos.
* Las colisiones pueden llevar a retransmisiones, reduciendo la eficiencia del canal.
* El rendimiento puede degradarse significativamente a medida que aumenta el número de dispositivos o la carga de tráfico.

## Detección de errores

### FCS (Frame Check Sequence)

Es un campo de 4 bytes al final de cada trama Ethernet que contiene un valor de verificación calculado mediante un algoritmo de Cyclic Redundancy Check (CRC). Cuando un dispositivo receptor recibe una trama, recalcula el valor CRC y lo compara con el valor FCS en la trama. Si los valores no coinciden, indica que ha ocurrido un error durante la transmisión y la trama es descartada.

## Colisión

Una colisión ocurre en un entorno de red de Ethernet compartida y es cuando dos dispositivos intentan transmitir datos simultáneamente en el mismo segmento de red.

## Direcciones MAC

Las tramas Ethernet utilizan direcciones MAC (Media Access Control) para identificar de manera única los dispositivos en la red. Estás son asignadas de la siguiente manera:

* 3 bytes (OUI) pertenecientes a cada fabricante, este debe solicitarlos a la IEEE.
* 3 bytes que cada fabricante le asigna al dispositivo.

## Repetidores (Hubs)

Un repetidor es un dispositivo de red que amplifica y regenera las señales de datos para extender el alcance de la transmisión en una red.

El repetidor recibe una señal de datos en un segmento de red, la amplifica y la retransmite a otro segmento. Esto ayuda a superar las limitaciones de distancia impuestas por la atenuación de la señal en el cableado.

Trabaja en el nivel físico (capa 1) del modelo OSI. En esta capa, el repetidor no interpreta los datos que transmite, simplemente amplifica la señal.

## Bridge

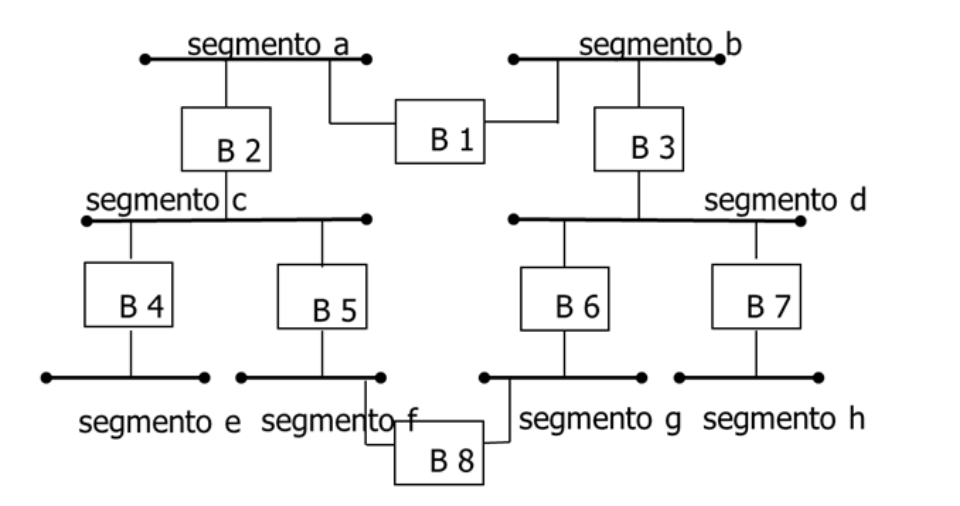
Es un dispositivo de red utilizado para conectar y segmentar diferentes redes locales (LANs) o segmentos de una misma red. Su principal función es filtrar, reenviar o bloquear tramas de datos según la dirección MAC de destino, mejorando la eficiencia y la gestión del tráfico de red.

Un bridge opera en la capa de enlace de datos (capa 2) del modelo OSI. En esta capa, los bridges trabajan con direcciones MAC y son responsables de la transferencia de datos entre segmentos de red, utilizando información de direcciones físicas para tomar decisiones de reenvío. Esto evita que se produzca colisión.

**¿Qué protocolo se utiliza para resolver los bucles que se pueden generar al unir varios bridges o switches que permiten tener más de un camino para vincular dos equipos?**

Spanning Tree Protocol (STP)

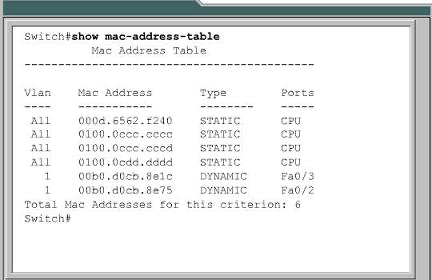
Se utiliza para seleccionar un único camino entre dos dispositivos para evitar la duplicación de tramas. Se analizan las rutas hacia todos los dispositivos y se bloquean las rutas duplicadas o menos eficientes.



## Switches

Un switch es un dispositivo de red que conecta múltiples dispositivos en una red local (LAN) y utiliza conmutación de paquetes para recibir, procesar y reenviar datos a dispositivos de destino específicos.

Opera principalmente en la capa de enlace de datos (capa 2) del modelo OSI. Hay algunos switches que pueden operar en la capa de red (capa 3), son los switches routers.



# WLAN

Las redes Wireless LAN son redes que permiten la comunicación y el intercambio de datos entre dispositivos utilizando ondas de radio en lugar de cables físicos.

La Wi-Fi Alliance es la organización responsable de la creación y gestión de la certificación Wi-Fi, basada en el estándar IEEE 802.11. La Wi-Fi Alliance es una organización mundial de la industria sin fines de lucro que promueve la adopción y evolución de las tecnologías Wi-Fi.

## Componentes WLAN

* Distribución: puntos de acceso (AP) y equipos mixtos
* Adaptadores de red inalámbrica o tarjetas de red: WNIC
* Antenas
* **Access Points (AP):** Un punto de acceso (AP) es un dispositivo que puede actuar como punto central de una red inalámbrica independiente (figura 9.1). Tiene una dirección IP que permite configurarlo y su función principal es proveer a los clientes de acceso a la red inalámbrica. Las funciones de enrutamiento y direccionamiento las suele delegar en servidores (routers).
* **Wireless Network Interface Cards (WNIC):** Estos adaptadores, dependiendo de su punto de interconexión con el dispositivo, pueden dividirse en los siguiente:
* Adaptadores integrados
* Tarjetas PCMCIA
* Tarjetas PCI
* Adaptadores USB

## Antenas

* **Isotrópica:** es una antena teórica que emite la misma potencia de radiación en todas las direcciones. Su diagrama de radiación es una esfera perfecta.
* **Omnidireccional:** es una antena que radia la misma cantidad de potencia en todas las direcciones de un plano de emisión. Su diagrama de radiación sería un toroide. Son las más utilizadas en las redes WLAN, ya que cubren de manera uniforme toda la superficie en la que se debe dar servicio inalámbrico.
* **Direccional:** es una antena que emite la máxima potencia en una dirección determinada. Suelen utilizarse para crear uniones punto a punto o conectar zonas muy alejadas. Pueden ser unidireccionales o bidireccionales.
* **Sectorial:** es una antena que emite su máxima potencia en un sector determinado. Suelen utilizarse en redes urbanas. Pueden cubrir sectores de 120°, 60°, etc..

### Características de una antena

* **Ganancia:** es el incremento de potencia de una antena en la dirección de máxima radiación en relación con una antena modelo. Puede medirse en dBi (decibelios respecto a una antena isotrópica) o dBd (decibelios respecto a un dipolo), dependiendo de la antena usada como referencia. Un dipolo posee un diagrama de radiación omnidireccional. Si el resultado es positivo, indica mayor potencia de radiación que el modelo; si, por el contrario, el resultado es negativo, indica menor potencia de radiación.
* **Ancho de banda:** son las bandas de frecuencia en las cuales trabaja la antena de manera óptima.
* **Eficiencia:** es la relación entre la potencia emitida por la antena y la que le es suministrada por el equipo transmisor. Cuanto mayor sea la eficiencia menor será la cantidad de potencia que se perderá en forma de calor.

## Modos de operación WLAN

* **Redes ad hoc:** es una red inalámbrica descentralizada. En ella todos los equipos están conectados sin necesidad de un nodo central que realice las funciones de router. Este tipo de redes no necesita ni puntos de acceso ni dispositivos mixtos; cada equipo actúa como punto de acceso y cliente inalámbrico.
* **Redes en infraestructura:** estas redes son aquellas en las cuales los dispositivos se conectan a la red mediante puntos de acceso. Añadiendo AP adicionales se aumentará el alcance de la red y el número de usuarios. Frente a las redes ad hoc, ofrecen una mejor escalabilidad, así como un sistema de seguridad centralizado.

## Tipos de Autenticación

* **Open System Authentication:** Es el método más básico y menos seguro. Permite que cualquier dispositivo se conecte a la red sin necesidad de autenticación. Es vulnerable a ataques de intrusión.
* **Shared Key Authentication:** Requiere que los dispositivos que intentan conectarse proporcionen una clave compartida. Esta clave se comparte entre el punto de acceso (AP) y los dispositivos cliente. Es más seguro que el método de sistema abierto, pero aún es susceptible a ataques de fuerza bruta.
* **WPA/WPA2-PSK:** Utiliza una clave precompartida para autenticar dispositivos en la red. Es más seguro ya que emplea cifrado AES (Advanced Encryption Standard) para proteger la comunicación.
* **802.1X/EAP:** Es un método más robusto que requiere un servidor de autenticación centralizado. Los dispositivos deben autenticarse utilizando credenciales individuales, como nombres de usuario y contraseñas, certificados digitales o métodos biométricos.

## Tipos de Cifrado

* **WEP (Wired Equivalent Privacy):** Fue el primer estándar de cifrado para WLAN, pero es muy vulnerable a los ataques y ya no se recomienda su uso.
* **WPA (Wi-Fi Protected Access) y WPA2:** Utilizan **cifrado TKIP** (Temporal Key Integrity Protocol) y AES para proteger la comunicación. WPA2 es más seguro que WPA y es el estándar recomendado en la actualidad.
* **WPA3:** Es el estándar más reciente y ofrece mejoras en seguridad sobre WPA2. Utiliza **cifrado AES-GCM** (Galois/Counter Mode) y ofrece protección contra ataques de fuerza bruta incluso si se interceptan las comunicaciones.
* **AES (Advanced Encryption Standard):** Es un algoritmo de cifrado simétrico utilizado para proteger la confidencialidad de los datos transmitidos.

## Ataques WLAN

* **Ataque de diccionario:** consiste en intentar averiguar una contraseña probando todas las palabras de una lista, como puede ser un diccionario. Conociendo alguno de los parámetros que intervienen en la generación de la clave se reduce el tiempo de proceso. Por ejemplo, en el sistema de cifrado AES sobre redes inalámbricas, se incorpora la SSID para generar la contraseña. Si se hace visible el nombre del punto de acceso se estarán facilitando los ataques por diccionario. Si se oculta el nombre del AP, sólo podrán acceder a la red aquellos usuarios que lo conozcan por adelantado, aunque existen programas que permiten averiguarlo.
* **Ataque de fuerza bruta:** consiste en probar todas las combinaciones posibles hasta encontrar la que permite el acceso. Es menos eficiente que el ataque por diccionario. Para provocar que sea tan costoso en tiempo que no merezca la pena intentarlo, se deberá aumentar la fortaleza de la contraseña. Utilizaremos para ello el máximo número de caracteres permitidos por el sistema de acceso para la contraseña, así como los diferentes tipos de caracteres posibles: mayúsculas, minúsculas, números y símbolos. También es recomendable que los caracteres se dispongan aleatoriamente sin formar palabras reales.