UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

CARRERA DE INGENIERÍA EN TELECOMUNICACIONES

COMUNICACIÓN DIGITAL

ENERO 2025 JULIO 2025

INDICE

Capítulo IV

1. INTRODUCCIÓN

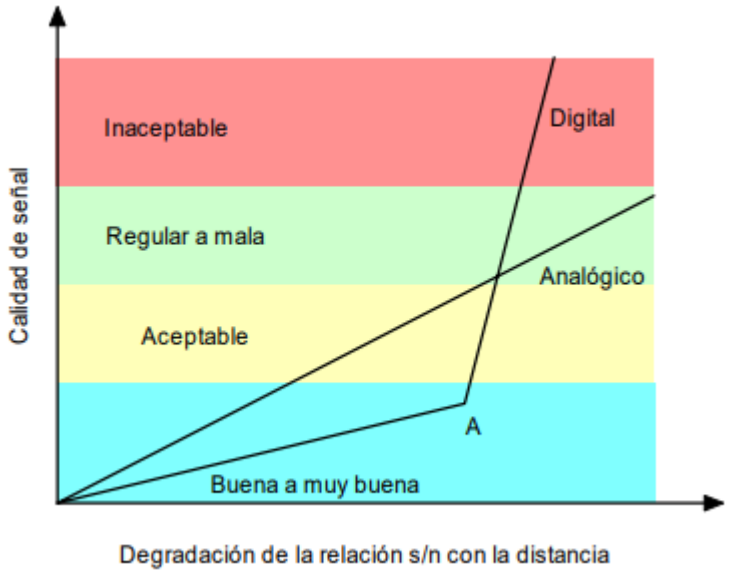
La codificación de canal es un concepto fundamental en el campo de las comunicaciones digitales que se utiliza para mejorar la confiabilidad de la transmisión de datos a través de un canal de comunicación con ruido.

Cuando los datos se transmiten a través de un canal, como una línea telefónica o una conexión inalámbrica, pueden ocurrir errores debido al ruido o interferencias presentes en el medio. Estos errores pueden distorsionar o corromper la información original, lo que resulta en una pérdida de datos o en una interpretación incorrecta de los mismos.

La codificación de canal se utiliza para mitigar estos errores y mejorar la calidad de la transmisión. Consiste en añadir información adicional, llamada redundancia, a los datos originales antes de transmitirlos. Esta redundancia se utiliza para detectar y corregir los errores en el receptor.

Existen diferentes técnicas de codificación de canal, como la codificación de bloque, la codificación convolucional y la codificación Reed-Solomon, entre otras. Cada técnica tiene sus propias características y ventajas dependiendo del tipo de canal y los requisitos de transmisión.

La codificación de bloque divide los datos en bloques de bits y añade bits de paridad para permitir la detección y corrección de errores. La codificación convolucional utiliza una secuencia de registros de desplazamiento y compuertas lógicas para codificar los datos y proporcionar una mayor resistencia al ruido. La codificación Reed-Solomon es especialmente útil para corregir errores en canales con pérdida de datos, como en las transmisiones satelitales.



En los sistemas analógicos la degradación de la señal es suave; es decir, la relación señal a ruido disminuye lentamente con la distancia y la señal, aunque con ruido, puede recibirse en condiciones aceptables en un rango considerable de distancias. En los sistemas digitales, por el contrario, la señal deja de recibirse cuando la tasa de errores aumenta por encima del valor que es capaz de manejar el receptor. La degradación en estas condiciones es muy brusca y se pasa rápidamente de una zona de recepción satisfactoria a una de recepción nula.

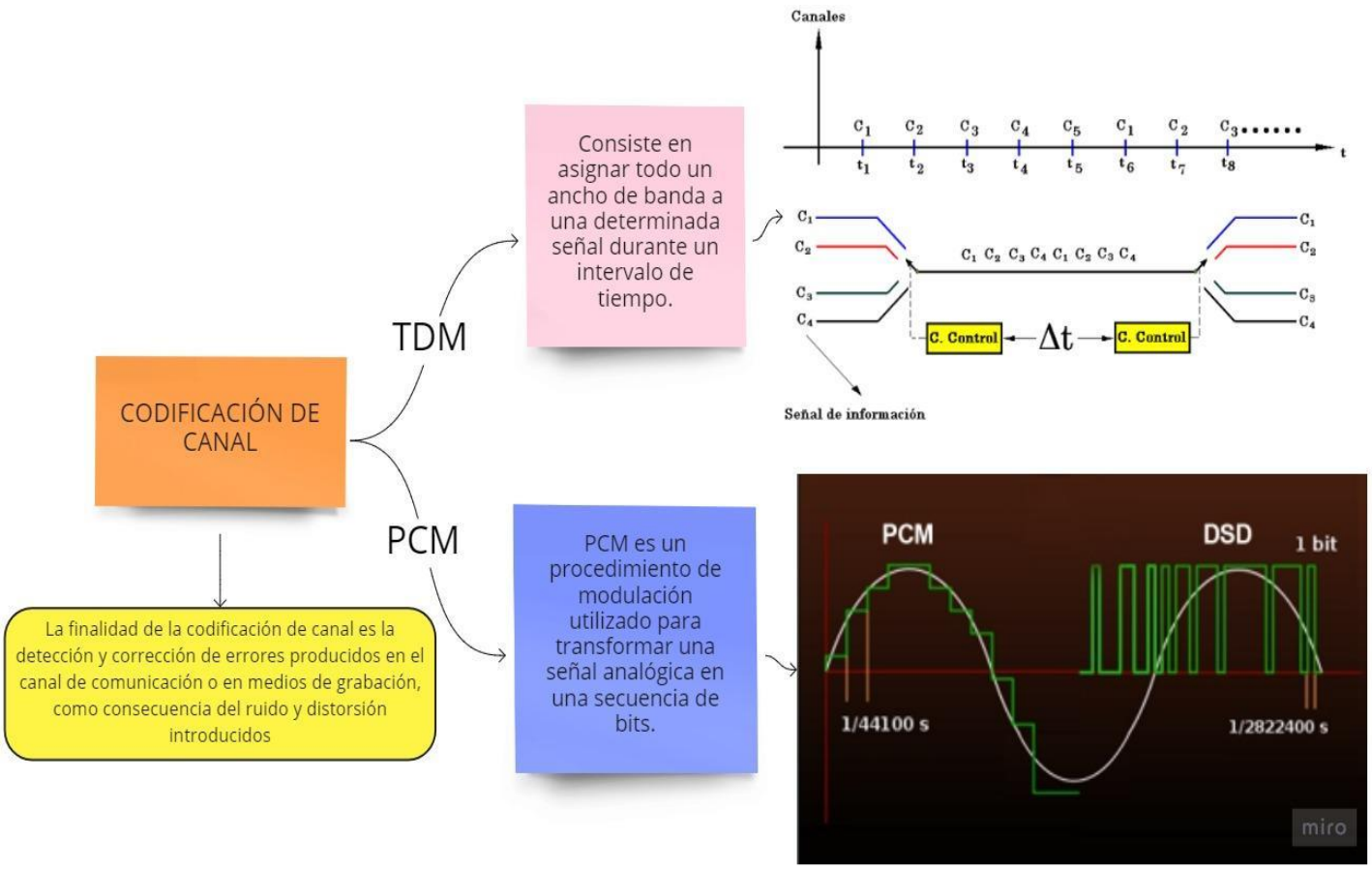
2. CODIFICACION DE CANAL

La codificación de canal juega un papel muy importante tanto en uno como en otro aspecto, ya que, como demostró Shannon en 1948, con una codificación apropiada se pueden reducir los errores producidos por un canal (líneas telefónicas, radioenlaces, enlaces vía satélite, etc.) o un soporte de almacenamiento (memorias de semiconductores, bandas magnéticas, discos compactos, etc.), ambos ruidosos, sin sacrificar ni la tasa de transmisión, ni su potencia, ni su ancho de banda. [1]

Existen dos tipos de codificación por canal:

1. TDM (Multiplexación por División de Tiempo).

2. PCM (Multiplexación por División de Pulsos) MIC en español**.**



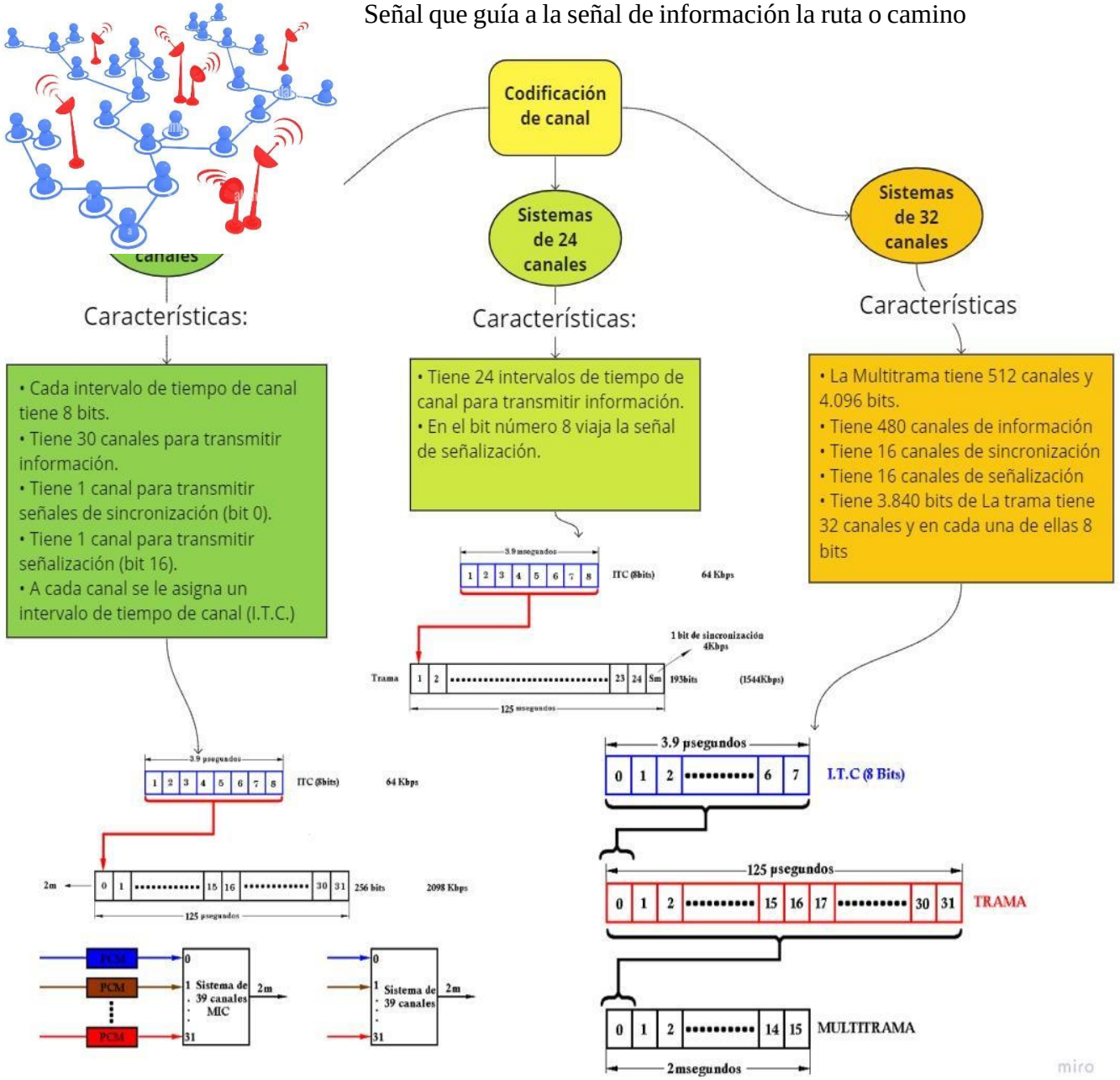
2.1. Multiplexado de la señal digital.

Multiplexado es la transmisión de información (en cualquier forma) de más de una fuente a más de un destino a través del mismo medio (instalación) de transmisión. Aunque las transmisiones sucedan en la misma instalación, no necesariamente suceden al mismo tiempo. El medio de transmisión puede ser un par de alambres metálicos, un cable coaxial,

un teléfono móvil PCS, un sistema de microondas terrestres de radio, uno de microondas satelitales o un cable de fibra óptica.

2.2. SEÑALIZACIÓN.

Señal que guía a la señal de información la ruta o camino



correcto para llegar desde el transmisor al receptor. Esta no nos permite entregar mucha información por lo que la CCITT normaliza lo siguiente.

La señalización busca la ruta o camino correcto para que lleguen los datos en buen estado.

Tipos de señalización:

✔ **Canal común:** Viaja por el mismo canal que la información

✔ **Canal Asociado:** La señal de señalización viaja por su lado independiente

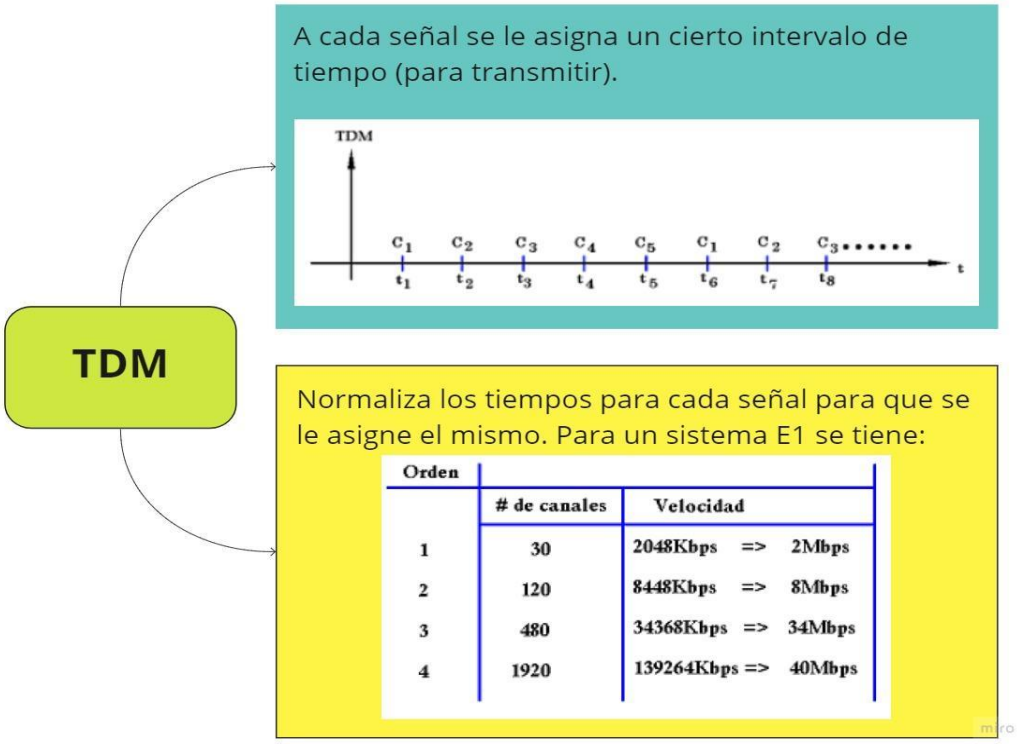
3. TÉCNICAS DE MULTIPLEXACIÓN Y ACCESO MÚLTIPLE

3.1. SISTEMA TDM (MÚLTIPLEXACION POR DIVISIÓN DE TIEMPO)

Es una técnica que permite la transmisión de señales digitales y cuya idea consiste en ocupar un canal (normalmente de gran capacidad) de trasmisión a partir de distintas fuentes. [2]

La multiplexación por división de tiempo (MDT) o (TDM) es el tipo de multiplexación más utilizado en la actualidad, especialmente en los sistemas de transmisión digitales. En ella, el ancho de banda total del medio de transmisión es asignado a cada canal durante una fracción del tiempo total (intervalo de tiempo). El multiplexor por división en el tiempo muestrea, o explora, cíclicamente las señales de entrada (datos de entrada) de los diferentes usuarios, y transmite las tramas a través de una única línea de comunicación de alta velocidad.

Los TDM funcionan a nivel de bit o a nivel de carácter. En un TDM a nivel de bit, cada trama contiene un bit de cada dispositivo explorado. El TDM de caracteres manda un carácter en cada canal de la trama. El segundo es generalmente más eficiente, dado que requiere menos bits de control que un TDM de bit. La operación de muestreo debe ser lo suficientemente rápida, de forma que cada buffer sea vaciado antes de que lleguen nuevos datos. [2]

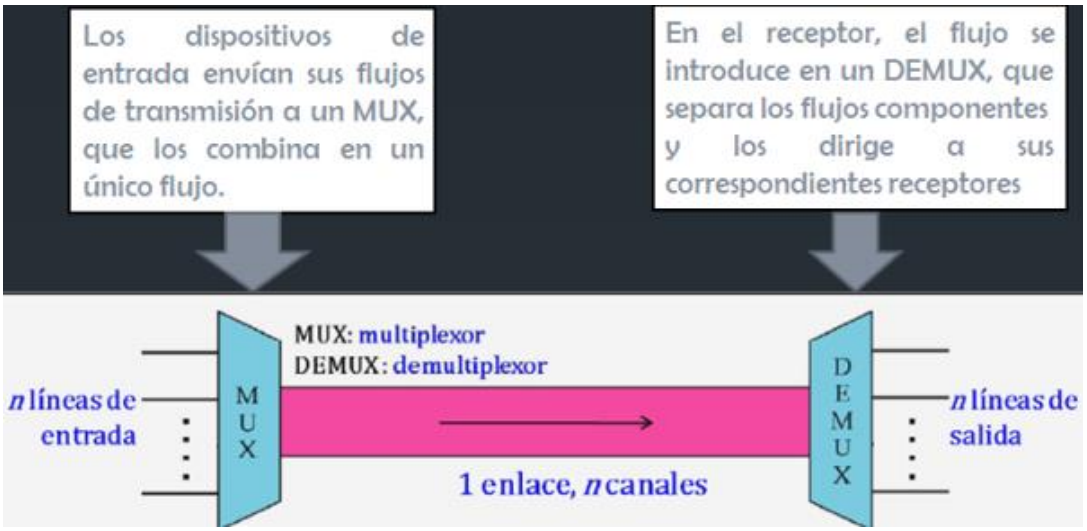


Ventajas de TDM	*Desventajas de TDM*
✔ Esto usa unos enlaces solos ✔ Esto no requiere al portador preciso que empareja a ambo final de los enlaces. ✔ El uso de la capacidad es alto. ✔ Cada uno para ampliar el número de usuarios en un sistema en un coste bajo. ✔ No hay ninguna necesidad de incluir la identificación de la corriente de tráfico en cada paquete	✔ La sensibilidad frente a otro problema de usuario es alta ✔ El coste inicial es alto ✔ La complejidad técnica, es más ✔ El problema del ruido para la comunicación análoga tiene el mayor efecto.

Tabla 1 Ventajas y Desventajas de TDM

3.2. SEÑAL FDM (MÚLTIPLEXACION POR DIVISIÓN DE LA FRECUENCIA)

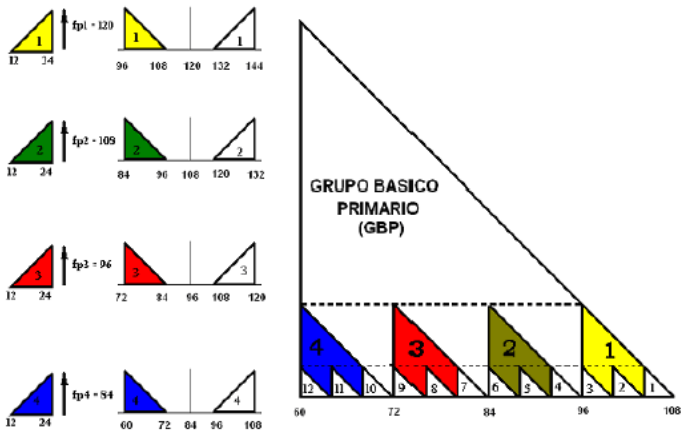
En las telecomunicaciones, la multiplexación por división de frecuencia es una técnica mediante la cual el ancho de banda total disponible en un medio de comunicación se divide en una serie de sub-bandas de frecuencias levemente distintas, cada una de las cuales se utiliza para transportar una señal separada. [2]



2.2.1 TÉCNICAS

GRUPO BÁSICO PRIMARIO

- ✔ Se agrupa en 4 pregrupos.
- ✔ Rango de frecuencia de 60KHz a 108 KHz
- ✔ Ancho de banda de 48 KHz



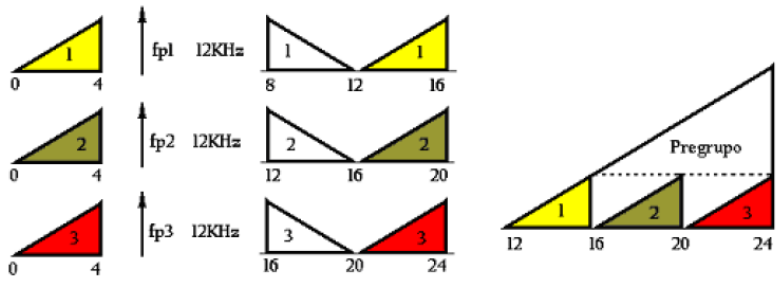
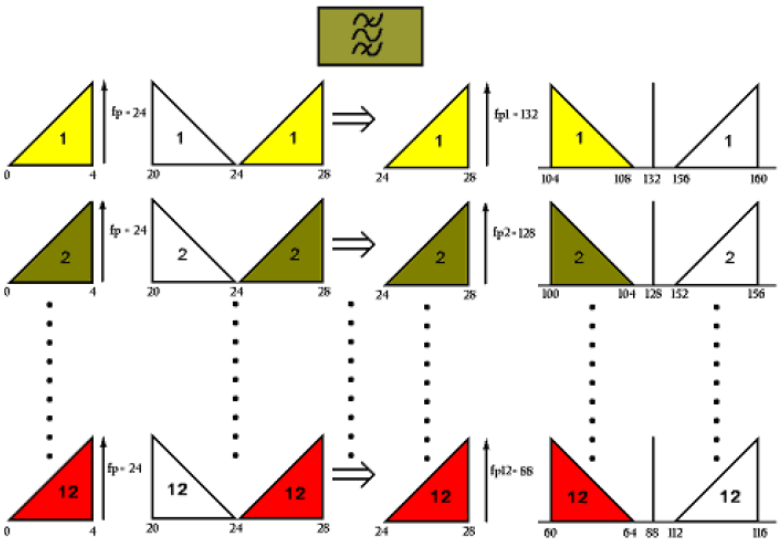
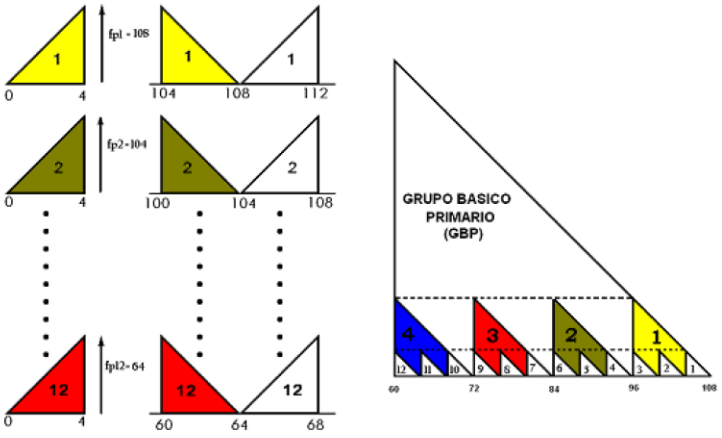
Se basa en tener tres canales de 4Khz cada uno, y multiplexarlo con una frecuencia estándar de 12Khz. Esta técnica se llama pregrupo.	
PREMODULACIÓN: Características ✔ Tiene dos modulaciones. ✔ En la primera modulación a todos los canales se la modulan con la misma frecuencia. ✔ La segunda modulación se le hace a diferentes frecuencias.	
MODULACIÓN DIRECTA: **Características** ✔ La relación señal ruido comparado con la técnica anterior mejora, pero los costos se incrementan.	

Tabla 2 Tipos de grupos básicos primarios

GRUPO BÁSICO SECUNDARIO O SUPERGRUPO

Características.

- ✔ Tiene 60 canales telefónicos por lo tanto se tiene 5 grupo básicos primarios (GBP).
- ✔ Ancho de banda 240 KHz: GBS = 5*GBP = 5*48 = 240
- ✔ Rango de frecuencia de 312 KHz a 552 KHz: 240+312=552
- ✔ Trabaja en la banda lateral superior.

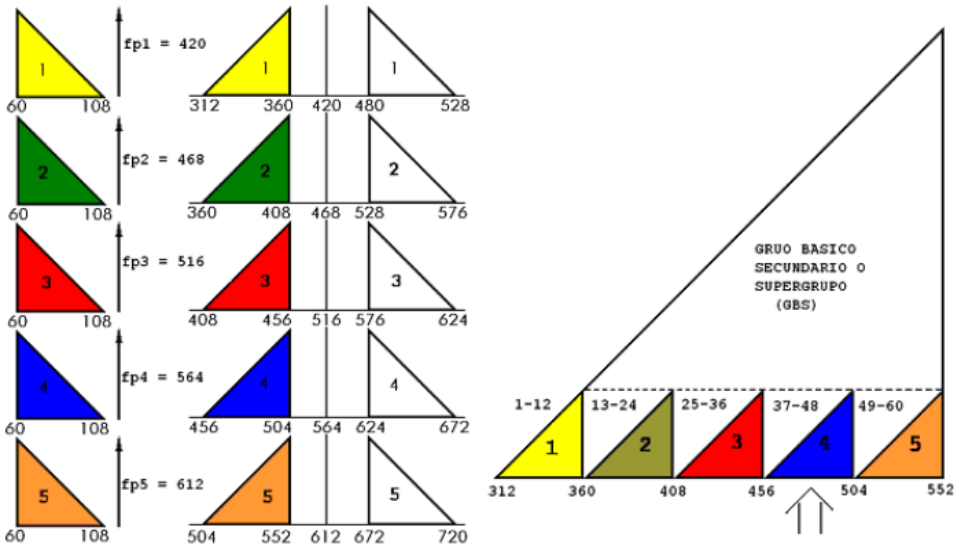


Ilustración 6 Grupo básico Secundario

GRUPO BÁSICO TERCEARIO

Características

- ✔ Tiene 300 canales. 60 *5= 300
- ✔ Utiliza 5 grupos básicos secundarios.

GBT =5*GBS =5*GBP= 5*5*48= 1200KHz

- ✔ Con un ancho de banda de 1200 KHZ:

AB = 1200 + 4(8) = 1.232 KHz

- ✔ Cuando se trabaja con bandas anchas muy grandes se habla que se tiene Guarda Bandas.
- ✔ Guarda Banda es el espacio que hay entre las bandas para seguridad de transmisión.
- ✔ Hay Guarda Bandas de 8, 16, 32 KHz.
- ✔ Utilizamos la banda lateral izquierda.

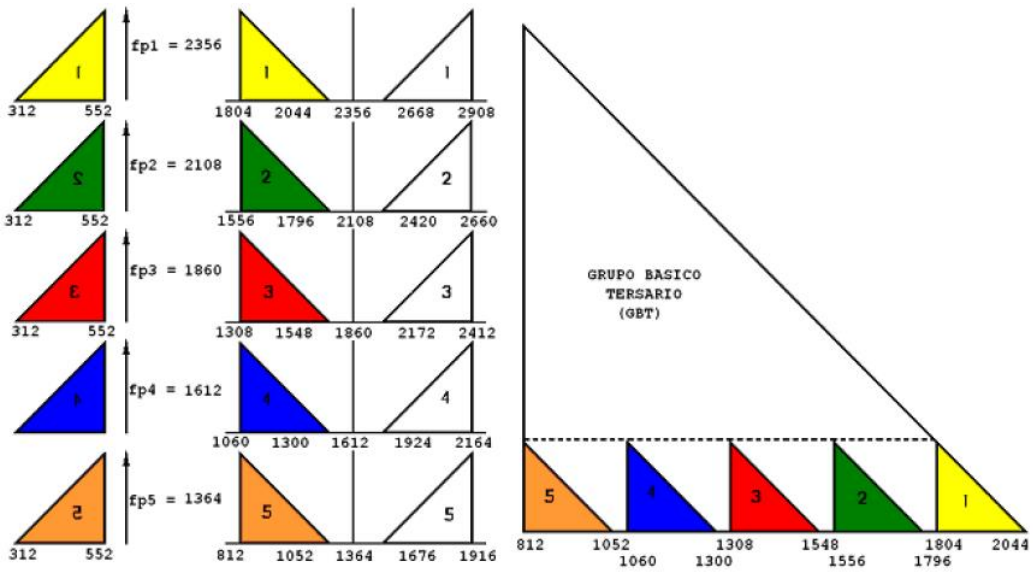
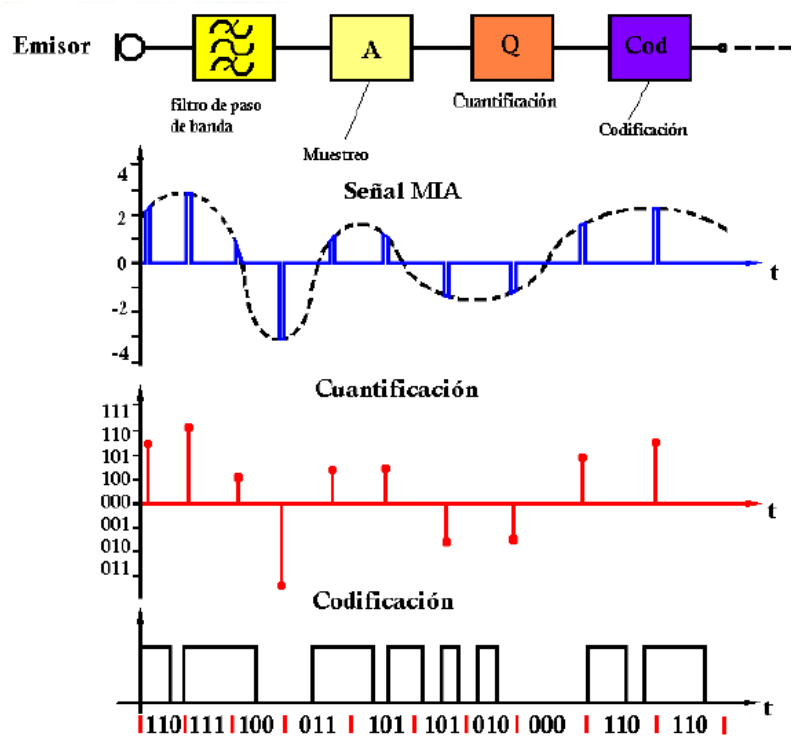


Ilustración 7 Grupo básico terceario

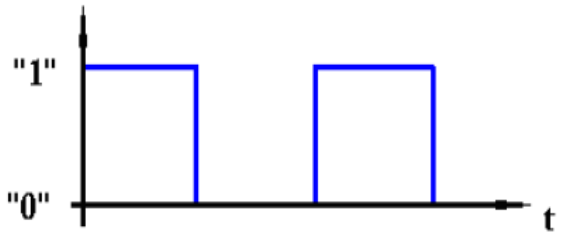
3. SISTEMA MIC

La señal MIC modulada en amplitud y considerada hasta este momento es todavía una señalanalógica; precisamente con un proceso de cuantificación se convertirá en una señal digital. [3]



3.1 Características

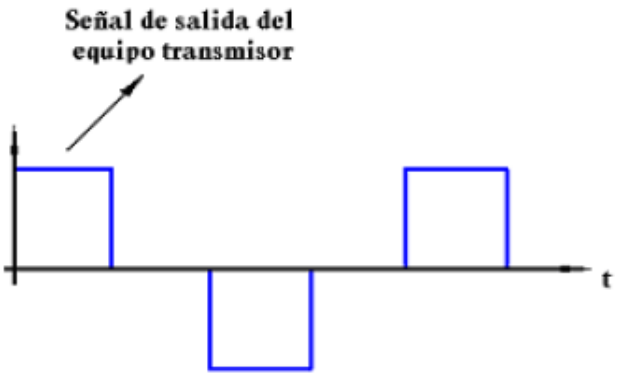
CONVERSIÓN DE POLARIDAD.



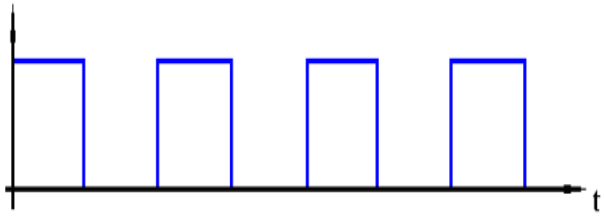
Para transmitir necesitamos pulsos bipolares (positivo y negativo), por eso los pulsos binarios los pasamos a un código binario de transmisión.

1. REGENERACIÓN

En los equipos MIC, la señal que se transmite sufre distorsiones, variaciones por el ruido a lo largo del medio de transmisión, en el trayecto se ubican repetidores o regeneradores. Existen dos tipos de regeneradores: repetidor pasivo y repetidor activo.



SINCRONIZACIÓN



Al hablar de sistema MIC es importante hablar de sincronización. En este sistema se trabaja con circuitos digitales que están sincronizados, o sea tienen una señal de reloj.

Existen tres tipos de sincronización:

a) Sincronización de dígito o bit
b) Sincronización de trama
c) Sincronización de la red

SISTEMA MIC

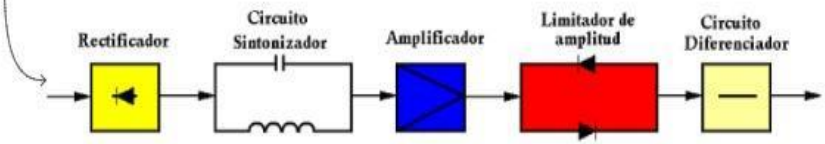
Sincronización

En este sistema se trabaja con circuitos digitales que están sincronizados, tienen una señal de reloj. Existen tres tipos de sincronización:

Sincronización de dígito o bit

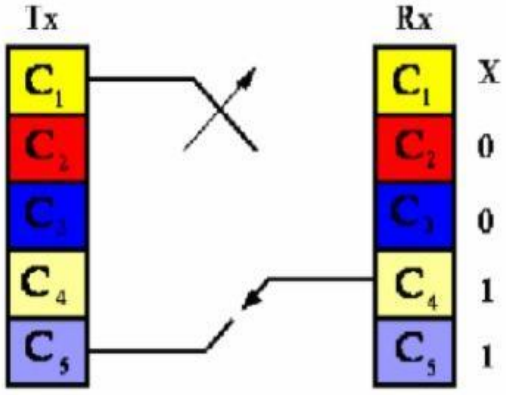
Se refiere a lo que es la sincronización del generador de la señal de reloj necesario para el codificador tantoen el transmisor como en el receptor.

- Circuito de Temporización
- Sincronización Interna
- Sincronización Externa.



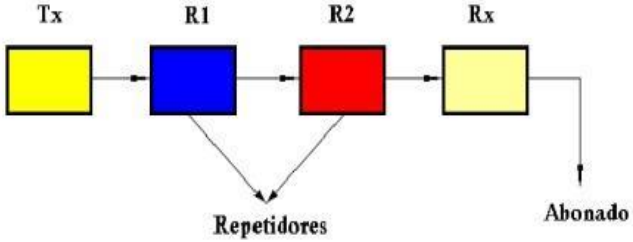
Sincronización de trama

Se refiere a la operación para encontrar una fase correcta que discrimina el principio y fin de una trama



Sincronización de la red

Debe tener una sincronización entre los equipos para que la calidad de la comunicación sea aceptable



4. PROTECCIÓN DE LOS DATOS: CONTROL DE ERRORES.

4.1. PROTECCIÓN DE LOS DATOS.

Los datos, cuya utilidad radica en su integridad y en su confidencialidad, están sujetos a dos tipos de amenazas:

Las causas por las que la señal eléctrica se deteriora al viajar por el canal de comunicación, ellas son: distorsión, atenuación, limitación del ancho de banda, ruido, interferencia y diafonía. Esta degradación de la señal puede hacer que recibamos en el receptor un carácter distinto al que fue emitido por el extremo transmisor, diremos entonces que se ha producido un error. Si bien es imposible evitar que ocurran errores, un buen diseño los minimizará.	Ya se ha hablado extensamente sobre el valor de la información, asegurar que esta información: - No sea vista o copiada por personas no autorizadas o no calificadas para ello. - No sea alterada en ningún sentido por personas o máquinas no autorizadas. - No sea creada y/o difundida engañosamente simulando fuentes reales o inexistentes.
El control de errores se puede dividir en dos categorías generales: Detección de errores y Corrección de errores. [2]	

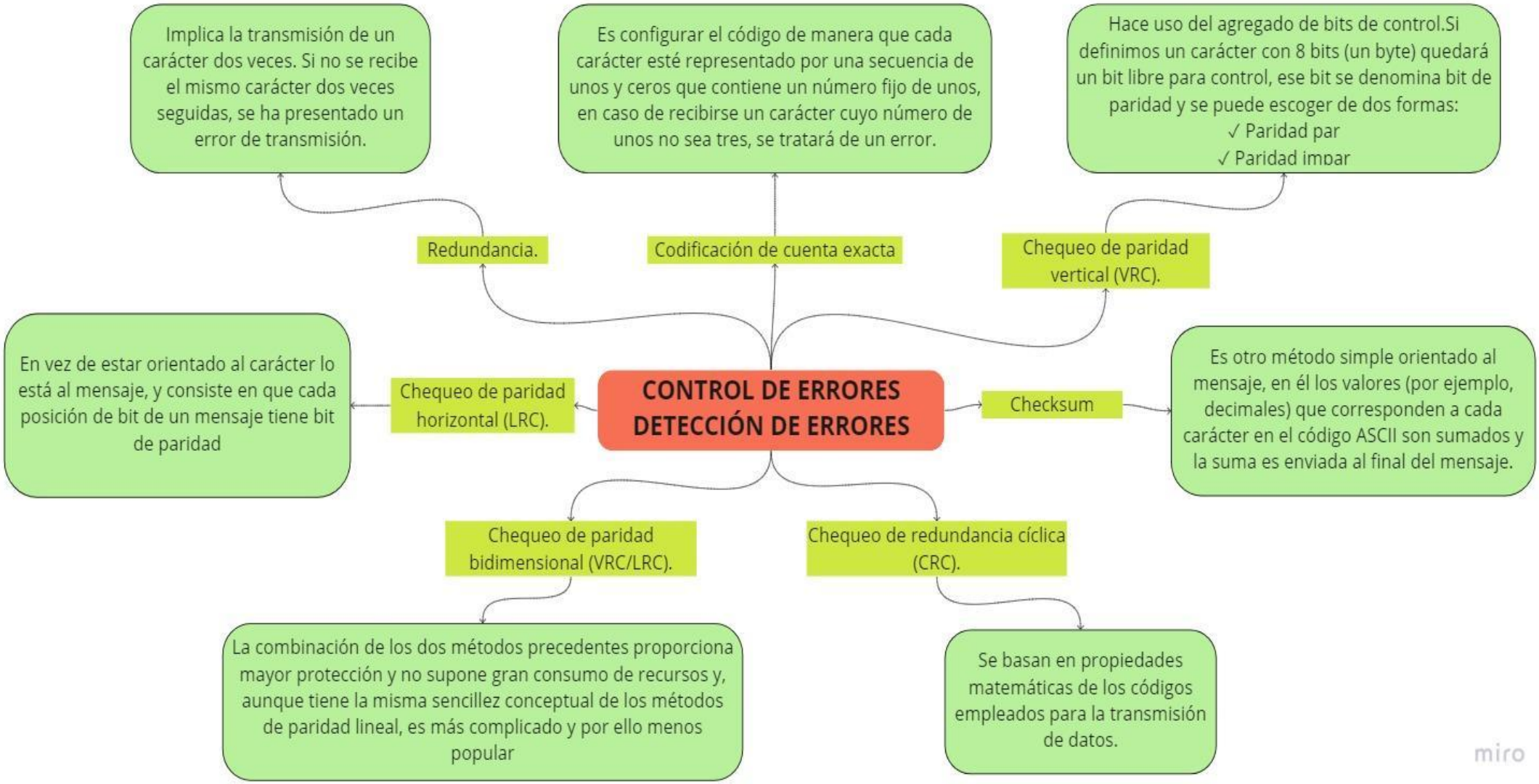
Tabla 3 Tipos de Amenazas

4.2. CONTROL DE ERRORES

DETECCIÓN DE ERRORES.

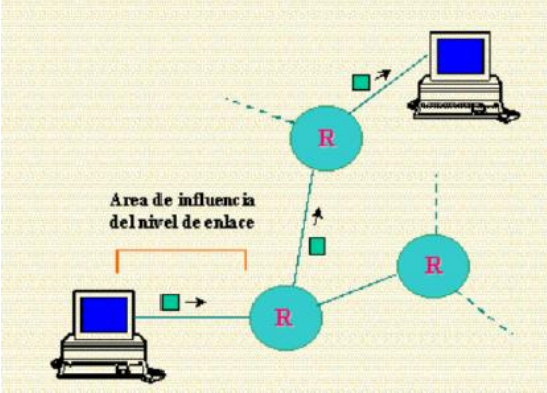
La detección de errores consiste en monitorear la información recibida y a través de técnicas implementadas en el Codificador de Canal ya descrito, determinar si un carácter, caso asincrónico, o un grupo de datos, caso sincrónico, presentan algún o algunos errores. Las técnicas más comunes son [2]:

1. Redundancia.
2. Codificación de cuenta exacta.
3. Chequeo de paridad vertical (VRC).
4. Chequeo de paridad horizontal (LRC).
5. Chequeo de paridad bidimensional (VRC/LRC).
6. Chequeo de redundancia cíclica (CRC).
7. Checksum

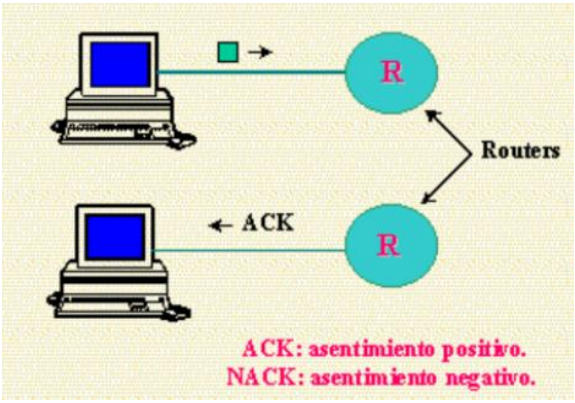

CONTROL DE ERRORES
DETECCIÓN DE ERRORES
Redundancia.
Implica la transmisión de un carácter dos veces. Si no se recibe el mismo carácter dos veces seguidas, se ha presentado un error de transmisión.
Codificación de cuenta exacta
Es configurar el código de manera que cada carácter esté representado por una secuencia de unos y ceros que contiene un número fijo de unos, en caso de recibirse un carácter cuyo número de unos no sea tres, se tratará de un error.
Chequeo de paridad vertical (VRC).
Hace uso del agregado de bits de control.Si definimos un carácter con 8 bits (un byte) quedará un bit libre para control, ese bit se denomina bit de paridad y se puede escoger de dos formas:
✓ Paridad par
✓ Paridad impar
Chequeo de paridad horizontal (LRC).
En vez de estar orientado al carácter lo está al mensaje, y consiste en que cada posición de bit de un mensaje tiene bit de paridad
Checksum
Es otro método simple orientado al mensaje, en él los valores (por ejemplo, decimales) que corresponden a cada carácter en el código ASCII son sumados y la suma es enviada al final del mensaje.
Chequeo de paridad bidimensional (VRC/LRC).
La combinación de los dos métodos precedentes proporciona mayor protección y no supone gran consumo de recursos y, aunque tiene la misma sencillez conceptual de los métodos de paridad lineal, es más complicado y por ello menos popular
Chequeo de redundancia cíclica (CRC).
Se basan en propiedades matemáticas de los códigos empleados para la transmisión de datos.

4.3. CONTROL DE FLUJO Y CONTROL DE ERRORES

Cuando una trama llega a una máquina conectada a algún tipo de red, antes de pasar la información a niveles superiores, la capa de enlace realiza una serie de operaciones sobre la trama que ocupan un espacio en la memoria e implican un tiempo, función de la máquina, de manera que el proceso de recepción no es instantáneo. [4]



Para evitar esta situación se hace necesario llevar un control del flujo en el enlace, manejando la velocidad a la que el emisor envía las tramas para que no sature al receptor. Este control de la velocidad requiere algún mecanismo de realimentación. [4]



Un protocolo de nivel de enlace que quiere enviar tramas eficientemente debe de alguna manera ser capaz de recuperar las tramas perdidas o descartadas. Esto se consigue normalmente usando una combinación de dos mecanismos fundamentales: acuses de recibo (acknoledgments) y temporizadores (timeouts). Un acuse de recibo, comunmente referido como ACK, es una pequeña trama de control con que el receptor informa al emisor de que ha recibido la transmisión. Si el emisor no recibe un ACK en un tiempo razonable la retransmite; este tiempo está medido por un temporizador. [4]

La estrategia general de usar ACKs y "timeouts" para implementar un envio eficiente se suele denominar automatic repeat request, normalmente abreviado ARQ.

- **Parada-y-Espera**

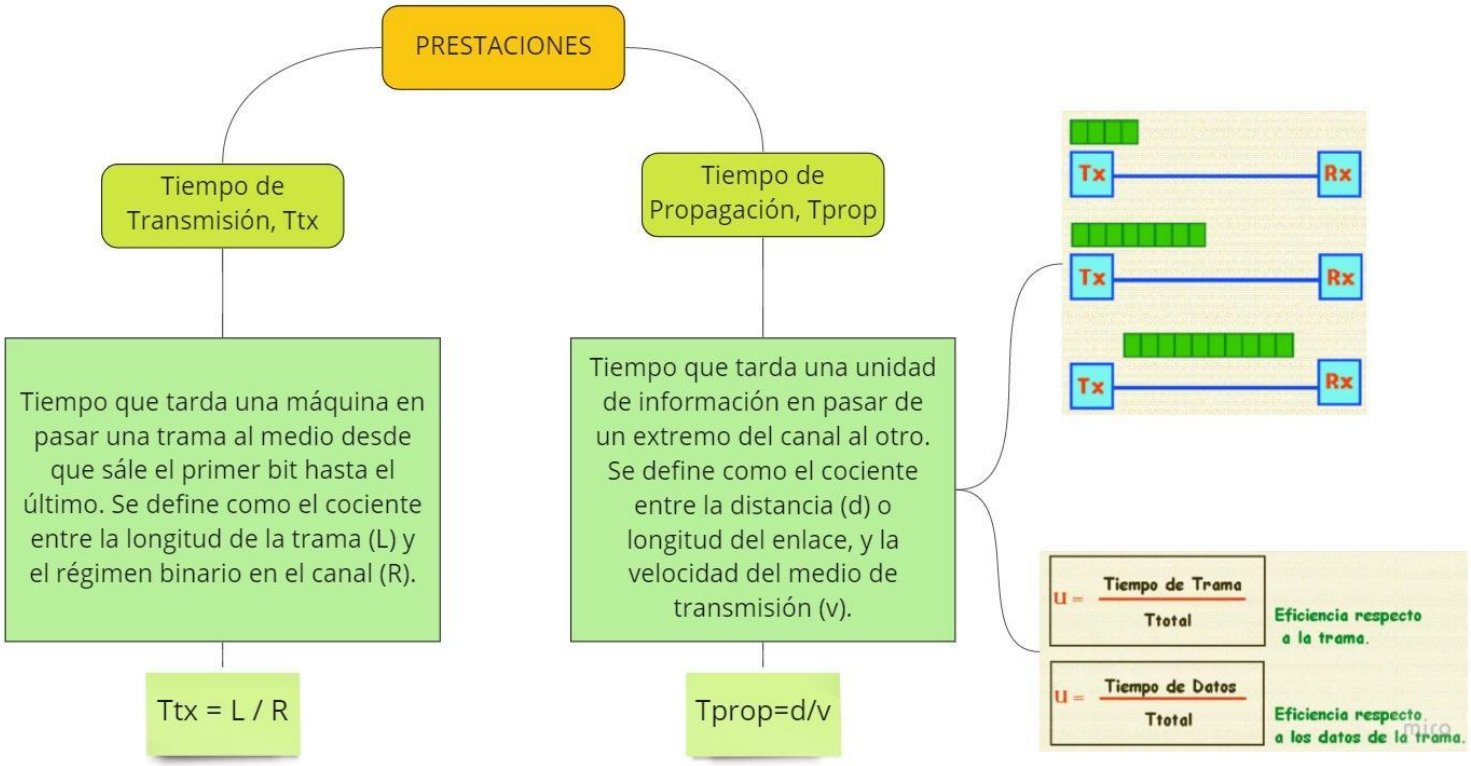
Es la más simple de las técnicas. Los pasos que llevarían a cabo las dos máquinas en diálogo serían:

1) El transmisor envía una trama al receptor.
2) El receptor la recoge, y devuelve otra trama de aceptación (ACK).

3) Cuando el transmisor recibe esta trama sabe que puede realizar un nuevo envío....
4) Si pasado un cierto tiempo predeterminado no ha llegado acuse de recibo, el emisor retransmite la trama.

PRESTACIONES

Restringiéndonos al caso en que sólo se puede enviar una trama cada vez, encontramos dos posibles situaciones:



4.4. VENTANA DESLIZANTE

Es un Buffer en el cual se almacenan copias de las tramas enviadas, Espera de recibir el ACK correspondiente, Si no llegan en el tiempo previsto, se realiza una nueva copia y se retransmite la trama. [4]

Número de secuencia de transmisión, N(S): Posición que ocupa la trama enviada en el buffer. El número de secuencia viaja en la cabecera de la trama.

Ventana de recepción se entiende el buffer donde se almacenan las tramas que llegan a una máquina por alguno de sus enlaces. En este buffer esperan a ser procesadas, y a que se devuelva el acuse de recibo correspondiente a cada una de ellas, para que la máquina origen sepan que la transmisión ha llegado sin problemas a su destino.

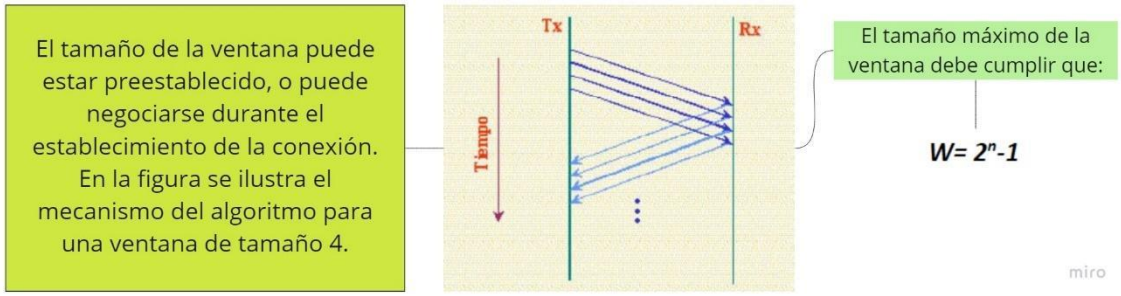


Ilustración 12 Ventana deslizante

5. DETECCIÓN, CORRECCIÓN DE ERRORES Y COMPRESIÓN EN MODEMS ANALÓGICOS.

El advenimiento de módems de más alta velocidad está vinculado a señalización multinivel, esto es consecuencia del siguiente análisis.

La empresa Microcom desarrollo un protocolo llamado MNP (Microcom Networking Protocol) que se ha convertido en el estándar en modems. MNP se puede implementar en software ó en hardware, sin embargo, opera más eficientemente cuando se coloca en el "firmware" del módem (que es software grabado en chips ROM que se encuentran en la tarjeta del módem). Los modems en ambos extremos deben usar el mismo MNP (veremos que hay varios) y eso se logra porque al iniciarse la comunicación el módem que la solicita "informa" que está usando MNP y el otro extremo automáticamente responde que sí,si tiene esa opción,lo que activa el software del módem solicitante. Cuando se implementa así el MNP cambia una serie de datos asincrónicos por una equivalente de datos sincrónicos y forma paquetes de datos continuos con CRC para detección de errores.

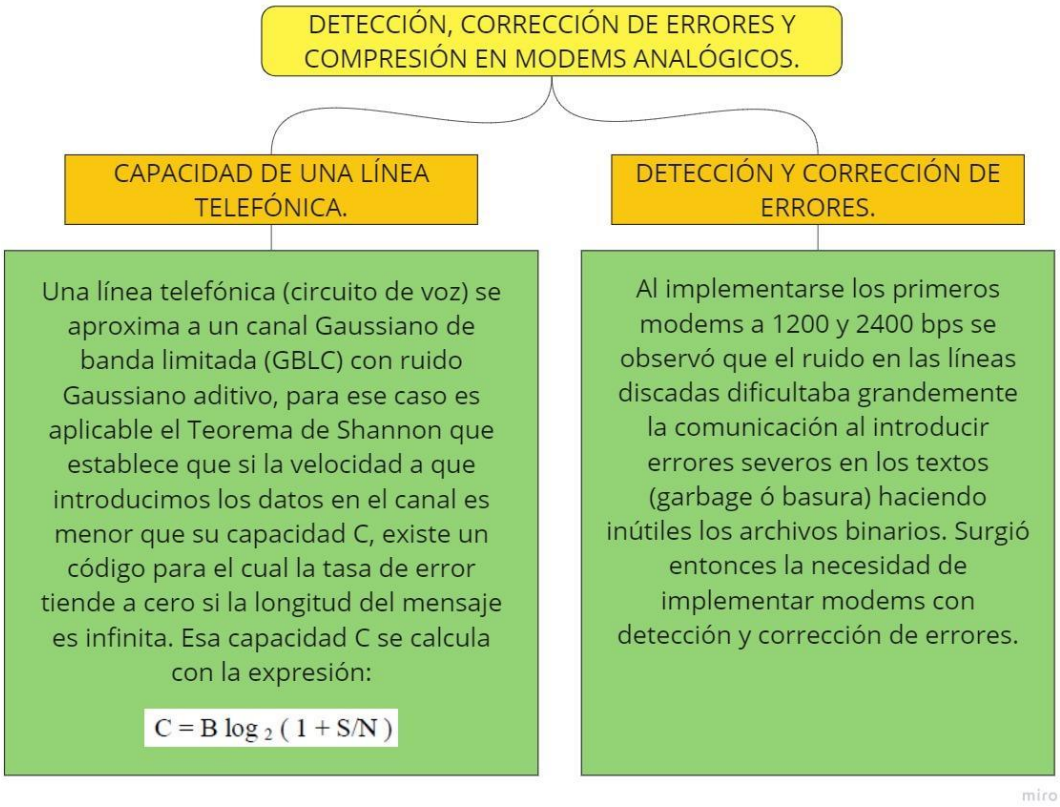
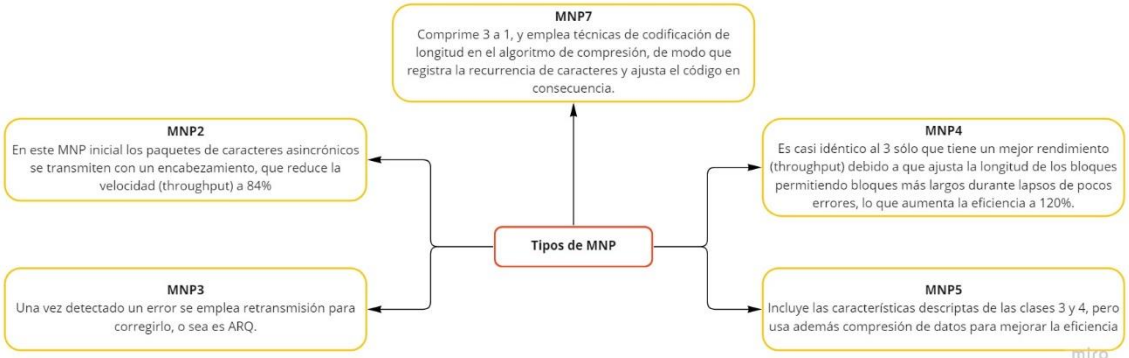


Ilustración 13 Detección y corrección de errores

La empresa Microcom desarrollo un protocolo llamado MNP (Microcom Networking Protocol) que se ha convertido en el estándar en modems. MNP se puede implementar en software ó en hardware, sin embargo, opera más eficientemente cuando se coloca en el "firmware" del módem (que es software grabado en chips ROM que se encuentran en la tarjeta del módem). Los modems en ambos extremos deben usar el mismo MNP (veremos que hay varios) y eso se logra porque al iniciarse la comunicación el módem que la solicita "informa" que está usando MNP y el otro extremo automáticamente responde que sí,si tiene esa opción,lo que activa el software del módem solicitante. Cuando se implementa así el MNP cambia una serie de datos asincrónicos por una equivalente de datos sincrónicos y forma paquetes de datos continuos con CRC para detección de errores.



Módems Analógicos

Historia de los módems analógicos

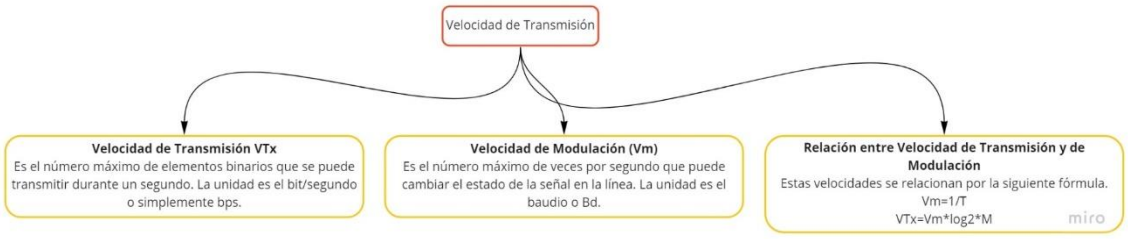
Los módems son dispositivos que convierten datos digitales seriales provenientes de un terminal transmisor a una señal adecuada para su transmisión sobre un canal telefónico y luego reconvierte esta señal en el otro extremo a datos digitales seriales que se entregan al terminal receptor. Su nombre proviene de las palabras Modulador-Demodulador.

Características Principales

Se enumeran las características principales de los módems.

1. Velocidades de transmisión y modulación
2. Tipos de transmisión
3. Modods de funcionamiento
4. Interface utilizada
5. Modulación
6. Frecuencias portadoras
7. Ecualizador
8. Aleatorizador

Velocidad de Transmisión



Tipos de Transmisión

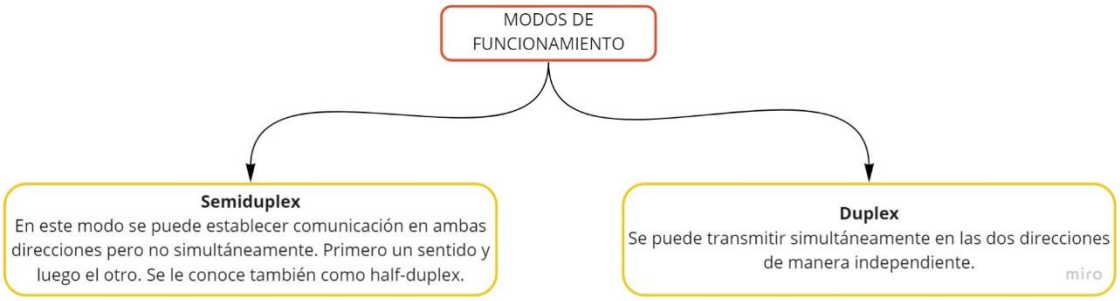
Hay dos tipos de transmisión: Asíncrona y Síncrona.

a) Transmisión Asíncrona: Es un método de enviar datos en el cual el intervalo entre los caracteres puede ser de diferente longitud. Como se usan caracteres asíncronos, no se requiere enviar sincronización adicional o una información de temporización. También se le conoce como transmisión start-stop.

b) Transmisión Síncrona: Transmisión en la cual los caracteres y bits de datos son transmitidos a una velocidad fija con el transmisor y receptor sincronizados. Esto elimina la necesidad de bits individuales de start y de stop alrededor de cada octeto, proporcionando una mejor eficiencia.

Modos de Funcionamiento

Hay dos modos de funcionamiento: Semiduplex y Duplex.



6. SEGURIDAD EN REDES.

Introducción

Todos los sistemas de comunicación de datos deberían poseer cierto grado de seguridad o privacidad de acorde a la importancia de la información manejada. Para esto existe una gran variedad de técnicas tales como: protección física, sistemas programados, encriptamiento, etc.

Aplicaciones de los Sistemas de Comunicación de Datos (SCD).	
Negocios	Usan los SCD para todas sus tareas diarias: Registros financieros; recepción, expedición y mantenimiento de cuentas; transferencia de fondos electrónicamente; inventarios y control de stock; control de procesos; órdenes de compra, comercio electrónico, reservaciones aéreas, hoteleras,etc.
Institutos Financieros	Varios de los primeros sistemas de computadoras comerciales fueron usados en bancos y finanzas para operaciones financieras, traslado de fondos, terminales financieros, cajeros automáticos, redes de datos.
Agencias de Gobierno	Aparte del uso militar están los sistemas de base de datos usados por la policía, el impuesto sobre la renta, etc.
Empresas	Intranet (redes internas de las empresas con correo electrónico, conferencias (audio o tele), acceso a bases de datos, bibliotecas, etc.).
Público	Internet

Tabla 4 Aplicaciones de SCD

ACCESO NO AUTORIZADO DE DATOS.

Cuando más y más datos se mueven entre computadores, mantener la confidencialidad de los datos comienza a ser un problema. Para nuestros propósitos, seguridad de datos significa “proteger los datos de alteración o acceso por partes no autorizadas”.

6.1. TÉCNICAS PARA SEGURIDAD DE DATOS.

ENCRIPTACIÓN.

proceso de codificación de la información, de tal manera de hacer difícil para el ladrón de información que lo robado tenga sentido para él. La codificación no debe ser demasiado compleja pues al usuario le sería engorroso entenderla, ni muy simple como para que un lector dedicado pueda aprender a descifrarla. En términos de encriptación, el mensaje original es referido como plain text, debido a que está en lenguaje sencillo o llano. La salida del proceso de encriptación se llama cipher text, debido a que es una versión codificada del texto sencillo de entrada

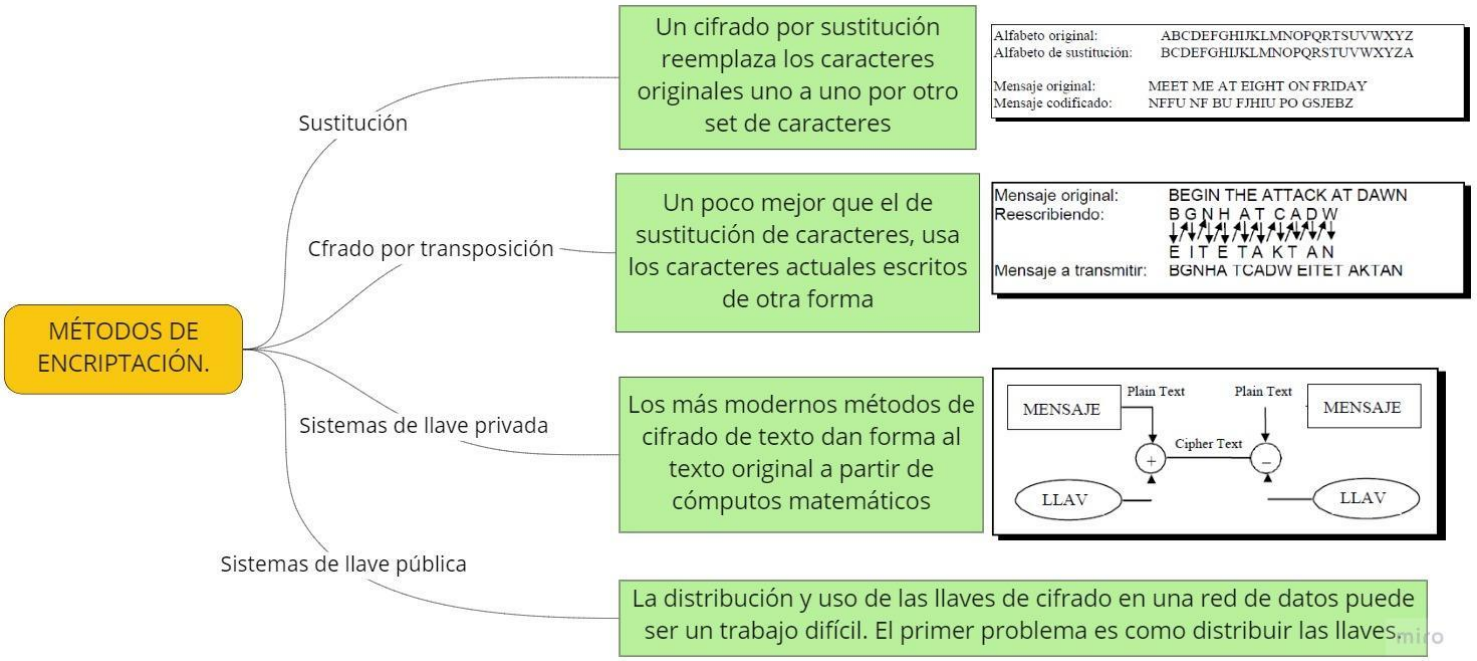
MÉTODOS DE ENCRIPTACIÓN.

a. Sustitución.

b. Cifrado por transposición

c. Sistemas de llave privada

d. Sistemas de llave pública.



7. ESTÁNDARES DE ENCRIPTACIÓN DE DATOS.

Para probar si los requerimientos de seguridad de datos se cumplen y también para proveer cierto grado de uniformidad, el National Bureau of Standards fue encargado en 1970 para desarrollar un Data Encryption Standard (DES) para ser usado en aplicaciones no relacionadas con defensa dentro del gobierno de los U.S. DES fue diseñado para satisfacer los siguientes criterios:

- ✔ Alto nivel de protección contra acceso y modificaciones de datos no autorizadas.
- ✔ Simple de entender, pero difícil de violar.
- ✔ Protección basada en llave y no dependiente de cualquier programa o proceso de encriptación.
- ✔ Económico y eficiente.
- ✔ Adaptable a diversas aplicaciones.
- ✔ Disponible para todos los usuarios y suplidores a un costo razonable.

8. AUTENTICACIÓN.

Encriptar no es suficiente es necesario “autenticar”, es decir, asegurar que las personas o entes participando en una “conversación” (intercambio de datos) son quienes dicen ser. Los mecanismos empleados van desde tarjetas de seguridad hasta autoridades de certificación. [2]

Una técnica muy popular es la “firma digital”, en ella se calcula con una función criptográfica de un solo sentido un valor llamado “hash”, se envía el texto original y el valor hash encriptado con una llave privada (que se denomina “firma”), en el extremo receptor se vuelve a calcular el valor hash, se desencripta la firma con clave pública y se compara con el hash calculado, si verifica el mensaje es auténtico.

9. Bibliografía

[1] E. M. Escabosa, «upcommons.upc.edu,» [En línea]. Available: https://upcommons.upc.edu/bitstream/handle/2099/9512/Article007.pdf?sequence=1&isAllowed=y. [Último acceso: 12 de Enero del 2024].

[2] W. Tomasi, Sistemas de Comunicaciones Electrónicas, México: PEARSON EDUCACIÓN, 2003. [Último acceso: 12 de Enero del 2024].

[3] J. P. P. Noroña, *CAPÍTULO IV CODIFICACIÓN DE CANAL,* Ambato, 2021. [Último acceso: 12 de Enero del 2024].

[4] B. A. Forouzan, *Data Communications and Networking,* McGraw-Hill Education, 2004. [Último acceso: 12 de Enero del 2024].