Universidad Nacional de la Matanza

Departamento:
Ingeniería e Investigaciones Tecnológicas

Cátedra:

Fundamentos de TIC’s

Jefa de Cátedra:
Mg. Artemisa Trigueros

UNIDAD NRO. 5

INTRODUCCIÓN A LA TELEINFORMÁTICA

COLABORACIÓN:
DOCENTES DE LA CÁTEDRA

CICLO LECTIVO:

2020

Contenido

Capítulo I: Características de los Sistemas Teleinformáticos

1.1 Conceptos básicos de teleinformática

Existieron diferentes tipos de revoluciones que marcaron hitos en las distintas culturas de la especie humana, un ejemplo lo constituyó la revolución industrial.

A partir de 1945 se dio inicio al diseño de equipos electrónicos digitales para el tratamiento de la información, que junto con los avances tecnológicos que lo sucedieron dieron origen a las computadoras, hecho que marcó una nueva etapa de origen revolucionario, que puede tener varias acepciones según el origen de los escritores que se refieren a ella:

- Revolución Post Industrial,
- La era Tecnotrónica (Tecnología Electrónica),
- La revolución Informática,
- La revolución de las NTIC (Nuevas Tecnologías de la Información y la Comunicación).

Esta revolución está basada en el manejo de volúmenes crecientes de información los cuales deben ser manejados necesariamente por **medios automáticos** para su tratamiento.

Así, el sector industrial se debió adecuar muy rápidamente al cambio tecnológico, reemplazando las tareas manuales por otros medios más sofisticados, incorporando robótica y sistemas automatizados de producción. Actualmente se utilizan computadoras manejadas por personal con un alto grado de capacitación, como por ejemplo; el pintado de autos en una fabricación serie. De esta manera casi todo el personal que participe en el proceso productivo debe estar capacitado para manejar el equipamiento moderno. Este cambio debe afectar no solamente a los conocimientos; debe producir un cambio de actitud para enfrentar los problemas creando y desarrollando soluciones a los nuevos requerimientos de las empresas modernas, diferenciando a esta revolución tecnológica de generaciones anteriores.

Esta nueva revolución, marcada por la introducción de la computadora en la vida diaria, produce grandes transformaciones en las estructuras de los pueblos y las naciones en todos los ámbitos sociales.

En este contexto el sector Industrial Moderno deberá poseer las siguientes características básicas:

- Adecuarse rápidamente al cambio tecnológico (sistemas automáticos de producción).
- Capacitar en forma permanente al personal para el manejo de los equipos modernos.
- Cambiar las actitudes en la manera de resolver los problemas de la era moderna.
- Cumplir con estándares de calidad Nacionales o Internacionales. Ejemplo: IRAM Instituto Argentino de Racionalización de Materiales (Nacional); ISO International Standard Organization (Internacional).
- Adecuarse a los nuevos mercados y prepararse para competir en mercados globales.

Con los elementos citados anteriormente nace el concepto de era postmoderna, en la que los países que integren el núcleo de "potencia mundial" serán aquellos que **posean y manejen mejor la información**.

En este contexto, hoy día, las empresas modernas mejoran su función de control con el concepto de "cruce de información" de sistemas informáticos o bases de datos asociadas. Puede pensarse al fenómeno informático como la expresión de un crecimiento acelerado de la capacidad de procesar información por parte de los sistemas de decisión.

1.1.1 La Sociedad de la Información

La información ha representado desde tiempos muy remotos un papel muy importante en el desarrollo de las sociedades, y ha venido evolucionando significativamente, presentándose de distintas maneras pero manteniendo el mismo objetivo, la comunicación entre las personas.

En la sociedad primitiva, la información se intercambiaba entre sus componentes para lograr sobrevivir en un ambiente hostil, hoy, el intercambio de información puede representar un factor vital para el desempeño de los procesos de muchas empresas. Los conocimientos que se van teniendo del entorno originan la necesidad de la comunicación. El nacimiento de la comunicación implica, asimismo, la existencia de los elementos que la hacen posible y que constantemente están interviniendo en el proceso de la comunicación*: **los interlocutores*** y ***el medio de comunicación***.

Un elemento importante en el proceso de la comunicación es la **codificación**, característica general a todo proceso de comunicación. Mediante la codificación se representan las informaciones en términos de alfabetos acordados entre los participantes para facilitar el proceso de transmisión y que sea útil y con coherencia para ambos elementos; ya nuestros antepasados utilizaban algunos métodos o alfabetos específicos como son las señales de humo o los reflejos en los espejos. Los elementos que integran el proceso básico de comunicación se pueden representar gráficamente:

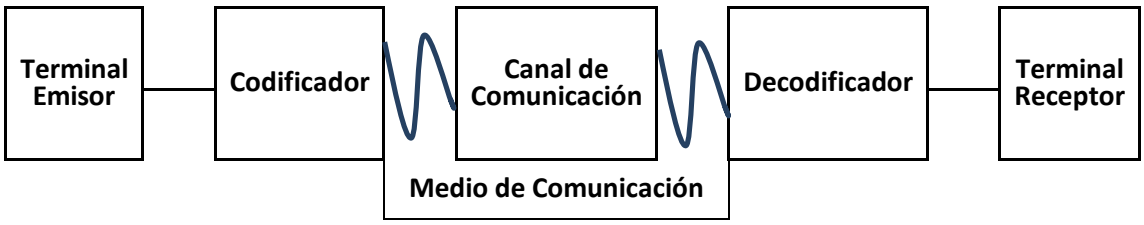


Fig. 1.1.1.a: Proceso general de la comunicación entre terminales distantes

En la actualidad la información es una parte no sólo constitutiva sino **imprescindible**, al igual que el hecho de compartir dicha información. La gran cantidad de conocimientos almacenados por la humanidad en el devenir de los años, junto con la incapacidad para almacenarlos en un único lugar físico hacen necesaria la transmisión de la información. Por tanto, como punto de partida para la adquisición de conocimiento en una sociedad genérica se crea la necesidad de acceder de una forma específica a la información que se encuentra almacenada en lugares concretos.

El inicio formal de la rama del conocimiento conocida como ***teleinformática***, ***telemática*** **o** ***transmisión de datos***, **se basa fundamentalmente en el acceso a la información la que se encuentra almacenada en un dispositivo informático situado en un lugar, en principio, distinto al de nuestra situación geográfica.**

Elementos intervinientes en todo proceso de comunicación:

- **Emisor:** Es el elemento terminal que proporciona la información.
- **Receptor:** Es el elemento terminal que recibe la información.
- **Canal o medio de Comunicación:** Es el elemento que se encarga de transportar la señal sobre la que viaja la información entre emisor y recepto. Un canal viene definido por sus propiedades físicas, que son: la naturaleza de la seña que puede transmitir, y otros elementos tales como la velocidad de transmisión, el ancho de banda, el nivel de ruido (interferencias), longitud y modo de inserción de emisores y receptores en el canal.

1.2 Conceptos introductorios

1.2.1 Conceptos Básicos de Comunicación e Informática

- ***Teleinformática:*** Este término se refiere básicamente a la disciplina que trata la comunicación entre equipos de computación distantes. Es la ciencia que trata la comunicación a distancia entre procesos. Formalmente, teleinformática (tele = a distancia) es la ciencia que estudia el conjunto de técnicas necesarias para poder transmitir datos a distancia por medio de sistemas informáticos, entre puntos situados en lugares remotos a través de redes de telecomunicaciones. Los objetivos de la teleinformática son:
  - Lograr que una computadora pueda dialogar con equipos situados geográficamente distantes, reconociendo características disímiles de la información como si la conexión fuera local, usando redes de telecomunicaciones.
  - Compartir recursos tanto lógicos, físicos como humanos (memoria, procesador, impresora, programas, etc.).
- ***Transmisión de datos:*** Es el movimiento de información codificada de un lugar a otro.
- ***Telecomunicaciones:*** Hacen referencia a la transmisión de datos a distancia.
- ***Teleprocesamiento:*** Permite que un sistema de computación utilice algún tipo de telecomunicación para procesar datos.
- ***Red de computadoras (Networking):*** conjunto de computadoras interconectadas con el objetivo de compartir trabajos, recursos e información.
- ***Protocolo:*** conjunto de normas, convenciones y procedimientos que regulan la comunicación de datos y el comportamiento de procesos entre diferentes equipos, bien totalmente o bien en alguno de sus aspectos.
- ***Bit (Binary Digit):*** Es la unidad más pequeña de información y es utilizada como unidad base en comunicaciones.
- ***Byte (Binary Term):*** Término binario. Número de bits utilizados para representar un carácter en un sistema de codificación dado. Según esta definición, un byte puede tener un número variable de bits, dependiendo de que se usen cinco, seis, siete, ocho o más bits para representar un carácter. Un hecho importante a tener en cuenta es que cuantos más bits utilice un sistema de codificación dado para representar un carácter, es decir, cuanto más largo sea el byte, mayor será la cantidad de información por carácter y, por lo tanto, mayor el tiempo que tardará en transmitir, por ejemplo, un texto.
- ***Caracter:*** Es una unidad de información que se corresponde con un símbolo. Por ejemplo letras, números, símbolos especiales y de control. Ej: en ASCII, la letra A es 01000001.

1.2.2 Señales analógicas y digitales

Por las redes de telecomunicaciones pueden transmitirse dos tipos de señales: **analógicas y digitales**. Es importante distinguirlas claramente porque su comportamiento es muy distinto en los diferentes elementos tecnológicos necesarios para construir las redes de telecomunicaciones, que consecuentemente pueden clasificarse en redes analógicas o redes digitales.

- ***Señal analógica:*** aquellas que pueden ser representadas por funciones que toman un número infinito de valores en cualquier intervalo considerado.

- ***Señal digital:*** *aquellas que pueden ser representadas por funciones que toman un número finito de valores en cualquier intervalo de tiempo.*

Los sistemas de telecomunicaciones, ya sean analógicos o digitales, transmiten **señales periódicas**.

Para efectuar la trasmisión de señales se debe utilizar un circuito eléctrico provisto de una determinada tensión eléctrica medida en Volts y una determinada corriente eléctrica medida en Amperes.

Señales analógicas

Una de las formas más comunes de las señales analógicas es la función sinusoidal armónica simple. Por lo cual estamos en presencia de una magnitud repetitiva o periódica a lo largo del tiempo, que se representa por medio de una función que cuenta con las siguientes características:

- Se define como **período** de una función repetitiva al tiempo transcurrido entre dos pasos consecutivos de la señal por el mismo valor en el mismo sentido. El período se representa con la letra "T". El período se mide en unidades de tiempo. Por ejemplo: un colectivo pasa por la misma parada, en el mismo sentido, 1 vez cada 90 minutos. En este caso su período es de 90 minutos. En el caso de las ondas utilizadas en teleinformática, se expresa en segundos.

- Se define como **frecuencia** de la señal periódica al número de ciclos completos que tiene lugar en la unidad de tiempo. La frecuencia se expresa con la letra "f" y se mide en Hertz. La frecuencia de 1 Hertz corresponde a un ciclo por segundo. La frecuencia y el período están relacionados por la expresión siguiente:

F=1/T (Frecuencia = 1 / Período)

- Se denomina **longitud de onda** a la distancia que recorre la onda durante un tiempo igual al período.

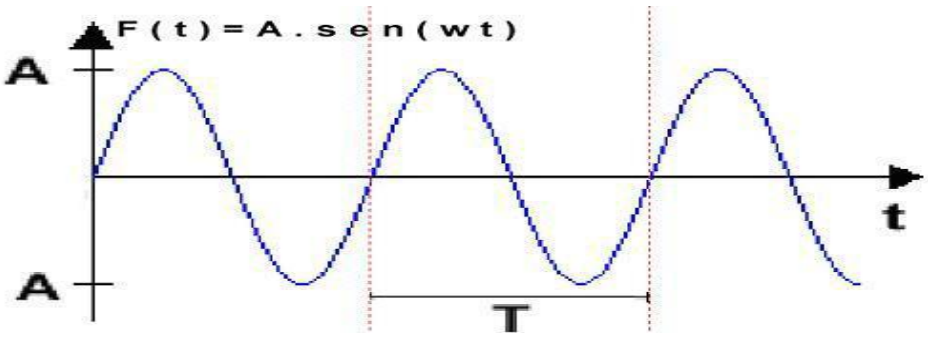


Fig. 1.2.2.a: Muestra una **Función periódica sinusoidal.**

La sinusoide generada se caracteriza por su **amplitud "A",** que corresponde **al valor máximo de la función en un período completo**, su período T (o su frecuencia "f =1/T") y su fase inicial "θ".

La función así definida está dada por la siguiente expresión:

$$\mathbf{F(t) = A \text{ sen } \omega t + \theta)}$$

Donde:

A= Amplitud (representa los valores de tensión o corriente de una señal)
ω=Velocidad angular = 2π**f**
f = frecuencia=1/T
T = Período
θ = Ángulo de fase (puede valer 0).

Señales digitales

Las señales periódicas no siempre tienen comportamiento sinusoidal. En el caso más simple, se puede pensar en una señal que adopte solamente dos valores, que pueden ser uno positivo y otro negativo, o bien uno de ellos uno positivo y el otro coincidente con la línea de referencia como se muestra:

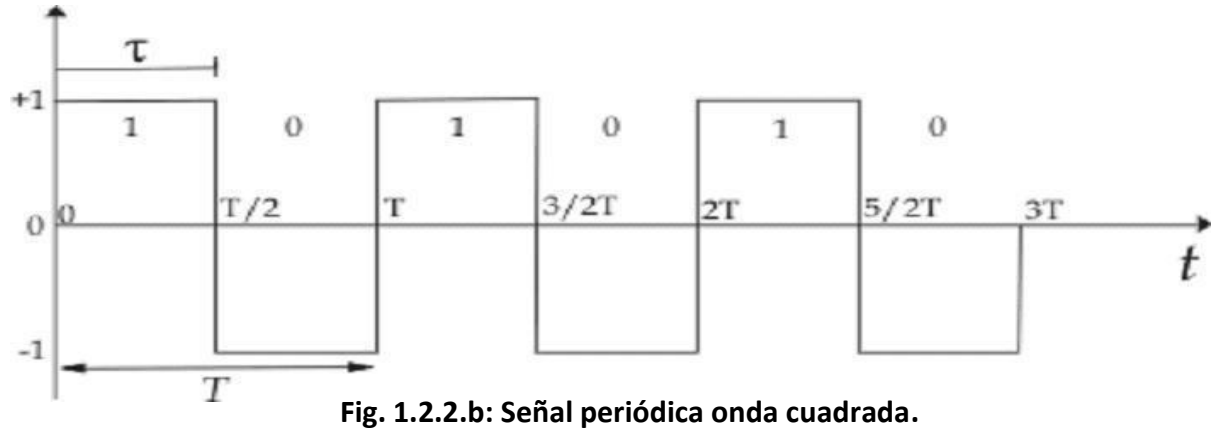


Fig. 1.2.2.b: Señal periódica onda cuadrada.

Una de las formas más comunes de las señales digitales es la función **onda cuadrada**. Esta señal es generada, normalmente, por equipos denominados generadores de pulsos que se basan en las técnicas de la electrónica digital. En este caso, la señal toma solo dos valores diferentes, por lo que estamos en presencia de una ***señal binaria***.

En este tipo de señal periódica se siguen manteniendo los conceptos de amplitud, período y frecuencia anteriormente descriptos. Si se considera como positivo a aquel tiempo en el cual la señal toma el mayor valor y como negativo al tiempo en el cual la señal toma el menor valor, se suele decir que la señal es cuadrada si ambos tiempos son iguales.

Denominamos pulso a cada una de las transiciones de estado de la señal, en un intervalo de tiempo. Comúnmente al conjunto de unos y ceros transmitidos se lo denomina tren de pulsos.

En las señales digitales aparece un parámetro muy importante denominado:

Ancho de pulso **(τ)**: **Es el intervalo de tiempo en el cual la señal produce efectos sobre los elementos sobre los que actúa.** En la función onda cuadrada el ancho de pulso es la mitad del período.

1.2.3 Transmisión de señales

Se pueden señalar las siguientes características de los sistemas de transmisión analógicos y digitales:

- Todos los sistemas de comunicaciones analógicos como digitales están capacitados para transportar señales de información para los servicios de voz, texto, imágenes y datos.
- En los sistemas de comunicaciones analógicos la propia forma de la onda de la señal transmitida es la que contiene la información que se transmite.
- En los sistemas digitales, los pulsos codificados de la señal transmitida son los que contienen la información.

Existen servicios de comunicaciones en los cuales las primeras señales generadas son típicamente analógicas, como en la transmisión de la voz, y otros en los cuales esas señales son típicamente digitales, como en el caso de la transmisión de los datos producidos por equipos informáticos, sin embargo, ambos tipos de señales pueden ser transmitidos por cualesquiera de los dos tipos de redes.

Cuando es necesario transportar señales digitales a través de redes analógicas, las señales deben sufrir previamente un proceso denominado **modulación**. El equipo que se utiliza para efectuar este proceso se denomina **módem** (contracción de **mod**ulador –**dem**odulador). El módem realiza las dos funciones: la directa, modular (transforma señal digital en analógica), y la inversa, demodular (transforma señal analógica en digital).

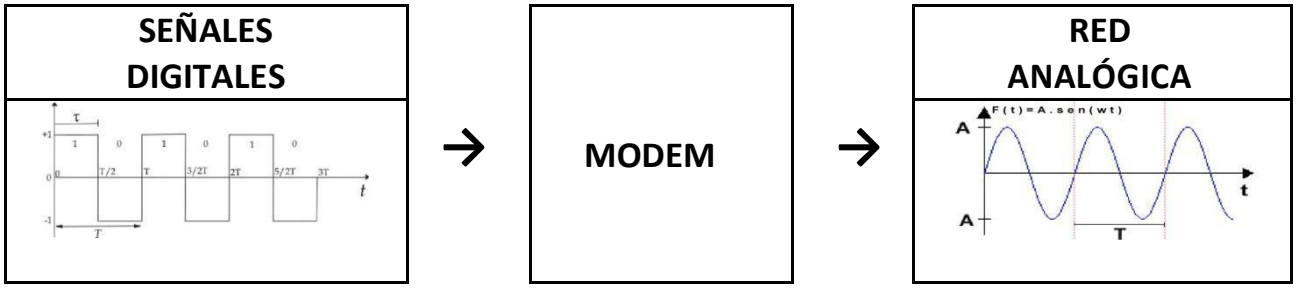


Fig. 1.2.3.a: MODEM (MODULADOR - DEMODULADOR).

Existen, en primera instancia, tres tipos de modulación en el proceso de transformación digital - analógico o su inversa:

- **Modulación en amplitud (AM):** se cambia la amplitud de la señal analógica respecto de la digital, pero ambas mantienen la frecuencia original de la señal:

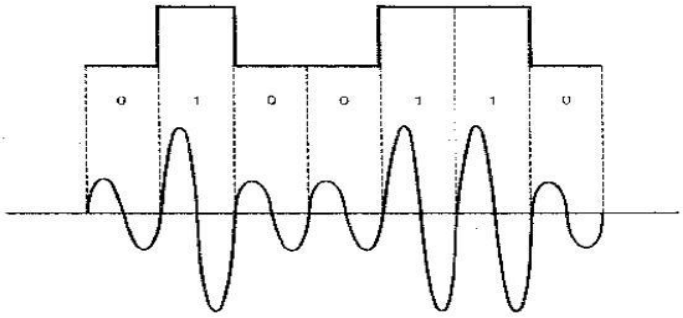


Fig. 1.2.3.b: **Modulación en Amplitud. (AM)**

- **Modulación en frecuencia (FM):** se mantiene la misma amplitud para el 1 y el 0, tanto en la señal analógica como digital, pero la frecuencia de la señal analógica varía respecto de la digital.

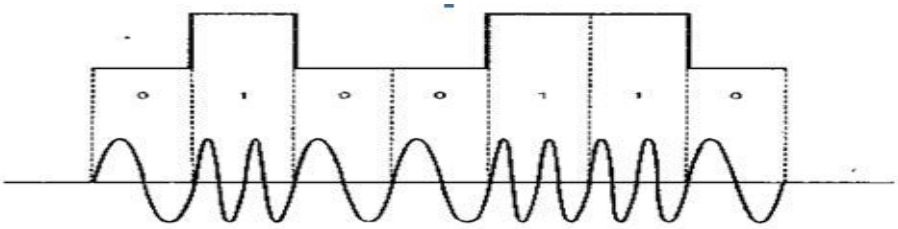


Fig. 1.2.3.c: **Modulación en Frecuencia. (FM)**

- **Modulación de fase (MF):** se mantiene la misma amplitud y frecuencia, pero se modifica la fase, es decir, el punto desde donde comienza la señal:

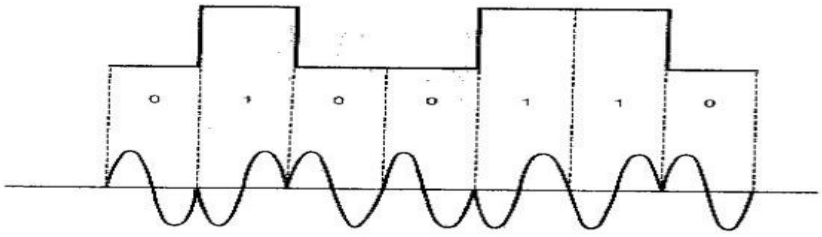


Fig. 1.2.3.d: **Modulación en Fase. (MF)**

1.3 El Decibel

El decibel es una unidad de medida muy utilizada en el campo de las telecomunicaciones para indicar la relación entre potencias, tensiones o corriente, en valores relativos. En realidad es un submúltiplo del Bel, que ha caído en desuso debido a que es una unidad muy grande.

*El decibel es una **unidad de medida relativa** que indica la relación de potencias, tensiones o corrientes entre dos valores conocidos.*

El decibel mide la pérdida o ganancia de la potencia de una onda. Los decibeles pueden ser valores negativos lo cual representaría una pérdida de potencia a medida que la onda viaja o un valor positivo para representar una ganancia en potencia si la señal es amplificada.

1.4 Características de la Transmisión de Datos

1.4.1 Tipos de Transmisión

Los distintos tipos de transmisión de un canal de comunicaciones pueden ser de tres clases diferentes:

- ***Simplex:*** la transmisión de datos se produce en un solo sentido, siempre existen un nodo emisor o transmisor y un nodo receptor que no cambian sus funciones:

Fig. 1.4.1.a: Transmisión Simplex.

- ***Half-Duplex:*** la transmisión de los datos se produce en ambos sentidos, pero alternativamente, en un solo sentido a la vez. Si se está recibiendo datos no se puede transmitir. Un ejemplo típico es la conversación entre radioaficionados. En estos sistemas son populares las expresiones "cambio" para indicarle al corresponsal que es su turno para hablar y "cambio y fuera" para terminar la conversación:

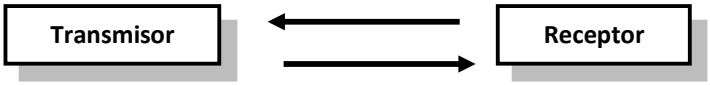


Fig 1.4.1.b: Transmisión Half Dúplex.

- ***Duplex:*** la transmisión de los datos se produce en ambos sentidos al mismo tiempo, un extremo que está recibiendo datos puede, al mismo tiempo, estar transmitiendo otros datos. Un ejemplo típico de esta transmisión es el teléfono:

Fig 1.4.1.c Transmisión Dúplex.

1.4.2 Concepto de sincronismo

Se denomina **sincronización** al proceso mediante el cual tanto el emisor como el receptor de los datos adoptan una base de tiempo común, de forma de reconocer inequívocamente la transmisión de un **1** o de un **0**.

Para la sincronización del emisor y el receptor es necesario disponer de *relojes* (**clock**) que funcionen a la misma frecuencia en ambos puntos de enlace.

1.4.3. Transmisión asincrónica y sincrónica

- ***Transmisión asíncrona*:** En el procedimiento asincrónico, cada byte a transmitir es delimitado por un bit denominado de *arranque* ***(start)***, y uno o dos bits denominados de *parada* ***(stop)***, ubicados al principio y al final. La misión de estas señales es:
  - Avisar al receptor de que está llegando un dato.
  - Darle suficiente tiempo al receptor de realizar funciones de sincronismo antes de que llegue el siguiente byte.

  Entre las características de la transmisión asincrónica podemos citar:
  - Los equipos emisor y receptor que funcionan en modo asincrónico se conocen también como terminales en modo carácter.
  - Entre dos caracteres puede mediar cualquier separación de tiempo.
  - En caso de errores se pierde siempre una cantidad pequeña de bytes, pues estos se sincronizan y se transmiten uno por uno.
  - Es un procedimiento que permite el uso de equipamiento más económico y tecnología menos sofisticada.
  - La transmisión asincrónica se denomina también arrítmica o start – stop.
  - Son especialmente aptos cuando no se necesitan lograr altas velocidades.
  - Debido a que por cada byte a transmitir se incorporan un bit de arranque y uno o más bits de parada, el aprovechamiento de la línea de transmisión es baja.
  - Bajo rendimiento de la transmisión.
- ***Transmisión síncrona:*** En el procedimiento sincrónico existen dos relojes, uno en el receptor y otro en el emisor, y la información útil es transmitida entre dos grupos de bytes denominados delimitadores. Un grupo delimitador es el de encabezado, que se encarga de resincronizar los relojes, y el otro grupo es el de terminación.

A causa de la tecnología que se emplea en estas transmisiones, los relojes deben permanecer estables durante un tiempo relativamente largo (se utilizan relojes con una precisión superior a 1:1.000.000). Por ello, los relojes se deben resincronizar periódicamente.

Las características de la transmisión sincrónica son las siguientes:
- Mejor aprovechamiento de la línea de transmisión.
- Los equipos necesarios son de tecnología más compleja y de costos más altos.

- Son especialmente aptos para ser usados en transmisiones de altas velocidades.
- En caso de errores de transmisión, la cantidad de bytes a retransmitir es importante.
- El rendimiento de la transmisión es superior al 99%, si transmito bloques de 1024 bytes con no más de 10 bytes de cabecera y terminación.
- La señal de sincronismo puede ser generada por el módem o por el equipo terminal de datos.

1.4.4 Formas de Transmisión

Las dos formas básicas de transmisión son: Transmisión en Serie y transmisión en Paralelo.

- ***Serie:*** Los bits se transmiten de uno a uno sobre una línea única. Es aquella en la que los bits que componen cada carácter se transmiten en n ciclos de 1 bit cada uno. Se utiliza para transmitir a la distancia.

  Posee las siguientes características:

  - Se envían un bit uno detrás de otro, hasta completar cada carácter.
  - Este modo es el típico de los sistemas Teleinformáticos.
  - La secuencia de los bits transmitidos se efectúa siempre al revés de cómo se escriben las cifras en el sistema de numeración binario. Cuando se transmite con bit de paridad, éste se transmite siempre en último término.

La *transmisión en modo serie* tiene dos procedimientos diferentes, el denominado *asincrónico* y el *sincrónico.*

- Antes de que el sistema se active la línea de transmisión se encuentre en estado de tensión máxima (lo que podría equivaler, por ejemplo, a un 1).
- El bit de arranque indica donde empieza el carácter transmitido y activa los mecanismos encargados de contar y recibir las señales transmitidas. Este bit corresponde a una señal de mínima tensión en la línea y se puede corresponder a un 0, es decir, hace pasar a la línea que estaba en estado de máxima tensión (un 1), a un estado de mínima tensión (un 0).
- Luego se transmiten los bits de datos.
- El bit o bits de parada se encargan siempre de volver a colocar la señal en el nivel máximo de tensión, para esperar así el byte siguiente.
- Mientras no vuelva a recibirse el bit de arranque, la señal quedará en reposo en el nivel máximo de tensión hasta que vuelva a aparecer una nueva transición de 1 a 0.

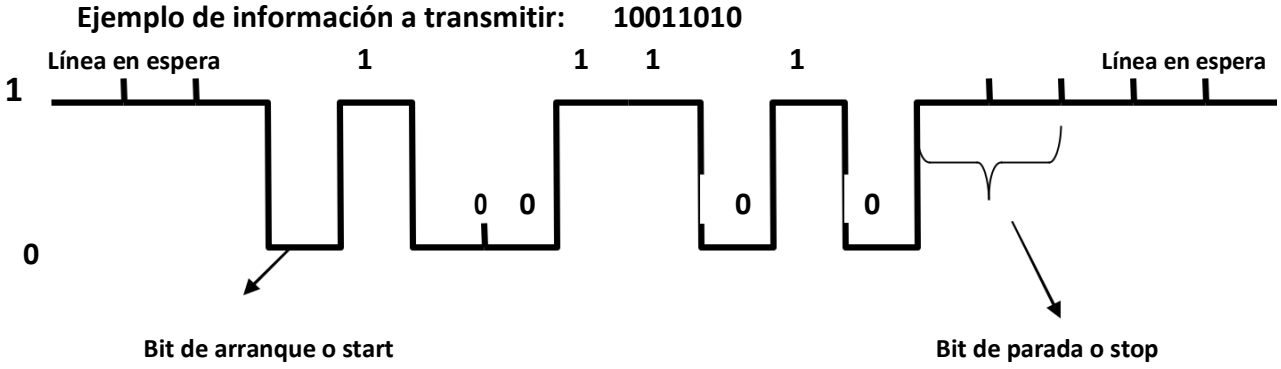


Fig. 1.4.4.a: Transmisión en modo serie asincrónico.

- ***Paralelo:*** Los bits se transmiten en grupo sobre varias líneas al mismo tiempo. Es aquella en la que los n bits que componen cada byte o carácter se transmiten en un solo ciclo de n bits, es utilizada básicamente en el interior de una computadora.

1.4.5 Conversión entre formas

En muchas ocasiones, las señales que son transmitidas por los vínculos de telecomunicaciones, al llegar a los equipos informáticos deben pasar al modo paralelo y viceversa. Este proceso de transformación se denomina ***deserialización*** y ***serialización,*** respectivamente.

Por lo general, la comunicación **entre computadoras se realiza en modo serie**, o sea a través de un solo "hilo conductor", en cambio básicamente **en el interior de la misma, el modo en que viaja la información es en paralelo,** por lo tanto, frecuentemente es necesario efectuar la conversión de datos paralelos a datos series en la conexión de salida hacia el medio de comunicación o red, y la conversión de datos series a paralelos en la entrada.

Se puede observar que los datos que en forma de unos y ceros ingresan en paralelo, luego del proceso de serialización, los bits quedan ubicados en la salida del canal de comunicaciones, para ser enviados en serie o sea bit por bit, como se muestra:

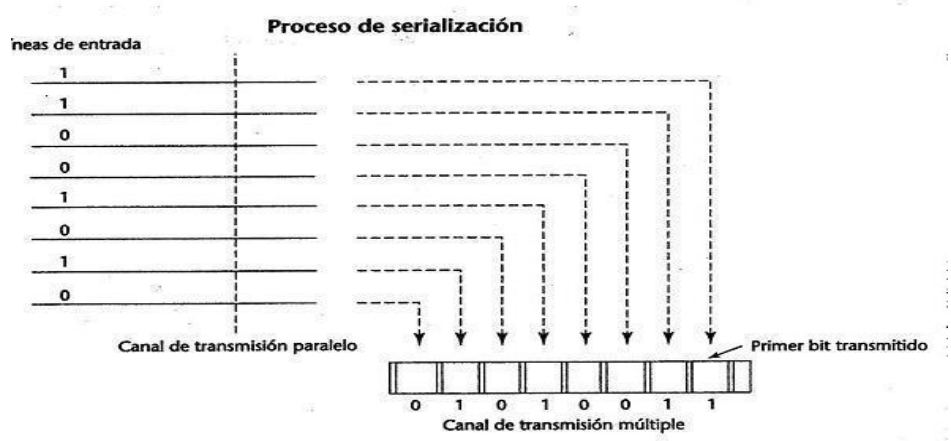


Fig. 1.4.5.a: **Proceso de serialización.**

Capítulo II: Técnicas de transmisión de la Información

2.1 Conceptos de velocidad

2.1.1 Velocidad de modulación

El concepto de **velocidad de modulación** es típicamente un concepto usado en telecomunicaciones y se define como:

La inversa de la medida del intervalo de tiempo nominal más corto entre dos instantes significativos sucesivos de la señal modulada.

También se suele definir como:

La inversa del tiempo que dura el elemento más corto de señal, que se utiliza para crear un pulso.

La velocidad de modulación se mide en ***baudios*****,** tal que:

Vm = 1/τ donde **τ =** duración del pulso (*ancho del pulso*)

En unidades, resultará:

[Vm] = 1 / [seg] = [baudio]

Con pulsos de señal de igual duración, la velocidad de modulación medida en baudios es el número de dichos pulsos por segundo, o el máximo número de transiciones de estados del canal por segundo (pasajes de 1 a 0). A la velocidad de modulación también se la suele llamar ***velocidad de señalización***. Esta velocidad está relacionada con la línea de transmisión.
En la siguiente figura, se muestra como se transmite un carácter (byte), en el Servicio Télex, en modo asincrónico, usando el ***Código Baudot***, donde las señales de arranque y de datos tienen una duración de 20 ms y la de parada de 30 ms. En efecto, para este ejemplo resultará:

Vm = 1 / 20 ms = 1 / 0.02 = 50 baudios

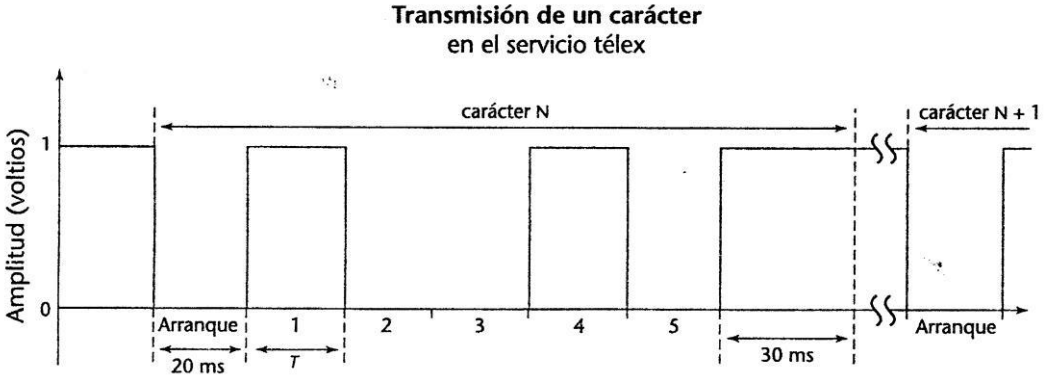


Fig. 2.1.1.a: Transmisión de un carácter usando Código Baudot.

2.1.2 Velocidad binaria o velocidad de transmisión

El concepto de velocidad binaria y el de velocidad de transmisión son en general motivo de cierta controversia. La Unión Internacional de Telecomunicaciones (UIT-T), Ginebra, 1985, define solamente lo que denomina **velocidad binaria.** Sin embargo, muchos autores prefieren utilizar la expresión **velocidad de transmisión.** A pesar de que las definiciones son diferentes, a nuestro criterio los conceptos son equivalentes.

En un canal de datos, se denomina velocidad de transmisión:

Número de dígitos binarios transmitidos en la unidad de tiempo, independientemente de que los mismos lleven o no información.

La velocidad binaria o de transmisión se mide en ***bits por segundo*** **– [bps].**

En las transmisiones asincrónicas este concepto carece de sentido porque la separación entre caracteres puede ser variable. Es por ello que en este tipo de transmisiones es recomendable utilizar solamente la noción de velocidad de modulación, dado que ésta no tiene en cuenta la separación entre caracteres ni tampoco los bits de arranque y parada.

La velocidad binaria o de transmisión se usa entonces en los sistemas sincrónicos. En ese caso, si las transmisiones no son del tipo multinivel (número de niveles que puede tomar la señal es mayor a 2) ambas coinciden.

Para un enlace de m canales, y de N niveles, la velocidad de transmisión será:

$$V_t = \sum_{i=1}^{i=m} \frac{1}{T_i} \log_2 N_i$$

Donde:

m = número de canales que transmiten en paralelo.

$\mathbf{T_i}$ = es la menor duración teórica de un elemento de la señal, expresada en segundos, para el i-ésimo canal.

$\mathbf{N_i}$ = es el número de estados significativos de la modulación del i-ésimo canal.

2.1.2.1 Formas particulares de la fórmula de la velocidad binaria o de transmisión

A fin de poder obtener posteriormente importantes conclusiones sobre estos conceptos, analicemos algunos casos particulares:

Para un solo canal que transmita en el modo serie, la expresión, al ser *m* = 1, quedará simplificada de la siguiente manera:

En el caso de que la modulación sea binaria, es decir, n = 2, la expresión se podrá simplificar aún más y quedará como se muestra, ya que $\log_2 2 = 1$

$$Vt = 1/\tau \cdot \log_2 N = [bps]$$

$$V_t = 1/\tau \; . \; 1$$

Esta expresión coincide con la correspondiente a la de velocidad de modulación, por lo que en este único caso particular ambas velocidades poseen la misma expresión pero distintas unidades.

Para el caso de modulaciones de cuatro, ocho y dieciséis estados significativos, resultan, de acuerdo con la expresión:

$$\log_2 4 = 2; \quad \log_2 8 = 3; \quad \log_2 16 = 4$$

Luego la velocidad de transmisión para dichos estados será:

$$V_t = 1/\tau \cdot 2 \qquad V_t = 1/\tau \cdot 3 \qquad V_t = 1/\tau \cdot 4 \quad [*]$$

2.1.2.2 Relación entre la velocidad binaria o de transmisión y la velocidad de modulación

Para establecer una relación entre ambas velocidades, recordemos que la Vm = $1/\tau$, por lo tanto reemplazando en la expresión **[*]** resultará:

$$Vt = 2\ Vm \qquad Vt = 3\ Vm \qquad Vt = 4\ Vm$$

A partir de estas expresiones se deduce que al aumentar el número de estados significativos de la señal (cuatro, ocho y dieciséis niveles respectivamente), es posible duplicar, triplicar o cuadruplicar la *velocidad binaria* o de transmisión sin aumentar la *velocidad de modulación.*
Otra consecuencia importante es que para pulsos de señal de igual duración, si se aumenta la velocidad de modulación (disminución del ancho de pulso), sin alterar el número de niveles que puede tomar la señal aumenta la velocidad binaria o de transmisión. Resumiendo, los dos procedimientos clásicos para aumentar la velocidad binaria o de transmisión son:

- Aumentar el número de niveles significativos de la señal sin alterar la velocidad de modulación.
- Disminuir el ancho de pulso de la señal, sin alterar el número de niveles que puede tomar la señal.

Se puede observar que la velocidad de transmisión depende del logaritmo en base 2 del número N de niveles que toma la señal.

En efecto:

$$V_t = 1/\tau \cdot \log_2 N$$

Donde N = número de niveles de una señal.

Se denomina transmisión multinivel a aquélla en la que el número de niveles que puede tomar la señal es mayor que 2.

Cuando el número de niveles es 2, la transmisión se denomina **binaria**. Para ello, considérese transmitir la señal digital 100011100101, donde cada bit se transmite por medio de un pulso.

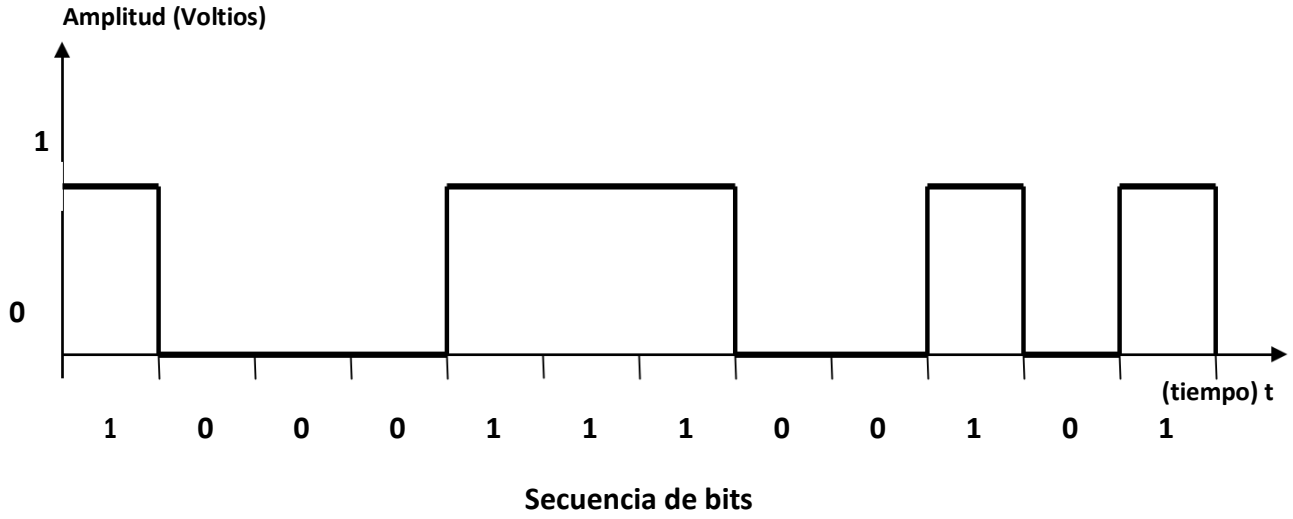


Fig. 2.1.2.2.a: Transmisión binaria donde cada bit se transmite por medio de un pulso.

Cuando el logaritmo en base 2 de N es mayor que uno, la velocidad de transmisión aumenta sin que aumente la velocidad de modulación por lo tanto, se podrá transmitir una mayor cantidad de bits por baudio, aumentando la eficiencia del canal de comunicaciones.

2.2 Transmisión Multinivel

Como ya se ha dicho, un aumento de la velocidad de modulación sin un aumento del ancho de banda hace que la cantidad de errores vaya aumentando, y a veces puede llegar a ser tan elevada que hace que la comunicación sea prácticamente inútil.

Es por ello que se han ido explorando técnicas que, sin alterar el esquema físico antes señalado, permitan mejorar sustancialmente la cantidad de información que se puede transmitir por un ancho de banda determinado.

También es importante destacar que un canal se puede hacer más eficiente bajando el nivel de ruido del mismo, y mediante otras técnicas de transmisión que reciben el nombre de **ecualización de los canales.** Estas técnicas dependen de la voluntad del proveedor de los servicios de transmisión de datos.

Existen técnicas de transmisión multinivel cuyo uso y aplicación están al alcance de los usuarios, y que son:

- **Dibits**

Dado que la cadencia de una transmisión de datos binaria es el número de veces que una señal cambia de nivel, veremos cómo podremos enviar dos unidades de información (bits) mediante un solo cambio de nivel (baudio), es decir un solo pulso.

Para ello se transmitirá la misma cadena digital: 100011100101

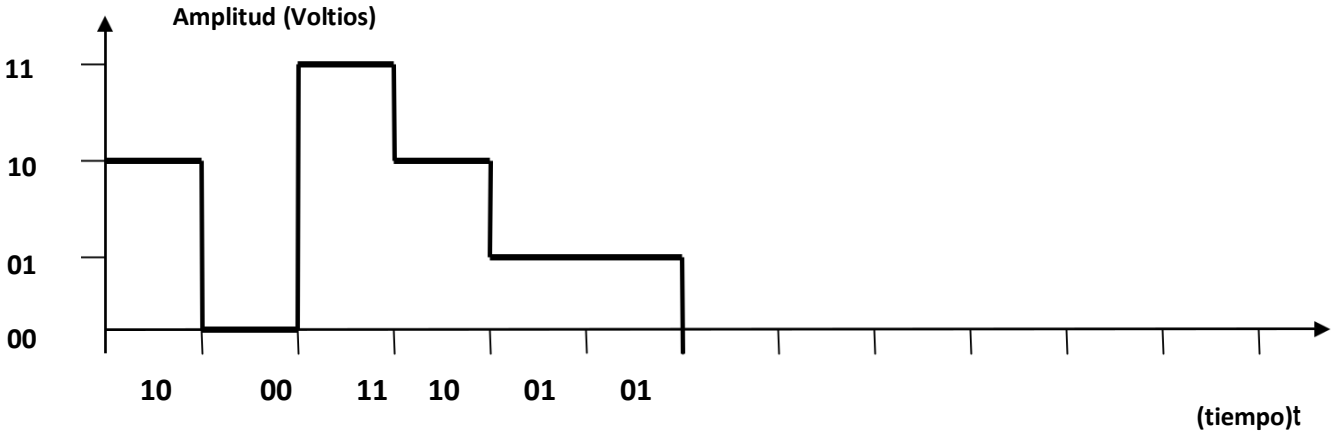
Si a los 12 bits de la cadena de información a transmitir, los tomamos de dos en dos, es decir, si formamos grupos de dos bits consecutivos, que denominaremos ***dibits***, tendremos los siguientes pares:

10	**00**	**11**	**10**	**01**	**01**

Como se puede observar, al tomar de dos en dos las señales binarias, que sólo pueden ser ceros (0) o unos (1), solamente hay cuatro combinaciones posibles, a saber:

Combinaciones Posibles	00	01	10	11

Si a estos pares de bits le asignamos distintos niveles de señal, tendremos la siguiente secuencia de bits:



Secuencia de dibits

Fig. 2.1.2.2.b: Transmisión por medio de dibits

Por lo tanto, la secuencia de datos de la señal binaria (originalmente un tren de pulsos de 12 bits), se transformó en transmisión de dibits. Como no se ha modificado el ancho de pulso, la velocidad de modulación no varía, pero se transmite el doble de la información, en otras palabras, ***la velocidad de transmisión se duplica sin que la velocidad de modulación cambie.***

- **Tribits y Cuatribis**

De la misma manera, si se quisiera mejorar aún más el coeficiente ***n*** de la expresión anterior, la cantidad de niveles necesarios para enviar **3 bits** en un solo pulso, resultaría ser:

$$N = 2^n$$

Donde:

N = número de niveles a transmitir.
n = Número de bits por pulso transmitido.

Luego:

Para n = 2, se necesitarán 4 niveles y se obtendrán ***dibits*****.**
Para n = 3, se necesitarán 8 niveles y se obtendrán ***tríbits***. (Ver **Fig. 2.1.2.2.c**)
Para n = 4, se necesitarán 16 niveles y se obtendrá ***cuadribits***

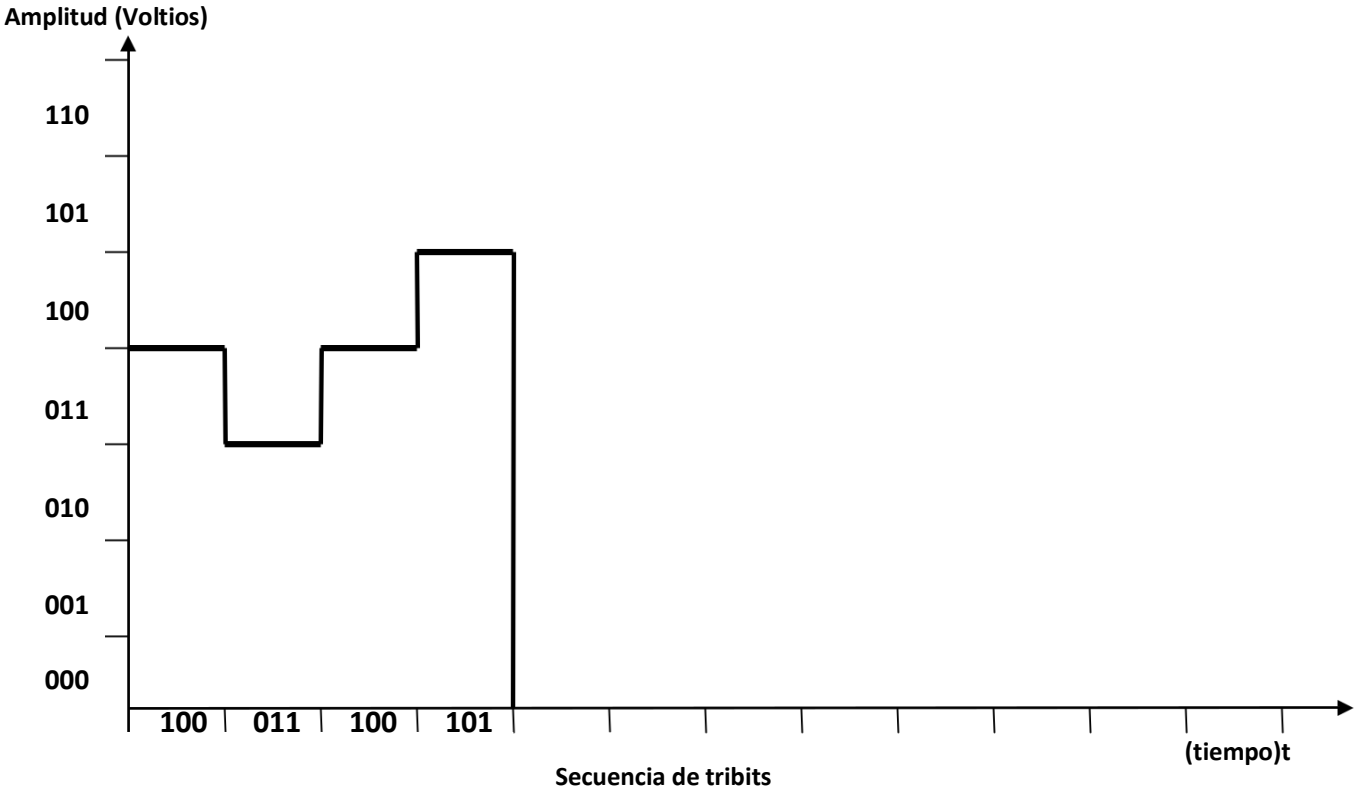


Fig. 2.1.2.2.c: Transmisión por medio de tribits

La mayoría de los equipos (modem) que transmiten a velocidades de más de 2400 bps, emplean este método para aumentar las velocidades de transmisión al tiempo que mantienen la velocidad de modulación en 2400 baudios.

Cuando se procede a hacer una conexión a la red usando las facilidades que muchos de los sistemas operativos actuales ofrecen, en el momento de la conexión suelen indicar la velocidad de transmisión a la que el módem se conectó con el corresponsal; y muchas veces se advierten velocidades menores a las que el equipo ofrece como velocidad máxima. Lo que ha ocurrido es que por defectos en la línea de comunicaciones, el módem prefirió utilizar una velocidad menor, para que la cantidad de errores fuese razonable.

2.3 Velocidad de transferencia de datos

Se puede definir un concepto de velocidad que se encuentra relacionada con el enlace de datos y se refiere a los bits que contienen exclusivamente información. Ésta se denomina **velocidad de transferencia de datos** y se define como:

El número medio de bits por unidad de tiempo que se transmiten entre equipos correspondientes a un sistema de transmisión de datos.

Vtd = número de bits transmitidos / tiempo empleado

Normalmente la Vtd se mide en bps (bits por segundo), aunque si en lugar de bits, se consideran bytes, caracteres, palabras o bloques, se obtendrán unidades del tipo bytes/seg. o caracteres/seg.

Corresponde siempre señalar entre que puntos se ha considerado esta velocidad, por lo que debe indicarse los equipos terminales de datos que hacen de fuente, y los equipos terminales (módem) o intermedios del circuito de datos.

La velocidad de transferencia de datos se refiere siempre a las señales digitales enviadas por la fuente y recibidas por el colector, por ello se relaciona con los bits que contienen **información.**

2.3.1 Velocidad real de transferencia de datos

Otra definición importante surge cuando se tienen en cuenta los errores de transmisión, si los hubiera; y así se puede definir la llamada **velocidad real de transferencia de datos**.

Número medio de bits por unidad de tiempo que se transmiten entre los equipos de un sistema de transmisión de datos, a condición de que el receptor de los mismos los acepte como válidos.

Como se puede apreciar, esta definición es exactamente igual a la de velocidad de transferencia de datos, a excepción de que *aquí se requiere que se midan sólo los bits, bytes, palabras o bloques sin errores de transmisión*, que han llegado de la fuente transmisora al equipo receptor.

Vrtd = Vtd * R (R = rendimiento)

Como R es un valor inferior a la unidad, siempre Vrtd será inferior a Vtd, lo que equivale a decir que *el régimen de **bps** disminuye*, por lo tanto el tiempo de transmisión aumenta.

(Rendimiento) R = Total bits válidos / Total Bits transmitidos * 100

Tr = Tc / R (Tr = Tiempo Real de transmisión y Tc = Tiempo Calculado)

El siguiente ejemplo nos permite fijar el concepto:

La velocidad de un canal es de 8000 baud y se emplean 4 niveles. El sistema transmite en forma sincrónica y la información no se comprime. El número medio de bits por unidad de tiempo que se transmite entre los equipos del sistema de transmisión de datos, a condición que el receptor de los mismos los acepte como válidos es el 70 % de la calculada teóricamente. Indique el tiempo real que tardara en transmitir 22400 caracteres de 8 bits cada uno.

¿Qué pregunta el problema?

- TIEMPO

¿Qué datos proporciona?

- Vm= 8000 baud.
- N= 4
- R= 70%
- Mensaje= 22400 caracteres de 8 bits cada uno.

¿Cómo utilizamos los datos para obtener el resultado?

Si bien Vm se mide en baud se sabe que:

Vm = 1 / τ donde τ es el ancho de pulso que se mide en segundos. De allí se obtiene el tiempo.

Como τ = 1 / Vm entonces τ = 1 / 8000 baud y se obtiene τ = 0,000125 seg

Como se emplean 4 niveles, se transmiten 2 bits por cada pulso, es decir en 0,000125 seg, se transmiten 2 bits.

Tiempo en transmitir un bit = τ / 2 = 0,0000625 s.

Sabemos que un carácter tiene 8 bits entonces

Tiempo en transmitir un carácter = Tiempo en transmitir un bit * 8 = 0,0000625 seg * 8 =>

Tiempo en transmitir un carácter = 0,0005 seg

Entonces el tiempo para transmitir 22400 caracteres es:

Tiempo en transmitir un carácter * 22400 = 0,0005 s * 22400

Tiempo en transmitir 22400 caracteres = 11, 2 s (Tiempo calculado)

Por enunciado se sabe que *e*l sistema de transmisión tiene un rendimiento del 70 %.

Tiempo Real = Tiempo calculado / Rendimiento (Tr = Tc / R) entonces

Tr = 11, 2 s / 0.7 = ***16 s***

Respuesta: El **tiempo real** que tardara en transmitir **22400 caracteres de 8 bits c/u,** es **16 seg.**

2.5 Ancho de Banda

El concepto de ancho de banda es uno de los más importantes y actuales en el campo de las telecomunicaciones. En inglés se denomina Bandwidth (BW).

Se denomina ancho de banda al Intervalo de frecuencias para las cuales la distorsión lineal y la atenuación permanecen bajo límites determinados y constantes. Los valores que se toman como valores de referencia pueden ser arbitrarios.

$$\Delta f = f_2 - f_1$$

La ocupación del ancho de banda se puede definir como:

La cantidad de información que puede fluir a través de una conexión de red en un período dado.

Si bien los límites pueden ser arbitrarios, en la generalidad de los casos, se definen para una atenuación de 3 dB con respecto al valor que tiene la señal a la frecuencia de referencia. Los valores de F_1 y F_2 se denominan límites inferior y superior del ancho de banda de una señal. Para los mismos la atenuación de la señal es de **3 dB** respecto al valor f_0 de referencia, que se encuentra a **0 dB.**

2.5.1 Importancia del Ancho de Banda

Es esencial comprender el concepto de ancho de banda al estudiar redes, por las siguientes cuatro razones:

- **El ancho de banda es finito.** Independientemente del medio que se utilice para construir la red, existen límites para la capacidad de la red para transportar información. El ancho de banda está limitado por las leyes de la física y por las tecnologías empleadas para colocar la información en los medios.
- **El ancho de banda no es gratuito.** Comprender el significado del ancho de banda, y los cambios en su demanda a través del tiempo, pueden ahorrarle importantes sumas de dinero a un individuo o a una empresa. Por ejemplo, contratar a un proveedor del servicio un enlace de 300 Mbps no cuesta lo mismo que uno de 100 Mbps.
- **El ancho de banda es un factor clave a la hora de analizar el rendimiento de una red, diseñar nuevas redes.** La información fluye en una cadena de bits de una computadora a otra en todo el mundo. Estos bits representan enormes cantidades de información que fluyen de ida y de vuelta a través del planeta en segundos, o menos.
- **El ancho de banda es fundamental para el desempeño de la red.** No bien se construyen nuevas tecnologías e infraestructuras de red para brindar mayor ancho de banda, se crean nuevas aplicaciones que aprovechan esa mayor capacidad. La entrega de contenidos de medios enriquecidos a través de la red, incluyendo video y audio fluido, requiere muchísima cantidad de ancho de banda.

Más arriba definimos a la ocupación del ancho de banda como la cantidad de información que puede fluir a través de una red en un período dado. La idea de que la información fluye, sugiere dos analogías que podrían facilitar la visualización del ancho de banda en una red:

- **El ancho de banda es similar al diámetro de un caño.** Una red de tuberías trae agua a los hogares y se lleva las aguas servidas. Esta red de agua está compuesta de tuberías de diferentes diámetros. Las principales tuberías de agua de una ciudad pueden medir dos metros de diámetro, en tanto que la tubería de un grifo de cocina puede medir apenas media pulgada. El ancho de la tubería determina su capacidad de transporte de agua. Por lo tanto, el agua es como los datos, y el ancho de la tubería es como el ancho de banda, como se muestra a continuación:

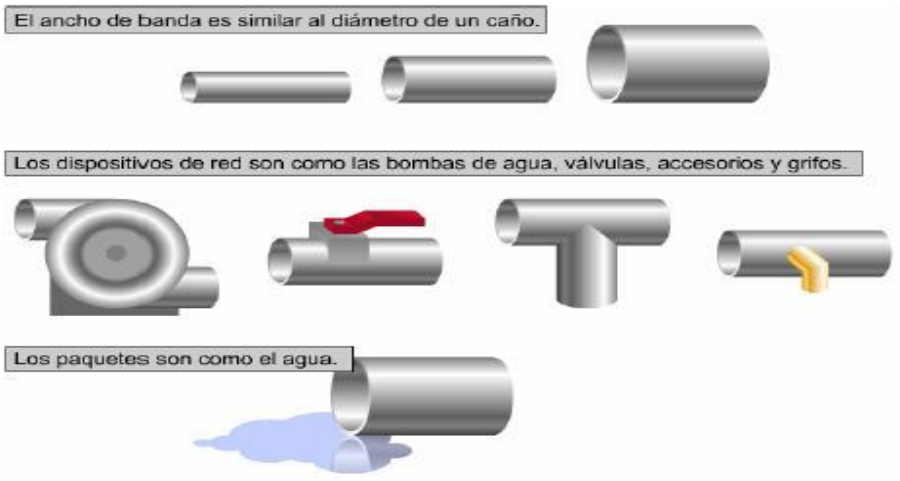


Fig. 2.5.1.a: Analogía del ancho de banda con la red de agua.

El ancho de banda puede compararse también con la cantidad de carriles de una autopista. Una red de caminos sirve a cada ciudad o pueblo. Las grandes autopistas con muchos carriles se conectan a caminos más pequeños con menor cantidad de carriles. Estos caminos llevan a otros aún más pequeños y estrechos, que eventualmente desembocan en las entradas de las casas y las oficinas. Cuando hay poco tráfico en el sistema de autopistas, cada vehículo puede moverse con libertad. Al agregar más tráfico, cada vehículo se mueve con menor velocidad. Eventualmente, a medida que se suma tráfico al sistema de autopistas, hasta aquéllas con varios carriles se congestionan y vuelven más lentas. Una red de datos se parece mucho al sistema de autopistas. Los paquetes de datos son comparables a los automóviles, y el ancho de banda es comparable a la cantidad de carriles en una autopista:

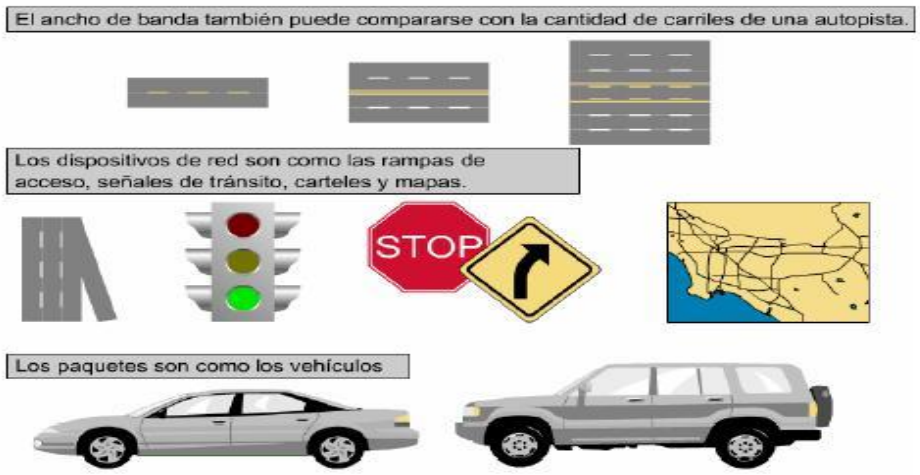


Fig. 2.5.1.b: Analogía del ancho de banda con la red vial.

2.5.1 Relación entre errores y el Ancho de Banda

Durante el proceso de transmisión, las señales sufren tres fenómenos: ***atenuación, distorsión y ruido***. Estos fenómenos son, en última instancia, la causa de los errores de transmisión, el retraso producido por implicancia de cualquiera de estos fenómenos se denomina latencia.

Por muchas razones, siempre se intenta que el tiempo de transmisión sea mínimo, algunas de ellas son las siguientes:

- Para lograr que el procesamiento de la información sea más eficiente, es necesario que llegue la mayor cantidad de datos por unidad de tiempo.
- Cuando se opera en tiempo real los operadores deben esperar una respuesta en el menor tiempo posible. Por ejemplo, una transferencia a través de Cajero Automático.

Por estas y otras muchas razones se busca transmitir a la mayor velocidad posible. Sin embargo, la velocidad está directamente relacionada con el ancho de banda disponible y con el nivel de ruido existente en el canal de comunicaciones que se use, y es precisamente la denominada *velocidad de modulación*, o *velocidad de señalización*, como se la llamaba antiguamente la que **está directamente relacionada con el ancho de banda disponible**.

Cuanto mayor es la velocidad de modulación, menor es el período T de cada ciclo transmitido.

Cuando se fuerza una determinada velocidad de modulación por encima de lo que permite el ancho de banda disponible entonces el canal de comunicaciones reaccionará aumentando la cantidad de errores.

En la siguiente tabla se presentan los principales fenómenos que alteran las comunicaciones:

Fenómenos	Características
Atenuación	○ Se caracteriza por la disminución de la intensidad de la señal a medida que recorre el medio de comunicaciones. ○ La atenuación aumenta en forma proporcional a la distancia recorrida desde el emisor. ○ Su efecto es la reducción en la amplitud de la señal. ○ La atenuación es propia del cable o elemento conductor. ○ El efecto es más notable en las redes analógicas.
Distorsión	○ En términos prácticos, el efecto es una deformación de la señal original. ○ El efecto es más notable en las redes digitales.
Ruido	○ Es toda perturbación o interferencia no deseada que se introduce en el canal de comunicaciones. ○ Su característica es la aditividad, pues su intensidad se suma a la de la propia señal de información que se desea transmitir. ○ El efecto del ruido es también el de una deformación. ○ Si se amplifica una señal, el ruido también es amplificado.

Tabla 2.5.1.a: Fenómenos que alteran las comunicaciones.

Para resolver estos fenómenos se utilizan distintos dispositivos que se exponen en la siguiente tabla:

Equipo	Características
Amplificador	○ Se utiliza para solucionar el problema de la atenuación en las redes analógicas. ○ Las señales que le **llegan,** están atenuadas respecto de su amplitud original; y las que **salen** tienen un nivel de amplitud tal que pueden ser detectadas por el receptor. ○ Tiene su propio ruido interno que se suma a la señal que se desea amplificar. ○ En consecuencia, si en un canal analógico se añaden cada vez más amplificadores para resolver el problema de la atenuación, se llega a un punto en el que el ruido es tan grande que la señal original se pierde.
Repetidor regenerativo	○ Permiten generar los pulsos luego que estos sufren fundamentalmente el proceso de distorsión en las redes digitales. ◦ No se trata de una amplificación, sino de la reconstrucción de la señal con una forma semejante a la original.
Filtros	○ Son aquellas partes de las redes de comunicaciones que presentan características selectivas respecto de las frecuencias. ○ El filtro permite seleccionar las frecuencias de las señales que pasarán libremente, de otras frecuencias indeseables, que no pasarán. ○ De esta manera la señal original queda libre de lo que se llama interferencias producidas por el ruido.

Tabla 2.5.1.b: Dispositivos para resolver fenómenos que alteran las Comunicaciones.

En resumen:

Fenómeno	Tipo de red	Afecta	Solución

Atenuación	Analógica	Amplitud	Amplificador
Distorsión	Digital	Deformación de la señal	Repetidores Regenerativos
Ruido	Ambas	Deformación de la señal	Filtros

Tabla 2.5.1.b: Resumen de los fenómenos, tipo de red afectada y su solución.

2.6 Compresión de Datos

El desarrollo de la informática y la teleinformática ha provocado en los últimos años un crecimiento acelerado de los volúmenes de información que deben ser almacenados en bases de datos.

La necesidad de transferir estos crecientes volúmenes de datos a través de redes de comunicación, ha ido acrecentando los problemas que deben resolver los administradores de red.

Los dueños de computadoras personales no han sido ajenos a este fenómeno, ya que hoy en día necesitan discos de mayor tamaño, más ancho de banda, y mayor capacidad de procesamiento para su instalación y operación.

Día a día se va exigido a la industria del hardware dispositivos más veloces y sistemas de multiplexado de canales de comunicaciones más eficientes (recordar concepto de multiplexor o selector). Estos equipos, se mejoran constantemente con el objeto de abaratar costos y optimizar el canal de las comunicaciones.

Dentro de este esquema, los sistemas de **compresión de datos** han ido ganando mercado rápidamente. Estos sistemas, al utilizar códigos más sofisticados o métodos lógicos de compresión, permiten reducir el volumen de datos y abaratar las transmisiones. Así se logra transferir mayor cantidad de información en tiempos menor tiempo sin necesidad de aumentar el ancho de banda.

La compresión de datos, en resumen, actúa sobre un **circuito teleinformático** de la misma manera que las señales multinivel, ya que mejora aún más la velocidad de transmisión, pero ésta vista desde la óptica exclusiva del Equipo Terminal de Datos. Esto significa que ***la velocidad de transmisión en el canal de comunicaciones queda totalmente inalterada.***

La compresión de datos permite aumentar la **velocidad real de transferencia de datos** manteniendo constante tanto la *velocidad de modulación* como la *velocidad de transmisión*.

La compresión de datos es una técnica que permite reducir el tamaño de un conjunto de datos sin alterar el significado de la información que contiene.

- Indice de compresión: **Es el número que resulta de dividir la longitud original de un conjunto de datos (medidos en bits o en bytes) por la longitud del mismo conjunto luego de haber sido comprimido.**

C = longitud original del conjunto de datos / longitud comprimida del conjunto de datos.

Como se puede apreciar, la longitud original del conjunto de datos a comprimir será siempre mayor que la de los datos ya comprimidos, por lo que el cociente será siempre mayor que uno.

C (índice de compresión) >1

Capítulo III: Redes de Información

3.1 Introducción a Redes

El crecimiento sin precedente de la industria de las computadoras, ha progresado en muy corto tiempo. El modelo de tener una sola computadora para satisfacer todas las necesidades de una organización se remplazó por otro que considera un número importante de computadoras separadas, **pero interconectadas**. Estos sistemas, se conocen con el nombre de **redes informáticas**.

3.1.1 Utilización de Redes de Computadoras

Inicialmente cada una de estas computadoras puede haber estado trabajando en forma aislada de las demás pero, en algún momento, se decidió **interconectarlas conformado una red**.

Por tanto, se infiere que el objetivo principal de una red es **compartir recursos**, además poseen los siguientes objetivos básicos:

✓ Hacer que todos los programas, datos y equipos estén disponibles para cualquiera de la red que así lo solicite, sin importar la localización física del recurso y del usuario.

✓ Proporcionar fiabilidad y respaldo, contar con fuentes alternativas de suministro, copia de archivos de resguardo, servidores redundantes, es decir si una computadora deja de funcionar, las otras pueden ser capaces de encargarse de su trabajo.

✓ Realizar un ahorro económico. Las computadoras pequeñas tienen una mejor relación costo / rendimiento, comparada con máquinas grandes, que son mucho más rápidas que el más rápido de los microprocesadores, pero su costo es altísimo.

✓ Proporcionar un poderoso medio de comunicación entre personas que se encuentran alejadas entre sí. Por medio de una red es mucho más fácil la cooperación e intercambio.

3.2. Tipos de redes

No existe un consenso que incluya todas las formas de redes de computadoras, pero se las puede encasillar en dos dimensiones básicas: **la tecnología de transmisión** y **la escala de difusión (de acuerdo a la cantidad de receptores)**. En términos generales hay dos tipos de tecnología de transmisión:

➢ **Redes de Difusión:** Tienen un solo canal de comunicación compartido por todas las máquinas de la red. Los "mensajes" que envía una máquina son recibidos por todas las demás, en los mismos existe un campo de dirección que especifica el destinatario. Al recibir el mensaje, la máquina verifica el campo de dirección, si está dirigido a ella, lo procesa; si está dirigido a otra máquina lo ignora. Los sistemas de difusión también ofrecen la posibilidad de dirigir mensajes a todos los destinos, mediante la utilización de un código especial en el campo de dirección. Así, un mensaje con este código, cada máquina en la red lo recibe y lo procesa. Este modo de operación se llama difusión (**"broadcasting**"). Algunos sistemas de difusión también contemplan la transmisión a un subconjunto de las máquinas, algo que se conoce como ***multidifusión***.

➢ **Redes de Punto a Punto:** Consisten en muchas conexiones entre pares individuales de dispositivos. Para ir del origen al destino un mensaje en este tipo de red puede tener que visitar uno o más dispositivos intermedios. A veces son posibles múltiples rutas de diferentes longitudes, por lo que los algoritmos de encaminamiento[1] son muy importantes en estas redes.

[1] El encaminamiento es un proceso a seguir para encontrar un camino entre dos puntos. Un algoritmo de encaminamiento es un método para calcular la mejor ruta entre ellos.

3.2.1 Intranet

Una intranet no es más que una red local funcionando como lo hace Internet, es decir usando el conjunto de protocolos TCP/IP en sus respectivos niveles.

Engloba a todo un conjunto de redes locales con distintas topologías y cableados, pero que en sus niveles de transporte y de red funcionan con los mismos protocolos. Este hecho facilita enormemente la conexión con otros tipos de redes a través de Internet, puesto que utiliza sus mismos protocolos. Además todas las herramientas y utilidades que existen para Internet, se pueden utilizar en una Intranet (creación de páginas Web, correo electrónico, etc.).

3.3 Extensión de las redes

Se pueden clasificar en:

- **LAN**: Red de Área Local o **L**ocal **A**rea **N**etwork

Cuando la información se comparte entre usuarios que están distribuidos en un mismo ámbito o edificio, es posible instalar una red cuyas principales **características** son las siguientes:

Es una red de transmisión privada para el entorno que se pretende cubrir.
Puede conectarse un gran número de recursos.
Su extensión suele ser a un edificio o conjunto de edificios cercanos
Permiten la conexión a otras redes.

Estas características hacen que la construcción de redes locales, forma y métodos de acceso varíen substancialmente con respecto a las redes de área extensa.

- **WAN:** Red de Área Extensa o **W**ide **A**rea **N**etwork

Surgen para satisfacer las necesidades de transmisión de datos a distancias mayores. Se utilizan principalmente para unir redes locales, son construidas por organizaciones o montadas por proveedores para brindar conexión a sus clientes entre distintas ciudades o países, utilizando la red pública de telefonía.

3.4 Criterios de Diseño de LAN

Medios de comunicación

A la hora de seleccionar equipo para el montaje de una red, o de planificar la expansión de una existente, se deberán conocer las distintas opciones que existen para implementar la conexión. La comunicación entre dos o más sistemas de computadoras por medio de señales eléctricas (como son los niveles de tensión), necesitan de un medio de transmisión. El tipo de medio que se utilice limita la velocidad de transmisión y la máxima distancia que puede existir entre los equipos que se intercomunican.

Una primera clasificación sería:

- **Aéreos:** basados en señales radio eléctricas (utilizan la atmósfera como medio de transmisión), en señales de rayos láser o rayos infrarrojos.

- **Sólidos:** principalmente el cobre en par trenzado o cable coaxial y la fibra óptica.

Previamente debemos recordar que las señales se propagan por los medios en forma de ondas electromagnéticas. Este concepto vale tanto para la propagación en medios sólidos como para los aéreos. La velocidad de propagación de la onda depende del medio, ya sea sólido o aéreo.

El alumno puede ampliar este tema en el ANEXO ubicado al finalizar este apunte.

Son varios los criterios que se deben tener en cuenta al planificar una red, entre ellos está la topología de la misma.

Topologías

La **topología** de una red es el patrón geométrico empleado para configurar los nodos (computadoras) y líneas físicas de la red. Actualmente las topologías están relacionadas con el método de acceso al cable, puesto que éste depende casi exclusivamente de la tarjeta de la red y ésta depende de la topología elegida. Se presentan a continuación las distintas variantes existentes.

3.4.1 Topología Física

Se ocupa de la forma en la que el cableado se realiza en una red. Se describen tres topologías físicas, pero se debe saber que en la actualidad las redes se diseñan con topología en estrella.

- ***Topología en bus***

En el tipo **Bus**, un cable común transita a través de todos los sitios donde exista una computadora que se conecta a la red. Por medio de un elemento llamado "*tap*", el usuario del nodo tiene acceso a los servicios del cable.

Fig. 3.4.1.1.a: Red LAN en topología BUS.

Topología en anillo

Con la topología en **Anillo,** se logra una conexión punto a punto entre cada par de computadoras vecinas de manera unidireccional y continua hasta cerrar el anillo.

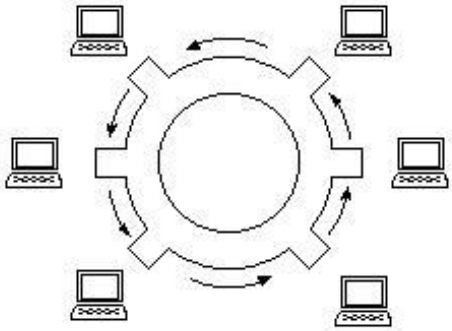


Fig. 3.4.1.1.b: Red LAN en anillo

Topología en estrella

La topología tipo **Estrella**, es la más utilizadas actualmente. Utiliza dispositivos concentradores**.** Los cables que se requieren para conectar más computadores a la red se conectan, entonces, a la salida de los dispositivos concentradores.

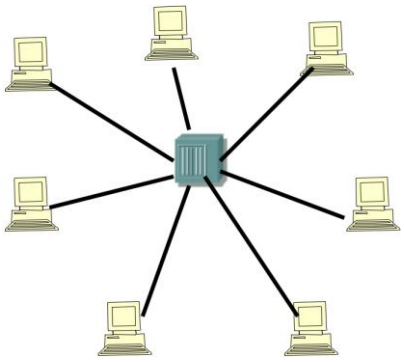


Fig.3.4.1.1.c: Topología en estrella

3.5 Dispositivos de Interconexión

- **Hubs:**

Dispositivo que interconecta host dentro de una red. Es el dispositivo de interconexión más simple que existe.

Fig. 3.5.a: Hub.

Sus principales características son:

- Se trata de un de un dispositivo de múltiples puertos o "bocas" donde se centralizan todas las conexiones de una red, es decir un dispositivo con muchos puertos de entrada y salida.
- No tiene ninguna función aparte de centralizar conexiones y distribuir la información a todos los puestos conectados (broadcast).
- Se suelen utilizar para implementar topologías en estrella física.

Estos dispositivos tienden a desaparecer dado que no permiten la segmentación de dominios y el costo es similar al de un Switch (cuya funcionalidad detallaremos más adelante).

- **Bridges** (puentes)

Es un dispositivo de interconexión de redes que permite conectar dos segmentos de una misma red. También permite segmentar una red en otras redes menores denominadas subredes. A nivel de enlace el Bridge comprueba la dirección de destino y hace copia hacia el otro segmento si allí se encuentra la estación de destino.

Fig. 3.5.b: Bridge

- **Switchs** (enlazadores)

Son los dispositivos más utilizados para interconectar los host las en redes de área local y proveer un filtrado de paquetes (es decir, que la información se transmite sólo hacia el dispositivo destinatario de la misma). Su símbolo se muestra en la Fig. 3.5.c. Los switches agregan inteligencia a la administración de transferencia de datos. No sólo son capaces de determinar si los datos deben permanecer o no en una LAN, sino que pueden transferir los datos únicamente a la conexión que necesita esos datos.

Fig.3.5.c: Símbolo de un Switch

Sus principales características son:

- Ayudan a resolver problemas de limitación de distancias, junto con el problema de limitación del número de nodos de una red.
- Los switchs no entienden de direcciones de **IP**, ya que trabajan en otro nivel, trabajan con direcciones físicas llamadas **MAC** (Media Access Control)[2].

[2] Es una dirección de 48 bits que identifica de forma única a cada placa de red.

- Tienen la capacidad de "aprender", mediante el armado de tablas, las direcciones MAC de los dispositivos a su alcance a través de cada uno de sus puertos. Utilizan esto para transmitir los datos únicamente hacia la conexión que los necesita, lo que ayuda a disminuir el tráfico de la red.
- Divide dominios de colisión[3].
- Un LAN Switch es un dispositivo con múltiples puertos, cada uno de los cuales puede soportar una simple estación de trabajo o bien toda una subred.
- Con una subred diferente conectada a cada uno de los puertos del Switch, este puede conmutar paquetes entre ellas, como sea necesario.
- Actúa como un Bridge multi-puerto, los paquetes son filtrados por el Switch basándose en su dirección de destino.

➢ **Routers** (encaminadores)

Estos dispositivos ayudan a direccionar los mensajes mientras viajan a través de una red. Realizan funciones de control de tráfico y encaminamiento de información por el camino más eficiente en cada momento. Son capaces de modificar el camino establecido entre dos puntos de la red de acuerdo al tráfico.

Los routers pueden regenerar señales, concentrar múltiples conexiones, convertir formatos de transmisión de datos, y manejar transferencias de datos. También pueden conectarse a una WAN, lo que les permite conectar LAN que se encuentran separadas por grandes distancias. Ninguno de los demás dispositivos puede proporcionar este tipo de conexión.

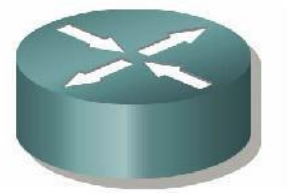


Fig. 3.5.d: Símbolo de un Router.

Sus principales características son:

- **Permite conectar redes de área local y de área extensa**. Habitualmente se utilizan para conectar una red de área local a una red de área extensa.
- **Son capaces de elegir la ruta más eficiente** que debe seguir un paquete en el momento de recibirlo.
- Posee una interfaz por cada una de las redes que conecta.

➢ **CPE (Equipo local del cliente)**

Antiguamente, las redes públicas de telefonía eran exclusivamente analógicas y, para poder conectar los equipos digitales a ellas, debían utilizarse equipos denominados modems. Cualquier usuario que quería conectarse a internet desde su hogar u empresa, debía tener un MODEM (las funciones de este dispositivo se comentaron en el capítulo 1). Hoy en día, la mayoría de las redes son digitales, por lo que no debe realizarse este proceso de modulación/demodulación para acceder a ellas; sin embargo, siguen siendo necesarios equipos del lado del cliente para acceder a internet; a estos quipos se los denomina CPE.

Un CPE es un equipo que se instala al "final" de una red, del lado del receptor. El CPE se conecta por un lado con la red del proveedor de servicios y, por el otro con los equipos informáticos del cliente. Engloba tanto a los equipos necesarios para comunicar una red doméstica como una empresarial. Algunos ejemplos conocidos de CPE son: los routers y los STBs (Set Top Boxes, para conectar con las TV).

[3] Los dominios de colisión son segmentos de red en los que pueden producirse colisiones entre las tramas de información.

Capítulo IV: Protocolos. Modelo OSI – ISO. Direccionamiento IP.

4.1 Protocolos

Antes de sus normalizaciones, cada fabricante establecía sus propias normas o protocolos, lo que impedía la comunicación entre equipos de diferentes fabricantes y el uso de redes ajenas.

Es así que para posibilitar la interconexión de diferentes equipos informáticos a través de las distintas redes de comunicaciones, obteniéndose lo que se denomina sistemas abiertos, ha sido necesario establecer una serie de convenciones que afectan a los requerimientos físicos y los procedimientos a seguir. Para ello, diversos organismos Internacionales se han encargado de dictar las normas necesarias, principalmente la **ISO** (*International Standard Organization*) a escala mundial y el **CCITT** (*Consultive Committee for International Telephone and Telegraph*) en el ámbito europeo.

Se recuerda la definición del Capítulo 1: **Protocolo es el conjunto de normas, convenciones y procedimientos que regulan la comunicación de datos y el comportamiento de procesos entre diferentes equipos, bien totalmente o bien en alguno de sus aspectos.**

4.2 Uso de Capas para describir la Comunicación de Datos

Para el establecimiento de las normas que afectan a gran variedad de elementos implicados en la comunicación, se ha decidido dividir el problema en otros más pequeños, determinándose una serie de subconjuntos denominados **niveles de comunicación**. Cada nivel contempla una parte de elementos afectados. Sus requerimientos y convenciones se abordan de forma independiente, lo que permite que las modificaciones de un nivel no afecten a los restantes. Algunos autores cuando se refieren a niveles, lo denominan comúnmente ***capas.***

El concepto de capas se utiliza para describir la comunicación entre dos computadoras. La siguiente figura muestra un conjunto de preguntas relacionadas con flujo, que se define como el movimiento de objetos físicos o lógicos, a través de un sistema. Estas preguntas muestran cómo el concepto de capas ayuda a describir los detalles del proceso de flujo. Este proceso puede referirse a cualquier tipo de flujo, desde el flujo del tráfico en un sistema de autopistas, al flujo de datos a través de una red:

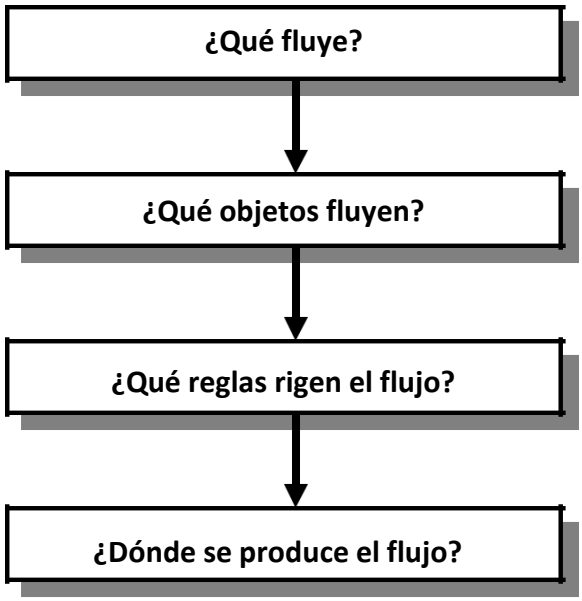


Fig. 4.2.a: Preguntas relacionadas con flujo a través de un sistema.

El mismo método de división en capas explica cómo una red informática distribuye la información desde el origen al destino. Cuando los computadores envían información a través de una red, todas las comunicaciones se generan en un origen y luego viajan a un destino.

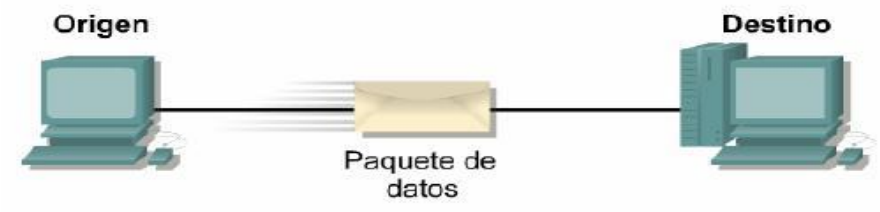


Fig. 4.2.b: Transmisión de Información utilizando paquetes.

Generalmente, la información que se desplaza por una red recibe el nombre de *datos* o *paquete*. Un *paquete* es una unidad de información, lógicamente agrupada, que se desplaza entre los sistemas de computación. A medida que los datos atraviesan las capas, cada capa agrega información que posibilita una comunicación eficaz con su correspondiente capa en cada dispositivo de la red.

Los modelos **OSI** y **TCP/IP** se dividen en capas que explican cómo los datos se comunican de una computadora a otra. Los modelos difieren en la cantidad y la función de las capas. No obstante, se puede usar cada modelo para ayudar a describir y brindar detalles sobre el flujo de información desde un origen a un destino.

Para que los paquetes de datos puedan viajar desde el origen hasta su destino a través de una red, es importante que todos los dispositivos de la red hablen el mismo lenguaje o protocolo, y cada capa usa el suyo. Tomando como ejemplo la capa 4, decimos que la Capa 4 del computador de origen se comunica con la Capa 4 del computador de destino. Las normas y convenciones utilizadas para esta capa reciben el nombre de protocolos de la Capa 4. El protocolo en una capa realiza un conjunto determinado de operaciones sobre los datos al prepararlos para ser enviados a través de la red. Los datos luego pasan a la siguiente capa, donde otro protocolo realiza otro conjunto diferente de operaciones.

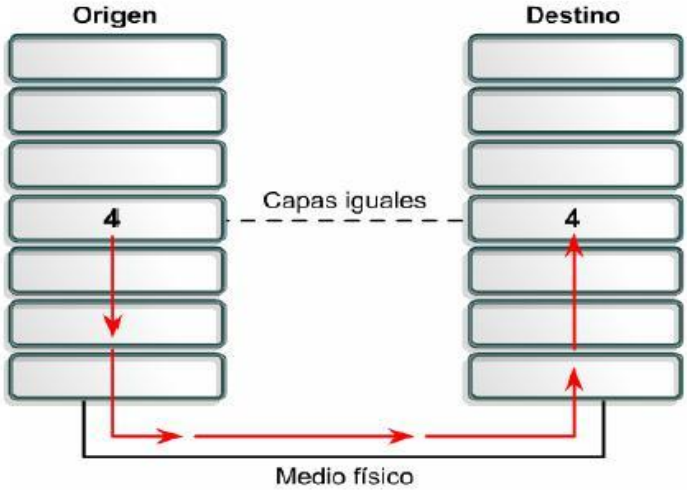


Fig. 4.2.c: Transmisión a través de capas.

Una vez que el paquete llega a su destino, los protocolos deshacen la construcción del paquete que se armó en el extremo de origen. Esto se hace en orden inverso. Los protocolos para cada capa en el destino devuelven la información a su forma original, para que la aplicación pueda leer los datos correctamente.

4.3 Modelo OSI-ISO

El inicio del desarrollo de las redes fue en cierto modo caótico. A comienzos de la década de 1980 se produjo una gran expansión en el área del desarrollo de redes. Y comenzaron a manifestarse los primeros inconvenientes producto de esta expansión. Cada vez era más difícil que las redes que utilizaban diferentes especificaciones e implementaciones pudieran comunicarse entre sí.

Para abordar el problema, la *Organización Internacional para la Normalización* (**ISO**) investigó los distintos esquemas de redes. Como resultado de esta investigación, la *ISO* reconoció la necesidad de crear un modelo de red que pudiera ayudar a crear redes que pudieran trabajar compatible e interoperativamente con otras redes. El modelo de referencia OSI (*Open System Interconnection*), lanzado en 1984, fue el esquema descriptivo que crearon y ofreció a los fabricantes un conjunto de estándares que garantizó mayor compatibilidad e interoperatividad entre los diversos tipos de tecnologías de redes que producían las diversas empresas mundiales.

El modelo de referencia *OSI* se convirtió rápidamente en el modelo principal para las comunicaciones de red. El modelo de referencia *OSI* no es algo tangible. Se trata de un marco conceptual, un modelo de estudio que especifica las funciones de red que se producen en cada capa. Está compuesto de siete capas, cada una de ellas tiene sus propias especificaciones y un protocolo.

- **Ventajas de un modelo en capas:**
  - Reduce la complejidad.
  - Estandariza Interfaces.
  - Facilita la Ingeniería modular.
  - Simplifica la enseñanza y el aprendizaje.

4.3.1 Capas del Modelo OSI

Las siete capas del Modelo OSI están representadas en el cuadro siguiente, donde se puede apreciar el orden, la denominación y la función de cada una de ellas:

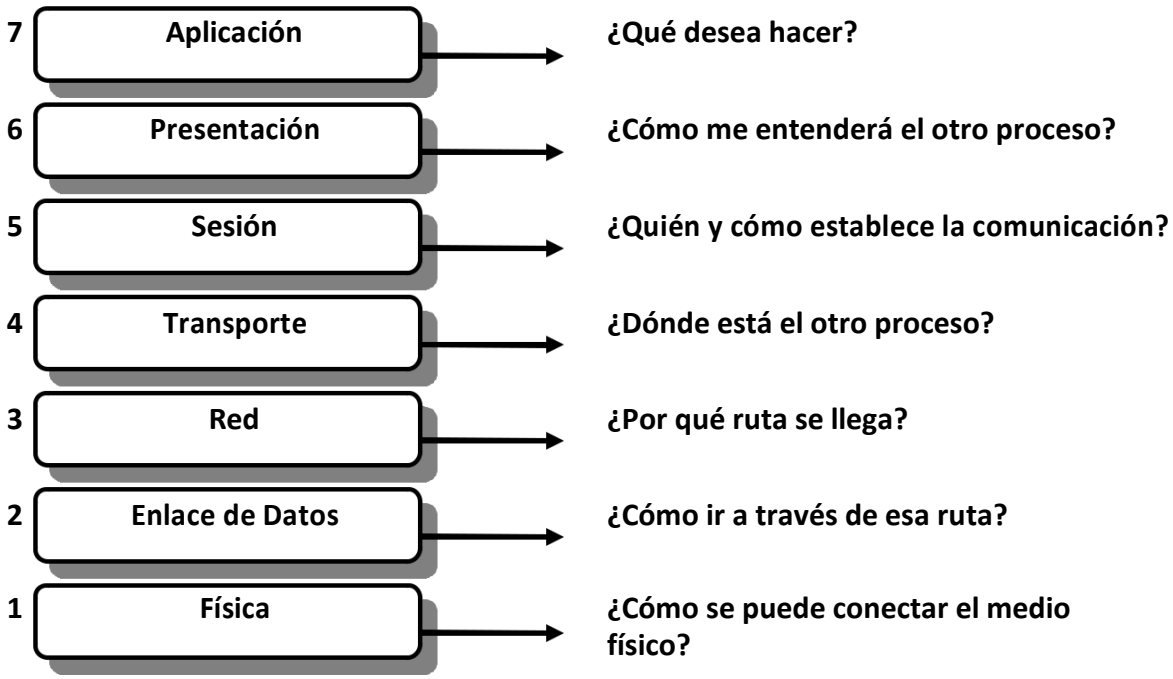


Fig. 4.3.1.a: Las 7 capas del modelo OSI.

Cada capa se comunica exclusivamente con las capas adyacentes, por ejemplo una capa de nivel N se comunica con la de nivel (N-1) y con la de nivel (N+1).

Según este modelo, al conjunto de datos generado en el equipo terminal que actúa como emisor o fuente se le va añadiendo, a través de los distintos protocolos de capa, la información necesaria para permitir el procesamiento del protocolo en el equipo que actuará como receptor. Cada conjunto de datos o información añadida se denomina **encabezamiento (header)**, y se van añadiendo a medida que pasa de una capa a otra hasta llegar a la capa física, capa que finalmente procederá a la transmisión de los correspondientes bits hacia el otro extremo.

El conjunto de información compuesta por **encabezamiento + datos,** recibe distintos nombres según el nivel en que están situados, a saber:

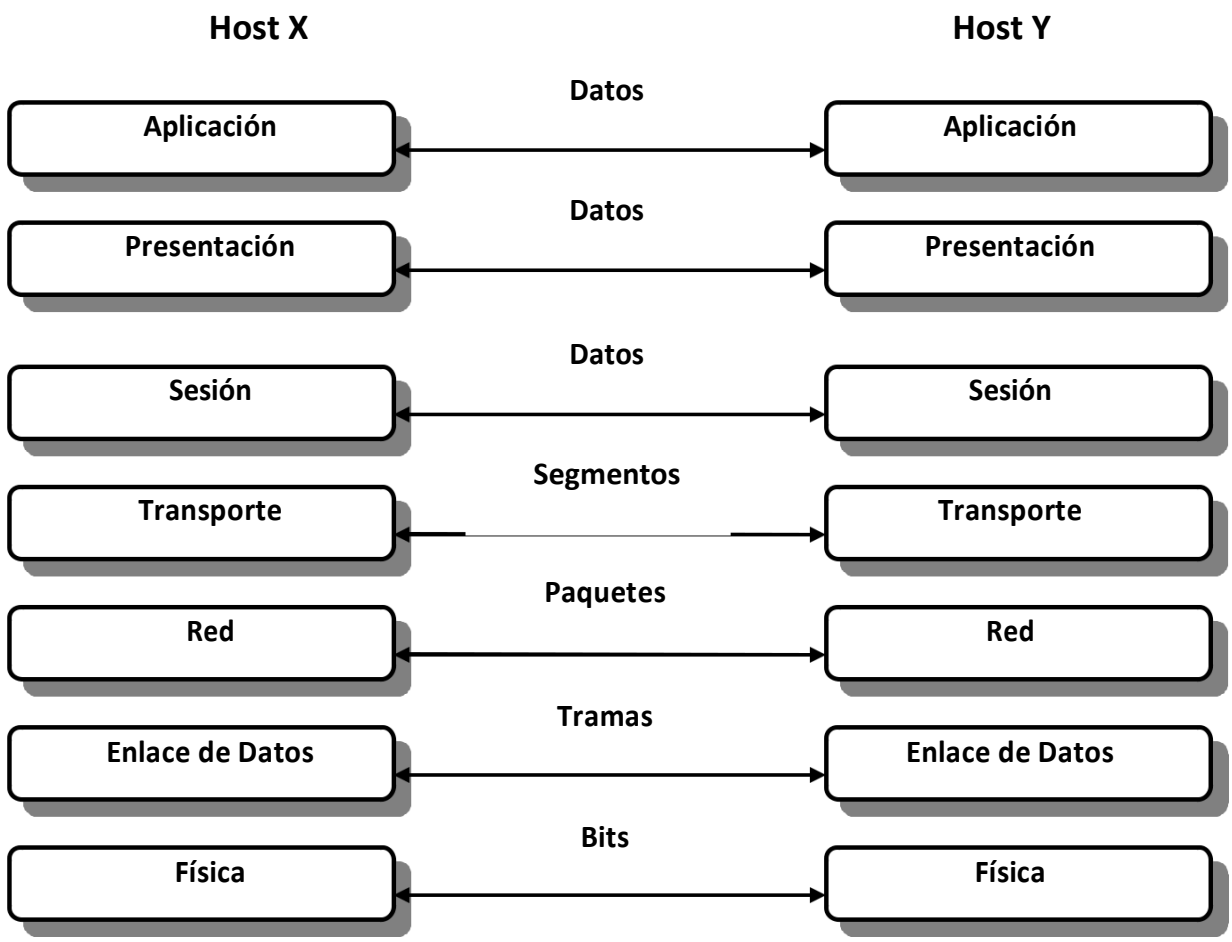


Fig. 4.3.1.b: Nombre del conjunto de bits a transmitir, según cada capa.

El modelo de referencia **OSI** describe la forma en que la información o los datos recorren el camino que va desde los programas de aplicación pasando por un medio de red hasta llegar a un programa de aplicación ubicado en otra computadora de la red.

La función de cada capa se muestra en la siguiente tabla:

N°	Capa	Función de la capa	Características	Palabra clave	Conjunto de bits
7	**Aplicación** **Dispositivo: Gateway**	¿Que desea hacer?	Es la capa más cercana al usuario. Proporciona servicio a las aplicaciones externas al modelo.	Navegadores	Datos
6	**Presentación**	¿Como me entenderá el otro proceso?	Garantiza el entendimiento entre las capas de aplicación de los distintos sistemas.	Formato de datos	Datos
5	**Sesión**	¿Quién y como establece la comunicación ?	Establece, gestiona y termina las sesiones entre los hosts.	Dialogo y conversaciones	Datos
4	**Transporte**	¿Dónde está el otro proceso?	Segmenta los datos en el emisor y los reordena en el receptor.	Control y confiabilidad	Segmento
3	**Red** **Dispositivo: Router**	¿Por qué ruta se llega?	Establece la ruta que deben seguir los paquetes, los encamina de la forma más eficiente.	Selección de la ruta	Paquetes
2	**Enlace de datos** **Dispositivo: Switch y Bridge**	¿Cómo ir a través de esa ruta?	Gestiona el enlace entre el emisor y el receptor.	Acceso a los medios	Trama (Frame)
1	**Física** **Dispositivo: Hub**	¿Cómo se puede conectar el medio físico?	Conecta a la computadora con el medio físico.	Señales y medios	Bits

Tabla 4.3.1.a: Función de cada capa del modelo OSI.

4.4 Protocolos de Enlace de Comunicaciones

Se denomina ***protocolo de enlace de comunicaciones*** al conjunto de especificaciones técnicas que definen las condiciones físicas y los procedimientos lógicos que deben cumplirse para lograr la transferencia de datos extremo a extremo de una red de comunicaciones.

Este conjunto de reglas que constituye un protocolo está destinado especialmente a normalizar las interfaces entre el equipo terminal de datos y la red a la cual éste se encuentra conectado.

Dos equipos determinados están asociados mediante una **interfaz** que incluye elementos físicos concretos que permiten la interconexión entre ellos.

Definición de interfaz (desde el punto de vista teleinformático):

Conjunto de normas y procedimientos que permiten la interconexión de dos equipos que realizan funciones diferentes.

Los objetivos más importantes que cumplen los protocolos son:

- Utilizar con la mayor eficiencia posible el canal de comunicaciones.

- Asegurar la secuencia correcta e integridad de los datos.

Principales acciones que llevan a cabo los protocolos

- Control del flujo de datos hacia la estación receptora, a efectos de no saturarla con un volumen de información superior al que puede manejar.
- Control de la actividad en el canal de comunicaciones.
- Garantizar que los bloques de datos lleguen a su destino libre de errores, sin pérdidas u omisiones y sin duplicaciones indeseadas.
- Encaminar los datos hacia la estación destinataria.
- Informar a las estaciones involucradas en la transmisión de datos el estado operativo de cada una de ellas y de las líneas, de forma que las mismas sepan cuales están activas y cuáles no.

4.4.1 Protocolos Orientados a la Conexión y No Orientados a la Conexión

En un **protocolo orientado a la conexión** absolutamente todos los paquetes que se transmiten entre los dos nodos pasan por la misma ruta durante todo el tiempo que dura la conexión. Ej. **TCP** (Protocolo de Control de Transmisión) aplicado en la Capa de Transporte.

Por el contrario en un **protocolo no orientado a la conexión** se establece las normas para que los paquetes alcancen su destino, lo que no se garantiza es cuándo lo van a alcanzar, o en qué orden. Ej. **IP** (Internet Protocol) encargado del direccionamiento de paquetes aplicado en la Capa de Red.

Finalmente el protocolo que principalmente se identifica con Internet es el **TCP/IP.**

4.5 Protocolo TCP/IP

TCP / IP son las siglas de "*Transfer Control Protocol / Interconection Protocol*". Éste es el lenguaje establecido para la Red Internet, por lo que **IP** también se lo denomina *Internet Protocol*. Las aplicaciones que corren sobre **TCP/IP** no tienen que conocer las características físicas de la red en la que se encuentran, con esto, se evita el tener que modificarlas o reconstruirlas para cada tipo de red. Esta familia de protocolos genera un modelo llamado **INTERNET** cuya correspondencia con el modelo **OSI** queda reflejada en la siguiente:

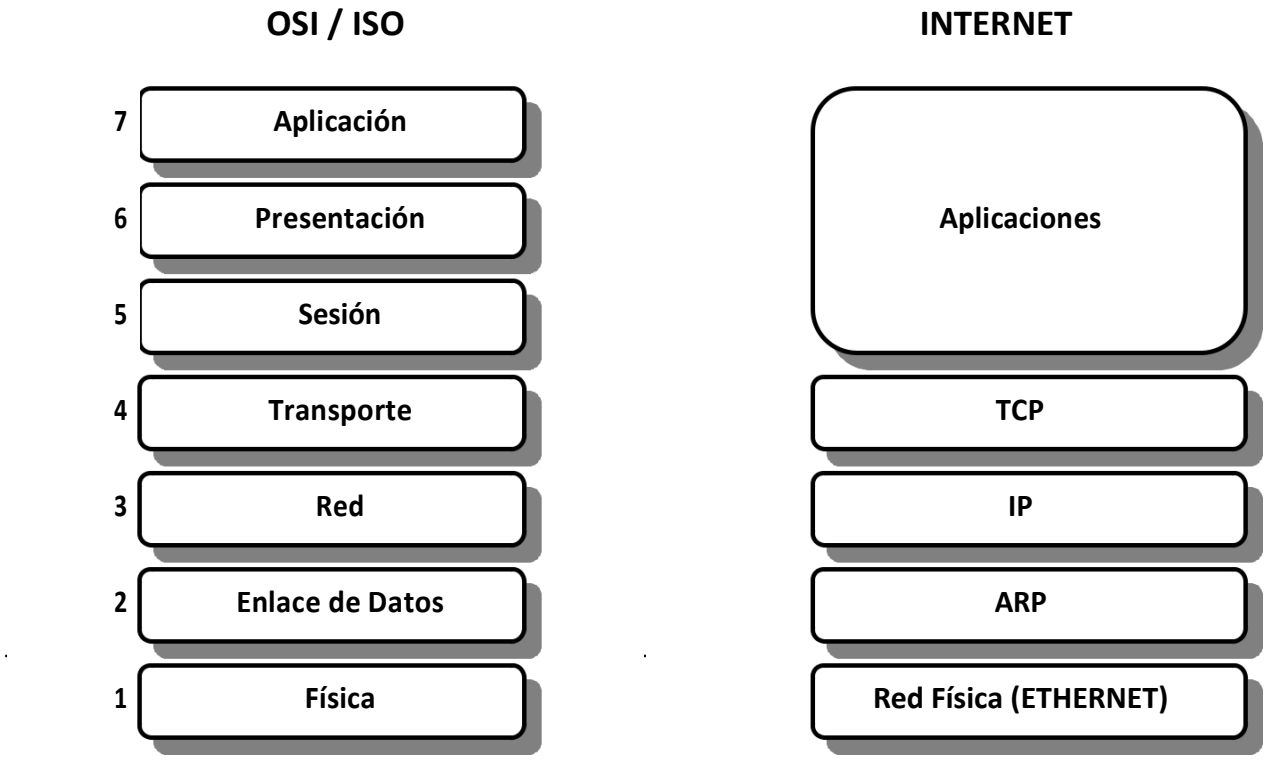


Fig. 4.5.a: Correspondencia entre el modelo OSI y el modelo INTERNET.

- ***Protocolo IP***

Se trata de un protocolo a nivel de red cuyas principales características son:

- **Ofrece un servicio no orientado a la conexión**, esto significa que cada trama en la que ha sido dividido un paquete es tratado en forma independiente. Las tramas que componen un paquete pueden ser enviadas por caminos distintos e incluso llegar desordenados.
- **Ofrece un servicio no muy fiable porque a veces los paquetes se pierden**, duplican o estropean y este nivel no informa de ello pues no es consciente del problema.

- ***Protocolo TCP***

Sus principales características son:

- **Se trata de un protocolo orientado a la conexión y al flujo**: el servicio TCP envía al receptor los datos en el mismo orden que fueron enviados.
- **Conexión con circuito virtual**: no existe conexión física dedicada, sin embargo, el protocolo hace creer al programa de aplicación que sí existe esta conexión dedicada.

- ***Características de TCP/IP***

- Provee conectividad de extremo a extremo especificando cómo los datos deberían ser formateados, direccionados, transmitidos, enrutados y recibidos por el destinatario.
- Proporciona una conexión fiable entre dos máquinas en cualquier punto de la red.
- Ofrece la posibilidad de interconectar redes de diferentes arquitecturas y con diferentes sistemas operativos.

- ***Funcionamiento de TCP/IP***

Una red que basa su funcionamiento en TCP/IP transfiere datos mediante el ensamblaje de bloques de datos en paquetes conteniendo:

- La información a transmitir.
- La dirección IP del destinatario.
- La dirección IP del remitente.
- Otros datos de control.

4.5.1 Direcciones IP .Clasificación de direcciones IP.

Se llama **dirección IP** a un número de 32 bits que representa de forma unívoca a un host en la red. Generalmente se utiliza el formato de 4 números enteros separados por puntos (192.128.160.45). Una dirección IP consta de dos partes bien diferenciadas:

a) Una parte que identifica la dirección de la red (NET ID). Esta parte es asignada por el NIC (Network Information Center). Si la red es local, no va a conectarse con otras redes, no es necesario solicitar a ese organismo una dirección. El número de bits que ocupa esta parte depende del tamaño de la red y puede ser de 8,16 o 24 bits.

b) Una parte que identifica **la dirección de la máquina dentro de la red** (*HOST ID*). Las direcciones de los host son asignadas por el administrador de la red.

Los 32 bits se agrupan en 4 bytes de 8 bits cada uno. Con 8 bits, en decimal el número máximo representable es 255, por lo que una dirección se representa entonces por cuatro valores decimales entre 0 y 255, separados por puntos, siendo cada uno un byte:

(0…255) . (0…255) . (0...255) . (0...255)

Así, por ejemplo, una dirección **IP** podría ser: 155.210.13.45

En binario: **10011011. 11010010.00001101.00101101**
En decimal: **155. 210. 13. 45**

No está permitido que coexistan **en una misma Red dos dispositivos distintos con la misma dirección**, puesto que de ser así, la información solicitada por uno de ellos no sabría a cuál dirigirse.

Existen direcciones **IP Dinámicas** y Direcciones **IP Estáticas** (también llamadas direcciones IP fijas). Si en una red se utilizan direcciones IP dinámicas, cada vez que un dispositivo (por ejemplo una PC) se conecte a la red se le asignará una dirección IP diferente. Para realizar dicha asignación existe un protocolo llamado **DHCP** (Dynamic Host Configuration Protocol).

En cambio, las direcciones IP estáticas no cambian con el tiempo. Una dirección IP estática es asignada por el administrador de la red en forma manual. Los servidores de correo, DNS, FTP públicos, y servidores de páginas Web necesariamente deben contar con una dirección IP fija o estática, ya que de esta forma se permite su localización en la red.

Las direcciones IP también pueden clasificarse en **Públicas** y **Privadas**. Esta clasificación se realiza en referencia a quién las administra y el ámbito en el cuál se las utiliza. Las direcciones IP **privadas** pueden utilizarse cuando se requiera comunicarse con otras terminales dentro de la red interna, pero no con Internet directamente. Las direcciones **privadas** son comunes en esquemas de redes de área local (LAN) y es el administrador de la red quién se encarga de su asignación.

Si un dispositivo de una red privada necesita comunicarse con otro dispositivo de otra red privada distinta, es necesario que cada red cuente con una "puerta de enlace o Gateway" con una dirección IP pública, de manera de que pueda ser alcanzada desde afuera de la red y así se pueda establecer una comunicación. Distintas compañías pueden usar el mismo rango de direcciones privadas sin riesgo de que se generen conflictos con ellas, es decir, no se corre el riesgo de que una comunicación le llegue por error a un tercero que esté usando la misma dirección IP.

Una IP **Publica** se utiliza generalmente para montar servidores en Internet y necesariamente se desea que la IP no cambie por eso siempre la IP Publica se la configura de manera Fija y no Dinámica, aunque se podría hacerlo. Por el contrario, una IP Privada generalmente es dinámica y asignada por un servidor DHCP, pero en algunos casos se configura IP Privada Fija para poder controlar el acceso a Internet o a la red local, otorgando ciertos privilegios dependiendo del número de IP que tenemos.

- ***Clases de redes***

El tipo de red, depende entre otras cosas, del número de máquinas que forman la red; atendiendo esto se pueden distinguir tres clases de redes:

- ***Redes Clase A***

En una dirección IP de clase A, el primer byte representa la red.

El bit de mayor peso (el primer bit a la izquierda) está en cero, lo que significa que hay 2^7 (00000001 a 01111111) posibilidades de **red**, que son 128 posibilidades. Sin embargo, la red 0 (bits con valores 00000000) no se utiliza y **el número 127 está reservado para referenciar al propio equipo**.

Las redes disponibles de clase A son, por lo tanto, redes que van desde **1.0.0.0** a **126.0.0.0** (los últimos bytes en ceros indican que se trata seguramente de una dirección de red y no de equipos dentro de ella).

Los tres bytes de la derecha representan los equipos dentro de la red (HOSTS). Por lo tanto, la red puede contener una cantidad de **equipos** igual a: 2^{24}-**2** = 16.777.214 equipos.

NOTA: al número posible de host 2^{24} se le resta dos porque la primer dirección se utiliza para identificar a la red y la última para realizar Broadcast (mensajes de difusión a los dispositivos de la red).

El byte de red debe ser un número, en decimal, entre 1 a 126. El formato de direcciones es:

Identificador de red:	**Identificador de hosts:**
0_ _ _ _ _ _ _	_ _ _ _ _ _ _ _ . _ _ _ _ _ _ _ _ . _ _ _ _ _ _ _ _

4.5.1.a: Direccionamiento Clase A

Clase A	***RED***	***HOST***		
	Byte 1	***Byte 2***	***Byte 3***	***Byte 4***
Ejemplo	***7***	***125***	***67***	***244***
En binario	***00000111***	***01111101***	***01000011***	***11110101***

✓ ***Redes Clase B***

En una dirección IP de clase B, los primeros dos bytes identifican la red.

Los primeros dos bits son 1 y 0; esto significa que existen 2^{14} (**10**000000 00000000 a **10**111111 11111111) posibilidades de red, es decir, 16.384 redes posibles. Las redes disponibles de la clase B son, por lo tanto, redes que van de **128.0.0.0** a **191.255.0.0**.

Los dos bytes de la derecha representan los equipos de la red. Por lo tanto, la red puede contener una cantidad de equipos igual a: 2^{16}-**2** = 65.534 equipos. La Tabla 7 muestra un ejemplo de dirección Clase B.

El primer byte de red debe ser un número, en decimal, entre 128 y 191. El formato de direcciones es:

Identificador de red:	**Identificador de hosts:**
10 _ _ _ _ _ _ . _ _ _ _ _ _ _ _ .	_ _ _ _ _ _ _ _ . _ _ _ _ _ _ _ _

4.5.1.b: Direccionamiento Clase B

Clase B	**RED**		**HOST**	
	Byte 1	**Byte 2**	**Byte 3**	**Byte 4**
Ejemplo	**135**	**125**	**67**	**244**
En binario	**10000111**	**01111101**	**01000011**	**11110101**

✓ ***Redes Clase C***

En una dirección IP de clase C, los primeros tres bytes representan la red. Los primeros tres bits son 1,1 y 0; esto significa que hay 2^{21} posibilidades de red, es decir, 2.097.152.

Las redes disponibles de la clases C son, por lo tanto, redes que van desde **192.0.0.0** a **223.255.255.0**.

El byte de la derecha representa los equipos de la red, por lo que la red puede contener: 2^8-2 = 254 equipos.

El primer byte de red debe ser un número, en decimal, entre 192 y 223. El formato de direcciones es:

Identificador de red:	**Identificador de host:**
110 _ _ _ _ _ . _ _ _ _ _ _ _ _ . _ _ _ _ _ _ _ _	_ _ _ _ _ _ _ _

4.5.1.c: Direccionamiento Clase C

Clase C	**RED**			**HOST**
	Byte 1	**Byte 2**	**Byte 3**	**Byte 4**
Ejemplo	**195**	**125**	**67**	**244**
En binario	**11000011**	**01111101**	**01000011**	**11110101**

En la siguiente tabla se muestra los rangos de direcciones de cada clase:

Tabla 4.5.1.d: Rangos de cada clase

	Byte 1	**Byte 2**	**Byte 3**	**Byte 4**
Clase A	1…126	0…255	0…255	0…255
Clase B	128...191	0...255	0....255	0...255
Clase C	192…223	0...255	0....255	0...255

Existen más tipos redes, como la D, E y F cuyo rango de direcciones oscila entre 224.0.0.0 y 254.0.0.0; este tipo de redes son experimentales o se reservan para uso futuro.

4.5.2 Máscaras y Subnetting

Máscaras de subred:

Anteriormente se definió que una dirección IP está compuesta por números que identifican la red y números que identifican los host que pertenecen a esa red. La **máscara de red** se utiliza expresamente para determinar la red asociada con cada dirección. Si bien mantiene el formato de una dirección IP, está compuesta en su notación binaria por **unos** en lugar de los bits **destinados a la red** y por **ceros** en el lugar de los **bits destinada a los host**.

La ***máscara de subred*** muestra la **red** y oculta el **host**.

Una máscara de red me permite:

a) Determinar, de una dirección IP, cuales son los bits que identifican la red y cuáles son los que identifican el host.

Tanto los bits de red (unos) como los de host (ceros), en una máscara de red deben ser **CONSECUTIVOS Y ADYACENTES**. Los bits que identifican a la red comienzan siempre del lado izquierdo de la máscara.

Ejemplos de Máscaras en cada Clase de Dirección IP:

- ***Clase A***

En toda dirección IP de una red clase A, el primer byte identifica la red y los otros tres a los host.

La **máscara** de una dirección IP clase A entonces será:

En binario: 11111111.00000000.00000000.00000000
En decimal: **255 . 0 . 0 . 0**

- ***Clase B***

En toda dirección IP de una red clase B, los primeros dos bytes identifican la red y los otros dos a los host.

La máscara de una dirección IP clase B entonces será:

En binario: 11111111.11111111.00000000.00000000
En decimal: **255 . 255 . 0 . 0**

- ***Clase C***

En toda dirección IP de una red clase C, los primeros tres bytes identifican la red y el otro a los host.

La máscara de una dirección IP clase C entonces será:

En binario: 11111111.11111111.11111111.00000000
En decimal: **255 . 255 . 255 . 0**

Estas tres máscaras son llamadas habitualmente máscaras por defecto.

b) Dada la dirección IP de un host, la máscara de red permite determinar a qué red pertenece el mismo.

Para esto debo realizar un **Y lógico (producto lógico) entre la dirección IP y la máscara.**

Se recuerda que a . 1 = a y a . 0 = 0, es decir, la máscara "deja ver" aquellos bits de la dirección IP donde la máscara tiene bits en 1 y "oculta" aquellos donde la máscara tiene bits en 0.

Ejemplo:

Dada la siguiente dirección IP clase B: 145.54.95.18
Máscara: 255.255.0.0

Determinar a qué **red** pertenece el host.

Solución: Realizar un producto lógico entre la dirección IP y la máscara.

Producto lógico: Se multiplica, por byte, cada bit de la IP con el correspondiente bit del mismo peso de la máscara, como se puede apreciar en la Tabla 10:

Tabla 4.5.2.a: Producto lógico entre dirección IP y máscara

	Decimal	Binario			
IP	145.54.95.18	1 0 0 1 0 0 0 1	0 0 1 1 0 1 1 0	0 1 0 1 1 1 1 1	0 0 0 1 0 0 1 0
Máscara	255.255. 0 .0	1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0
Red	*Producto lógico*	1 0 0 1 0 0 0 1	0 0 1 1 0 1 1 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0
Red		145	54	0	0

Respuesta: el host con IP 145.54.95.18 y máscara 255.255.0.0 pertenece a la red 145.54.0.0

NOTA: si bien esto se podría haber determinado únicamente analizando la máscara, debido a que la misma tiene en uno los bits de red y en cero los de host; la explicación de la resolución por medio del ***and*** lógico nos será útil para comprender el cálculo de redes a partir de un host cuando utilice subnetting (subred).

Subnetting

Se utiliza este procedimiento, para armar subredes a partir de una red. Por ejemplo, en el caso que a una organización le asignen una única dirección IP pública, y se necesita armar más de una subred interna.

Para esto lo que se hace es **"tomar" algunos bits de la parte de host** y utilizarlos para armar las subredes.

1) ¿Cómo nos damos cuenta que se utilizó subnetting?

Si NO se utilizó subnetting las máscaras de red son únicamente las **máscaras por defecto**:

Clase A: 255.0.0.0; Clase B: 255.255.0.0; Clase C: 255.255.255.0

En estos casos, al hacer el producto lógico entre una dirección IP y su máscara, obtendré siempre la dirección de una red en la clase correspondiente (podemos verificar esto observando el rango del primer byte de la dirección de la red obtenida).

Por otro lado, en la máscara de red por defecto los números en decimal son únicamente 0 o 255.

Si se utilizó subnetting, en la máscara de red aparecerá un número en decimal DISTINTO de 0 y 255.

Ejemplos de máscaras de redes a las que se le aplicó subnetting:

Clase A: 255.**240**.0.0; Clase B:255.255.**192**.0; Clase C: 255.255.255.**224**

2) ¿Cuántas subredes se pueden armar?

Esto depende de la cantidad de bits de host que "tome" para armar las subredes. La siguiente fórmula permite calcular la cantidad de subredes:

$$N = 2^n$$

Donde:

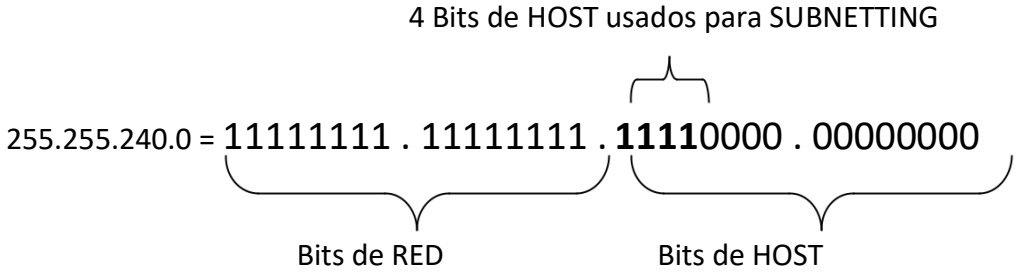
N= Cantidad de subredes que puedo armar
n= Cantidad de bits de host que utilizo para armar las subredes.

Ejemplo: Dada la dirección IP de una **red clase B**: 145.54.0.0 su máscara por defecto es: 255.255.0.0

Si decimos que su máscara de **subred** será: 255.255.**240**.0 (El 3º byte es distinto de 0 y 255)

a) ¿Cuántas subredes puedo armar? b) ¿Cuáles son esas subredes?

a) Pasando la máscara a binario nos queda:



Podemos ver que se toman 4 bits de host para armar subredes, por lo tanto **se pueden armar entonces 16 subredes pues: $2^4 = 16$.**

b) Para saber cuáles son las subredes que se pueden armar, se deben escribir todas las **posibles combinaciones** en binario con 4 bits (0000 ; 0001; 0010, etc.) en el byte en el que se tomaron esos 4 bits (en este caso en el 3º byte), siempre recordando que los bits de red deben ser CONSECUTIVOS y ADYACENTES (si tome cuatro bits, las 16 posibles combinaciones se arman con los cuatro bits de la izquierda del byte, los restantes serán cero), como muestra en la tabla:

Tabla 4.5.2.b: Las 16 combinaciones posibles al aplicar la máscara al 3º byte.

Bits de Subred	En decimal
0000 0000	0
0001 0000	16
0010 0000	32
0011 0000	48
0100 0000	64
0101 0000	80
0110 0000	96
0111 0000	112
1000 0000	128
1001 0000	144
1010 0000	160
1011 0000	176
1100 0000	192
1101 0000	208
1110 0000	224
1111 0000	240

A continuación, se arman las direcciones IP completas. Los bits de red por defecto de una IP clase B son 16; si se le suman los cuatro que se tomaron para armar subredes se tendrán en total 20 bits para la red. La siguiente tabla muestra la dirección IP de cada una de las 16 subredes:

Tabla 4.5.2.c: Dirección IP de cada subred obtenida al aplicar la máscara.

Bits con la máscara en 1			Bits con la máscara en 0		IP resultante en decimal
10 0 1 0 0 0 1	0 0 1 1 0 1 1 0	0 0 0 0	0 0 0 0	0 0 0 0 0 0 0 0	145.54.0.0
10 0 1 0 0 0 1	0 0 1 1 0 1 1 0	0 0 0 1	0 0 0 0	0 0 0 0 0 0 0 0	145.54.16.0
10 0 1 0 0 0 1	0 0 1 1 0 1 1 0	0 0 1 0	0 0 0 0	0 0 0 0 0 0 0 0	145.54.32.0
10 0 1 0 0 0 1	0 0 1 1 0 1 1 0	0 0 1 1	0 0 0 0	0 0 0 0 0 0 0 0	145.54.48.0
10 0 1 0 0 0 1	0 0 1 1 0 1 1 0	0 1 0 0	0 0 0 0	0 0 0 0 0 0 0 0	145.54.64.0
10 0 1 0 0 0 1	0 0 1 1 0 1 1 0	0 1 0 1	0 0 0 0	0 0 0 0 0 0 0 0	145.54.80.0
10 0 1 0 0 0 1	0 0 1 1 0 1 1 0	0 1 1 0	0 0 0 0	0 0 0 0 0 0 0 0	145.54.96.0
10 0 1 0 0 0 1	0 0 1 1 0 1 1 0	0 1 1 1	0 0 0 0	0 0 0 0 0 0 0 0	145.54.112.0
10 0 1 0 0 0 1	0 0 1 1 0 1 1 0	1 0 0 0	0 0 0 0	0 0 0 0 0 0 0 0	145.54.128.0
10 0 1 0 0 0 1	0 0 1 1 0 1 1 0	1 0 0 1	0 0 0 0	0 0 0 0 0 0 0 0	145.54.144.0
10 0 1 0 0 0 1	0 0 1 1 0 1 1 0	1 0 1 0	0 0 0 0	0 0 0 0 0 0 0 0	145.54.160.0
10 0 1 0 0 0 1	0 0 1 1 0 1 1 0	1 0 1 1	0 0 0 0	0 0 0 0 0 0 0 0	145.54.176.0
10 0 1 0 0 0 1	0 0 1 1 0 1 1 0	1 1 0 0	0 0 0 0	0 0 0 0 0 0 0 0	145.54.192.0
10 0 1 0 0 0 1	0 0 1 1 0 1 1 0	1 1 0 1	0 0 0 0	0 0 0 0 0 0 0 0	145.54.208.0
10 0 1 0 0 0 1	0 0 1 1 0 1 1 0	1 1 1 0	0 0 0 0	0 0 0 0 0 0 0 0	145.54.224.0
10 0 1 0 0 0 1	0 0 1 1 0 1 1 0	1 1 1 1	0 0 0 0	0 0 0 0 0 0 0 0	145.54.240.0

3) Dada una dirección IP de un host, ¿Cómo se determina a que red (o subred) pertenece?

Para saber a qué red pertenece un host debo realizar un **producto lógico** entre la dirección IP del host y la máscara.

Ejemplo: Dada la siguiente dirección IP clase B: 145.54.95.18
Máscara: 255.255.240.0

Determinar a qué subred pertenece el host.

Tabla 4.5.2.d: Determinación de la subred a la cual pertenece un host

	Decimal	Binario			
IP	145.54.95.18	1 0 0 1 0 0 0 1	0 0 1 1 0 1 1 0	0 1 0 1 1 1 1 1	0 0 0 1 0 0 1 0
Máscara	255.255. 240 .0	1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	1 1 1 1 0 0 0 0	0 0 0 0 0 0 0 0
Red	*Y (and) lógico*	1 0 0 1 0 0 0 1	0 0 1 1 0 1 1 0	0 1 0 1 0 0 0 0	0 0 0 0 0 0 0 0
Red		145	54	80	0

Respuesta:

El host con IP 145.54.95.18 y máscara 255.255.240.0 pertenece a la subred 145.54.80.0

4) ¿Cuántos bits se utilizan para indicar la red?

Los que son 1 (CONSECUTIVOS Y ADYACENTES) en la máscara de red, por lo tanto se utilizan 20 bits para la red.

NOTA: Otra nomenclatura comúnmente utilizada para indicar que se utilizan 20 bits paraindicar la red es al lado de la dirección IP escribir: ***/ la cantidad de bits para indicar la red.***

Ejemplo: IP 145.54.95.18 ***/ 20***

5) ¿Cuál es el rango de host de la red recién calculada? (145.54.80.0)

Necesitamos para ello saber cuál es el primer host de la red y cual el último.

a) Primer host de la red: 145.54.80.1
b) Ultimo host de la red: 145.54.95.254

Un método fácil para hallar el último host de la red es:

- ✓ Calcular primero la siguiente subred.
- ✓ Un host anterior sería el último de la red en la que estoy determinando el rango; como esta dirección se encuentra reservada para broadcast (difusión) "resto" otro host.

***Calcular la siguiente subred*:**

Si tenemos la tabla armada, sólo debo buscar la siguiente subred.

Otra forma de calcularla es: En la IP de red antes calculada (145.54.80.0); sumo 1 al último bit tomado para armar las subredes (los que están en gris) notar que este es el último bit de red.

Tabla 4.5.2.e: Cálculo de la siguiente subred.

Máscara	**255.255.240.0**	**1 1 1 1 1 1 1 1**	**1 1 1 1 1 1 1 1**	**1 1 1 1**	**0 0 0 0**	**0**
Red	**145.54.80.0**	**1 0 0 1 0 0 0 1**	**0 0 1 1 0 1 1 0**	**0 1 0 1**	**0 0 0 0**	**0**
Sumo 1 al último bit de red				**1**		
Siguiente subred		**1 0 0 1 0 0 0 1**	**0 0 1 1 0 1 1 0**	**0 1 1 0**	**0 0 0 0**	**0**
		145	**54**	**96**		0

Un host anterior sería: 145.54.95.255

(Esta es la dirección reservada para Broadcast)

Ultimo host de la red: 145.54.95.254

Respuesta: el rango de host de la red 145.54.80.0 va **desde el host 145.54.80.1 hasta el host 145.54.95.254**

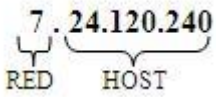
6) ¿Cuál es la dirección de Broadcast de la red antes calculada? (145.54.80.0)

La dirección de broadcast de la red es 145.54.95.255

4.6 Convención de Direcciones Especiales

Existen algunas direcciones (combinaciones de unos y ceros) que no se asignan como direcciones IP, sino que tienen un significado especial. Estas combinaciones son las que muestra la siguiente tabla.

Como ejemplo utilizaremos la dirección IP de una red clase A :



4.7 Nombres de Dominio

Cuando una organización decide tener presencia en la WWW (World Wide Web), debe crear un Sitio Web y reservar ante NIC (Network Information Center) un **nombre de dominio** a través del cual será reconocido en Internet y al que se le asignará una dirección IP. El sistema de nombres de dominio (DNS) ayuda a los usuarios a navegar en Internet. Como las direcciones IP (compuestas por una cadena de números) son difíciles de recordar, el protocolo DNS permite usar una cadena de letras. Por ejemplo, en el caso de la Universidad Nacional de la Matanza, el nombre de dominio es www.unlam.edu.ar y la Dirección IP asociada es 200.47.130.101.

Tabla 4.6.a: Direcciones especiales:

NOMBRE	ACCIÓN	GRAL	EJEMPLO
DIFUSIÓN DIRIGIDA BROADCAST	PERMITE DIRECCIONAR A TODOS LOS HOST DENTRO DE LA RED ESPECIFICADA	DIRECCIÓN DE RED. TODOS UNOS	7 . 255. 255. 255 00000111.11111111.1111111.1111111
LOOPBACK	SE UTILIZA PARA REALIZAR PRUEBAS DENTRO DE UN MISMO HOST (NO SALE POR PLACA DE RED)	127. CUALQUIER COMBINACIÓN (NORMALMENTE CERO.CERO.UNO)	127. 0. 0. 1 01111111.00000000.00000000.00000001
DIRECCIONA A HOST INTERNO	PERMITE DIRECCIONAR A UN HOST INTERNO DE LA RED	CERO. DIR DE HOST	0. 24. 120. 240 00000000. 00011000.0111100.11110000
DIFUSIÓN LIMITADA	DIRECCIONA A LOS HOST DE LA PROPIA RED	TODOS UNOS	255. 255. 255. 255 11111111.11111111.1111111.1111111
DIRECCIONA AL PROPIO HOST	PERMITE DIRECCIONAR AL PROPIO HOST	TODOS CEROS	0. 0. 0. 0 00000000. 00000000. 00000000. 00000000

La dirección 0.0.0.0 significa "este dispositivo" y solamente se utiliza cuando se está iniciando el sistema y no se conoce todavía la dirección asignada al dispositivo. No está permitido su uso como dirección de destino. En cambio, la dirección 127.0.0.1, que también significa "este mismo dispositivo", sí se puede usar como dirección de destino y el efecto es que los mensajes que se le envíen "rebotan" y vuelven a ser recibidos por el mismo dispositivo. Esto es muy útil para propósitos de pruebas.

Se aclara también que las direcciones de red que comienzan en 10 y en 192 se utilizan para las direcciones IP de redes privadas.

4.7. IPv6 - Un nuevo protocolo de Comunicaciones

El motivo básico por el que surge, en el seno del **IETF** (*Internet Engineering Task Force*), la necesidad de crear un nuevo protocolo, que en un primer momento se denominó **IPng** (*Internet Protocol Next Generation*, o "*Siguiente Generación del Protocolo Internet*"), fue la evidencia de la falta de direcciones.

Una dirección IPv4 está formada por 32 bits. La cantidad total de direcciones IPv4 es:

$$2^{32} = 4.294.967.296$$

Una dirección IPv6 está formada por 128 bits. La cantidad total de direcciones IPv6 es:

$$2^{128} = 340.282.366.920.938.463.463.374.607.431.768.211.456$$

Que constituyen $7{,}9 \times 10^{28}$ de direcciones (en total) más que en IPv4.

Permitiendo tener aproximadamente $5{,}6 \times 10^{28}$ direcciones IP por cada ser humano.

Direccionamiento

La representación de las direcciones **IPv6 divide la dirección en ocho grupos de 16 bits**, separados mediante "**:**", representados con dígitos hexadecimales.

Ejemplo:

2001:0DB9:AD3F:24E7:CADE:CAFE:F0CC:64C5

En la representación de una dirección IPv6 está permitido:

- Utilizar caracteres en mayúscula o minúscula.
- Omitir los ceros a la izquierda.
- Representar los ceros continuos mediante "::"

  Ejemplo: 2001:0DB8:0000:0000:130F:0000:0000:140B

  Puede escribirse como: 2001:db8:0:0:130f::140b

  Formato no válido: 2001:db8::130f::140b (genera ambigüedad)

Sin embargo, **IPv4** tiene otros problemas o "dificultades" que **IPv6** soluciona o mejora. Los creadores de **IPv4**, a principio de los años 70, no predijeron en ningún momento, el gran éxito que este protocolo iba a tener en muy poco tiempo, en una gran multitud de campos, no sólo científicos y de educación, sino también en innumerables facetas de la vida cotidiana.

Podemos recordar algunas "famosas frases" para entender hasta que punto, los propios precursores' de la revolución tecnológica que estamos viviendo, no llegaron a prever:

- "Pienso que el mercado mundial de ordenadores puede ser de cinco dígitos", (es decir, hasta 99.999 computadoras).
  Thomas Watson, Presidente de IBM en 1943.
- "64 KBytes de memoria (RAM) han de ser suficientes para cualquier usuario", Bill Gates, Presidente de Microsoft, 1981.
- "IPv4 proporciona un espacio de direccionamiento suficiente para Internet", Dr. Vinton Cerf, padre de Internet, 1977.

No es que estuvieran equivocados, sino que las Tecnologías de la Información han evolucionado de un modo mucho más explosivo de lo esperado. Además, recordemos: "es de sabios rectificar".

Algunas características fundamentales de IPv6 son las siguientes:

- Mayor espacio de direcciones.
- "**Plug & Play**": Autoconfiguración.
- Calidad de Servicio (**QoS**).
- **Multicast**: Envío de UN mismo paquete a un grupo de receptores.
- **Anycast**: Envío de UN paquete a UN receptor dentro de UN grupo.
- Posibilidad de paquetes con carga útil (datos) de más de 65.535 bytes.
- Precisamente, la **escalabilidad** es la baza más importante de **IPv6** frente a **IPv4**.

Capítulo V: Internet – Internet de las cosas - Cyberseguridad

5.1 Internet

5.1.1 Introducción

Algunos definen **Internet** como "*La Red de Redes*", y otros como "*La Autopista de la Información*".

Efectivamente, **Internet** es una Red de Redes porque está hecha a base de unir muchas redes de dispositivos informáticos. Hace unos años la gran mayoría de estos dispositivos informáticos eran computadoras, hoy otros dispositivos como televisores, teléfonos, tablets, consolas de juegos, smartphones, cámaras, GPS, dispositivos de seguridad y electrodomésticos, entre otros, se conectan a internet. Además, ésta es "La Red de Redes" porque es la más grande. Prácticamente todos los países del mundo tienen acceso a Internet.

Por la Red **Internet** circulan constantemente cantidades increíbles de información. Por este motivo se le llama también "La Autopista de la Información". Se dice "*navegar*" porque es normal ver información que proviene de muchas partes distintas del mundo en una sola sesión. Desde un punto de vista más amplio, **Internet** constituye un fenómeno sociocultural y comunicacional de gran importancia, una nueva manera de entender las comunicaciones que está transformando el mundo: millones de individuos acceden a la mayor fuente de información que jamás haya existido y provocan un inmenso y continuo intercambio de conocimiento entre ellos. **Internet** es una herramienta de trabajo, un periódico global, un buzón de correos, una tienda de software, una biblioteca, una plaza pública, un recurso educativo, una plataforma publicitaria…

Cuatro características podrían definir las virtudes de **Internet**:

- **Grande:** La mayor red de dispositivos informáticos del mundo.
- **Cambiante:** Se adapta continuamente a las nuevas necesidades y circunstancias.
- **Diversa:** da cabida a todo tipo de equipos, fabricantes, redes, tecnologías, medios físicos de transmisión, usuarios, etc.
- **Descentralizada:** No existe un controlador oficial, está controlada por los miles de administradores de pequeñas redes que hay en todo el mundo.

Internet crece a un ritmo vertiginoso. Constantemente se mejoran los canales de comunicación con el fin de aumentar la rapidez de envío y recepción de datos. Cada día que pasa se publican en la Red miles de documentos nuevos, y se conectan por primera vez miles de personas. Con relativa frecuencia aparecen nuevas posibilidades de uso de **Internet**, y constantemente se están inventando nuevos términos para poder entenderse en este nuevo mundo que no para de crecer.

5.1.2 Organización

En **Internet** participan instituciones educativas y de investigación, organismos gubernamentales, empresas, organizaciones privadas y cada vez más empresas de todo tipo.

A través de **Internet** es posible, tanto para usuarios individuales como para las empresas, tener acceso a una serie de servicios, tales como: correo electrónico, transferencia de archivos, numerosos recursos de información, participación en grupos de interés, conversaciones interactivas, video, audio, juegos, mapas y mucho más.

En el punto más alto están las redes troncales o backbones (se usan para interconectar otras redes). Estas redes intermedias dan servicio a empresas proveedoras y éstas a usuarios finales.

Para administrar los recursos comunes se creó el **NIC** *(Network Information Center)*, que se encarga de la asignación de direcciones y del registro de nombres de dominio. Este trabajo está descentralizado por áreas geográficas:

- **Nivel mundial:** InterNIC
- **Europa:** RIPE NCC
- **España:** ESNIC (gestionado por RedIris-Artix)

Como vimos **Internet** se fue estructurando sobre la base a la denominada "*suite de protocolos*" **TCP/IP**.

Se denomina suite de protocolos al conjunto de protocolos compatibles entre sí que funcionan de manera conjunta para brindar distintos niveles de servicios.

La suite de protocolos **TCP/IP** está formada entre otros por los protocolos **IP**, **TCP**, **UDP**[4], etc. Estos permitieron que se organizasen muy rápidamente distintas redes que luego se podían interconectar a través del mismo. Este estándar, inicialmente de facto, se adoptó casi universalmente. **Internet** no tiene un presidente o un director, la autoridad final descansa en una organización no gubernamental, denominada ***Internet Society***. Esta institución fue creada en 1992 y la pertenencia a ella es voluntaria. Los miembros de la Internet Society pueden ser individuos o empresas. Su conducción está a cargo de una Junta Administrativa denominada *Board of Trustees*, constituida por un Presidente, un Vicepresidente, un Director Ejecutivo. También existe un Consejo Asesor y varios comités que se dedican cada uno de ellos a actividades especiales.

5.2 Internet de las cosas (IoT)

El internet de las cosas (en inglés, Internet of Things, abreviado IoT) es un término que se utiliza para referenciar a la conexión a internet de los objetos de uso cotidiano. Note que decimos conexión de ***objetos***, no de personas. Estos objetos pueden transferir datos a la red, sin la intervención de las personas. El IoT se refiere a los miles de millones de dispositivos físicos en todo el mundo que ahora están conectados a Internet recolectando y compartiendo datos.

Internet de las cosas (IoT) es una red de objetos físicos que usa sensores y APIs (Interfaces de Programación de Aplicaciones) para conectarse e intercambiar datos por internet.

Fig 5.1.a: Internet de las cosas

[4] Protocolo no orientado a la conexión luego no proporciona ningún tipo de corrección de errores ni de flujo. Al detectar un error en un datagrama, lo descarta

Si bien es habitual que las computadoras y los teléfonos móviles se conecten a través de internet y posean de alguna forma identificadores que son únicos, la IoT se enfoca en aquellos dispositivos "cosas" cotidianos, que normalmente no se asocian con Internet, como por ejemplo: autos, electrodomésticos (heladeras, aires acondicionados, aspiradoras robot, etc), relojes inteligentes, sensores para medir niveles hídricos, o sensores para el monitoreo de cultivos en agricultura. La mayoría de los objetos físicos pueden transformarse en un dispositivo IoT si lo podemos conectar a Internet, por ejemplo, una lamparita que se puede encender usando una aplicación de celular es un dispositivo IoT. Los dispositivos pueden ser desde algo simple como esta lamparita, o complejos como un auto que se maneje sin un conductor.

Los dispositivos conectados a internet generan una cantidad enorme de datos de IoT que pueden analizarse y aprovecharse en tiempo real. Es decir que la internet de las cosas no solo se limita a la conexión de dispositivos sino que permite que estos se comuniquen e intercambien datos. Los dispositivos de IoT recopilan información y la envían a algún servidor de datos central. Allí, la información se procesa, recopila, destila y utiliza para facilitar la realización de una gran cantidad de tareas.

Los beneficios de IoT están relacionados con el bienestar de las personas, el cuidado del medio ambiente -por el uso eficiente de los recursos- y la búsqueda de eficiencias por parte de empresas y organizaciones.

5.3 Cyberseguridad

La cyberseguridad, también llamada **seguridad informática o seguridad de tecnología de la información**, son las medidas tomadas para impedir ejecuciones de acciones no autorizadas sobre un sistema o red informática. Estas medidas deben permitir identificar y eliminar vulnerabilidades en ellos.

Varias de las operaciones de las organizaciones dependen de la eficacia y eficiencia de los servicios informáticos, por lo que si ocurre un desastre informático, la continuidad será fuertemente afectada. Se podría definir desastre informático como aquello que provoca la interrupción y paralización de las actividades y/o procesos más esenciales de la Institución y que puedan afectar los servicios.

Los accesos no autorizados pueden conllevar daños sobre uno de los activos más importantes de la organización como es la información (comprometiendo su confidencialidad, autenticidad o integridad), o bien disminuir el rendimiento de los sistemas, incluso pueden bloquear el acceso de usuarios autorizados al sistema.

Con los años, las herramientas y los métodos de ataque a las redes han evolucionado. En los 80's los agresores debían tener conocimientos avanzados de informática, programación y networking para utilizar herramientas rudimentarias y realizar ataques básicos. Con el correr del tiempo, y a medida que los métodos y las herramientas de los agresores mejoraban, ya no necesitaban el mismo nivel avanzado de conocimientos. Quienes antes no hubieran cometido delitos informáticos, ahora pueden hacerlo sin necesidad de conocimientos muy avanzados. Por lo que es muy importante estar prevenidos.

Las amenazas pueden ser **internas** (se originan dentro de la red que se protege) o **externas** (se originan fuera de la red que se protege). Al analizar las amenazas internas se debe tener en cuenta que los usuarios pueden pertenecer a la misma organización, por lo tanto conocer la red y la información que se gestiona en la misma. También es muy probable que el atacante tenga un usuario con ciertos permisos en esa red. Para la protección de amenazas externas, el administrador de la red, cuenta con herramientas como los firewalls y otros sistemas de prevención de intrusos.

Dentro de los factores que pueden afectar la seguridad podemos encontrar, por ejemplo, las siguientes **amenazas a la seguridad**:

- ✓ Producidas por **usuarios de la misma red** (a quienes, por ejemplo, no se les restringieron correctamente los permisos.
- ✓ Producidas por **malware** (programas destinados a dañar recursos informáticos).
- ✓ **Vulnerabilidades no conocidas** (por ejemplo por errores en la programación o en los sistemas operativos).
- ✓ **Siniestros** (por ejemplo un incendio o una inundación).
- ✓ **Fallas en el suministro eléctrico**.
- ✓ **Desfiguración o defacement** (Es un tipo de ataque dirigido que consiste en la modificación de la página web corporativa con la intención de publicar mensajes no oficiales).
- ✓ **Ingeniería social** (Son técnicas basadas en el engaño, normalmente llevadas a cabo a través de las redes sociales. Por ejemplo, el usuario es inducido a pulsar sobre un enlace haciéndole pensar que es lo correcto).

Para poder identificar las vulnerabilidades, es indispensable realizar un análisis de los riesgos puedan llegar a afectar o interrumpir la continuidad y la disponibilidad del servicio, a fin de identificarlos en forma proactiva y no una vez que estos sucedan. Junto con este análisis se deben establecer planes de acción a ejecutar en caso de ocurrencia de alguno de ellos.
Toda organización debería elaborar una **Política de Seguridad de la Información**. La elaboración de la misma excede los conocimientos que pretenden mostrarse en este apartado. Sin embargo mencionaremos ciertas medidas que son consideradas las básicas para la protección: como por ejemplo la codificación de la información, las medidas de seguridad físicas (alarmas, alarmas de incendio, controles de acceso, cámaras, etc), las políticas de contraseñas seguras, el monitoreo de las redes, el control del software instalado, políticas de backup (respaldos de la información), los sistemas para segurización de las redes (firewall, sistemas de detección de intrusos, antispyware, antivirus), controles de acceso a los sistemas y a la información.

En resumen, **la seguridad en un ambiente de red informática es la habilidad de identificar y eliminar vulnerabilidades**. El desafío general de la seguridad es encontrar un equilibrio entre dos requisitos importantes: la necesidad de abrir redes para respaldar las oportunidades comerciales en evolución y la necesidad de protegerlas para garantizar la continuidad del negocio todo el día, los 365 días del año.

5.4 Cortafuegos (Firewalls)

Firewall es un componente o conjunto de componentes que restringen el acceso entre una red interna (intranet) protegida y cualquier otra red, generalmente Internet.

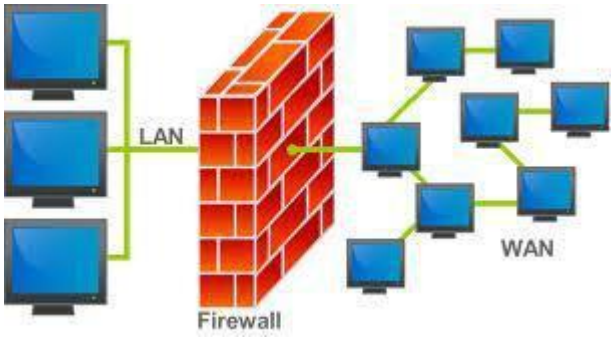


Fig. 5.4.a: Firewall

Las características de los firewalls son las siguientes:

- El firewall puede estar basado en hardware o software o en una combinación de ambos.
- El objetivo principal de un firewall es implementar una política de seguridad determinada.
- Se diseñan para bloquear los accesos no autorizados a la red. Habitualmente se utilizan para proteger los accesos a las redes LAN. Por ejemplo, se usan para que los usuarios no autorizados de internet no puedan acceder a una red privada.
- Un sistema de firewall permite de entrada establecer un primer punto fuerte de control. Es decir, se puede implantar ciertas medidas de seguridad que afecten a toda nuestra red y por lo tanto a las máquinas que la componen, pudiendo aplicar una administración única de este primer nivel de seguridad.
- Se puede distinguir fácilmente entre el interior y el exterior de la red.
- Permiten llegar donde los mecanismos de seguridad de los sistemas operativos a veces no pueden.
- Un sistema de firewall permite ofrecer y utilizar servicios de Internet de una forma más segura.

5.5 Servidor Proxy

Un **servidor "proxy"** es un programa que trabaja con servidores externos en nombre de clientes internos. Los clientes proxy se comunican con los servidores proxy, los cuales, a su vez, transmiten solicitudes aprobadas de clientes a servidores auténticos y luego transmiten de nuevo las respuestas a los clientes.

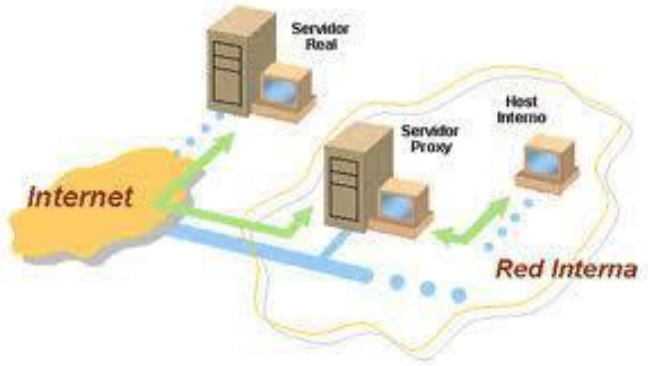


Fig. 5.5.a: Servidor Proxy

5.6 Gateways por defecto (puerta de enlace)

Un *default gateway* es normalmente un dispositivo de red configurado para permitir que las máquinas de una LAN conectadas a él tengan acceso a una red exterior. Es decir, que es un elemento necesario para enviar información fuera de la red local.

Sus principales características son:

- Los dispositivos dentro de una red deben tener configurada (habitualmente por software en la placa de red) la dirección del Gateway por defecto de la red a la cuál pertenecen.
- Un equipo dentro de una red local no puede comunicarse con elementos de otras redes utilizando su dirección IP. Cuando un host dentro de una red necesita comunicarse con dispositivos de otras redes, usa la dirección del Gateway por defecto para enviar la información fuera de la red local.
- Trabaja a nivel de **aplicación** (**Capa 7**) del modelo OSI.
- Habitualmente es una interfaz del route

ANEXO

1- Medios De Transmisión

Medios De Transmisión Sólidos

Cable de par no trenzado

Es el medio más sencillo para establecer comunicación. Cada conductor está aislado del otro, y se encuentra *balanceado,* es decir que ambos cables tienen igual longitud, espesor, etc. Ver Fig. 1.a.

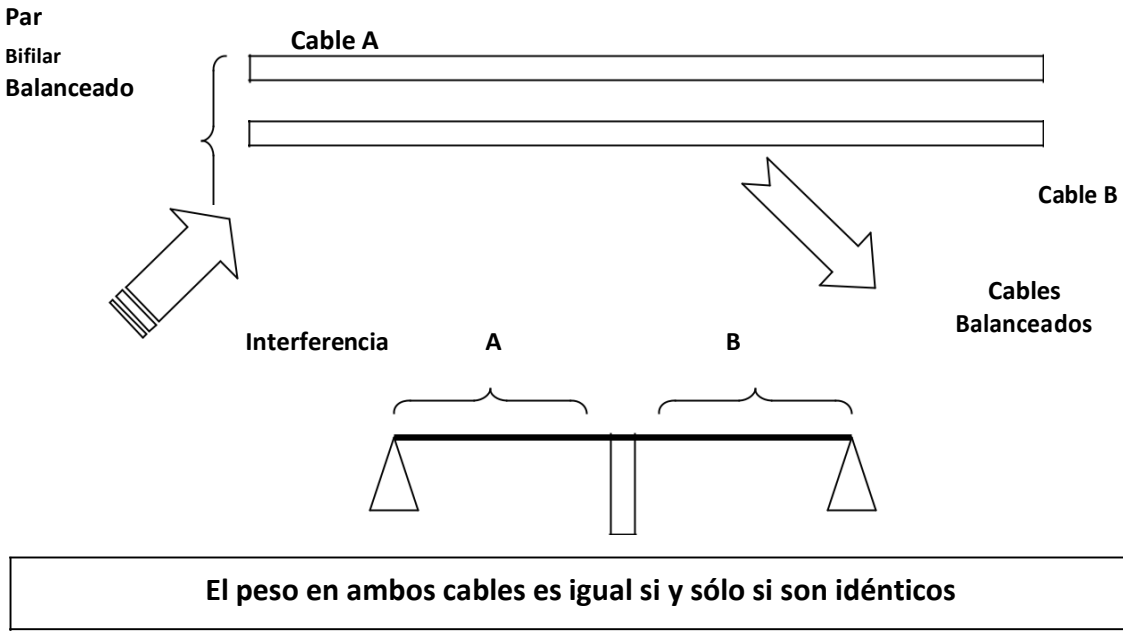


Fig. 1.a: Cable de par no trenzado.

Al ser los cables balanceados, cuando hay una interferencia, la misma se reparte entre ambos cables y se neutraliza (anula). Es el mismo caso que en una balanza equilibrada, se agregara un peso igual en ambos platillos: la balanza continuaría equilibrada.

Cuando se transmite una señal o dato, la línea se desbalancea, como si se agregara un grano de arena a uno de los platillos de la balanza. Por eso, este tipo de cable se utiliza en comunicaciones a una determinada distancia, no mayores a **1000 metros**. Es usado en telefonía. Si la distancia es mayor, obviamente, la velocidad disminuye.

Cable de par trenzado blindado (STP)

Si el cable trenzado se rodea con una malla conductora, se tiene el cable blindado ("**STP**, ***S**hielded **T**wisted **P**air*"), con el cual es posible reducir los efectos de interferencia de señales externas. Combina las técnicas de blindaje, cancelación (efecto de los pares trenzados de hilos para limitar la degradación de la señal que causan las interferencias electromagnéticas y de radiofrecuencia) y trenzado de cables.

Cada par de hilos está envuelto en un papel metálico. Los dos pares de hilos están envueltos juntos en una trenza o papel metálico. Según se especifica para el uso en instalaciones de redes *Token Ring*, el **STP** reduce el ruido eléctrico dentro del cable. También reduce el ruido electrónico desde el exterior del cable. Ver Fig. 1.b.

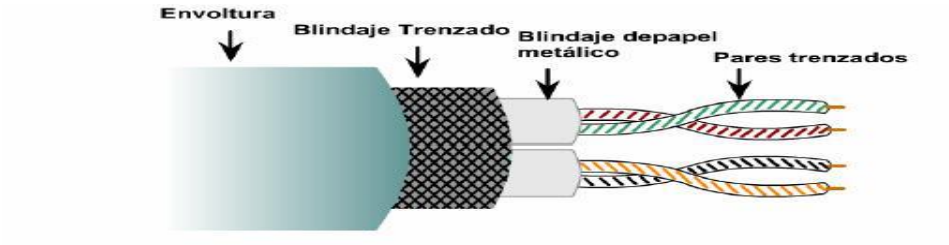


Fig. 1.b: Tipo de cable de par trenzado blindado (STP).

- ***Cable de par trenzado no blindado (UTP)***

En la red LAN, el cable trenzado no blindado ("UTP, Unshielded Twisted Pair") se utiliza para conectar la computadora a la red del ámbito respectivo.
Es un medio de cuatro pares de hilos que se utiliza en diversos tipos de redes. Cada uno de los 8 hilos de cobre individuales del cable **UTP** está revestido de un material aislante. Además, cada par de hilos está trenzado. Ver Fig. 1.c. Al igual que el cable **STP**, el cable **UTP** debe seguir especificaciones precisas con respecto a cuánto trenzado se permite por unidad de longitud del cable.

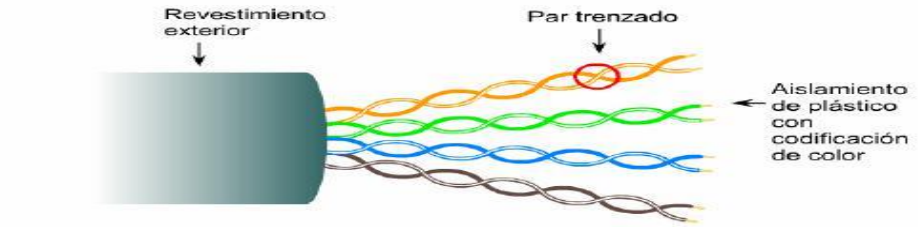


Fig. 1.c: Tipo de cable de par trenzado no blindado (UTP).

- ***Cable coaxial***

A medida que la velocidad de transmisión aumenta, la corriente eléctrica que circula por el cable tiende a hacerlo por la superficie exterior del mismo, de esta manera emplea menor sección del conductor, y por lo tanto se incrementa la resistencia eléctrica. Este fenómeno, se denomina **efecto pelicular**, hace que las pérdidas de transmisión a frecuencias altas sean considerables e impide el empleo de los cables **UTP** para velocidades mayores a 1 Mbps.

La estructura del cable coaxial, minimiza el efecto pelicular. El conductor sólido central es concéntrico al anillo del conductor externo o tierra que puede ser también sólido o mallado.

El espacio entre los dos conductores lo ocupa un **dieléctrico** (aislante), como se puede apreciar en la Fig. 1.d, el conductor central se encuentra aislado de los ruidos electromagnéticos externos. Con técnicas de modulación, que se verán más adelante, se aumenta considerablemente la distancia y la capacidad de cable. El cable coaxial se utiliza en las redes de TV por cable que transportan innumerable cantidad de canales de televisión.

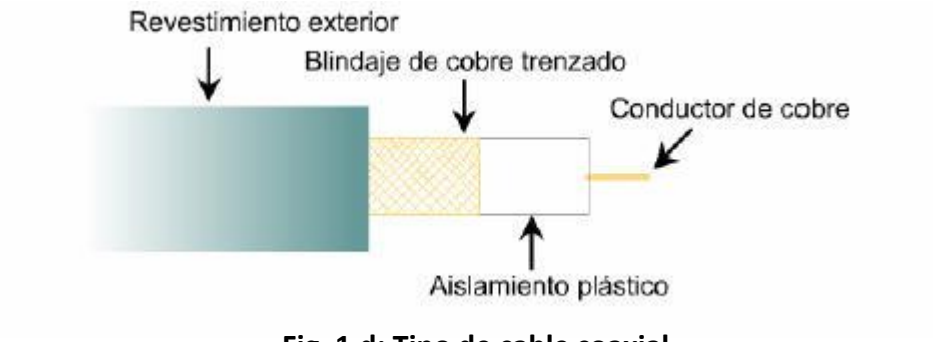


Fig. 1.d: Tipo de cable coaxial

- ***ADSL (Asymmetric Digital Subscriber Line) Línea de abonado digital asimétrica***

Bajo el nombre **xDSL** se definen una serie de tecnologías que permiten el uso de una línea de cobre (la que conecta nuestro domicilio con la central de Telefónica) para transmisión de datos de alta velocidad y, a la vez, para el uso normal como línea telefónica. Se llaman **xDSL** ya que los acrónimos de estas tecnologías acaban en **DSL**, que está por "*Digital Subscriber Line*" (línea de abonado digital): **HDSL, ADSL, RADSL, VDSL**. Cada una de estas tecnologías tiene distintas características en cuanto a prestaciones (velocidad de la transmisión de datos) y distancia de la central (ya que el cable de cobre no estaba pensado para eso, a cuanta más distancia peores prestaciones). Entre estas tecnologías la más adecuada para un uso domestico de Internet es la llamada ***ADSL.***

ADSL Permite la transmisión de datos a mayor velocidad en un sentido que en el otro (de eso viene el "asimétrica" en el nombre

Fibra óptica

La velocidad de transmisión que permite el cable coaxial es buena, pero limitada. Existe un medio de transmisión con principios tecnológicos diferentes que soluciona los problemas propios de los conductores de cobre. La **fibra óptica** no transporta la información como señales eléctricas sino que utiliza variaciones de un haz de luz a través de una fibra de vidrio. Las ondas de luz ofrecen un ancho de banda mucho mayor que la de las señales eléctricas. Además son completamente inmunes a las interferencias electromagnéticas y a todo tipo de ruido que tanto afectan las comunicaciones a través de cables de cobre.

Un cable de **fibra óptica** está compuesto por una fibra de vidrio para cada señal que se quiere transmitir, en un protector de plástico o **PVC** (*cloruro de polivinilo, "Poli Vinilo Cloruro*") que la aísla del exterior. La señal luminosa la debe generar un transmisor óptico que realiza la conversión de las señales eléctricas de los computadores de igual forma, en la recepción debe existir un elemento que realice la conversión inversa, o sea, de señal luminosa a señal eléctrica. Los componentes electrónicos encargados de realizar estas funciones de conversión son el **diodo emisor de luz** o **LED** y el **fototransistor** respectivamente.

La estructura de la fibra óptica consta de dos partes, como se puede observar en la Fig. 7:

- El núcleo de vidrio o material plástico.
- El cubrimiento también de vidrio pero con un **índice de refracción** (cociente entre la señal luminosa de salida y la de entrada) menor.

La luz se propaga a lo largo del núcleo según el ancho del mismo y de los materiales usados.

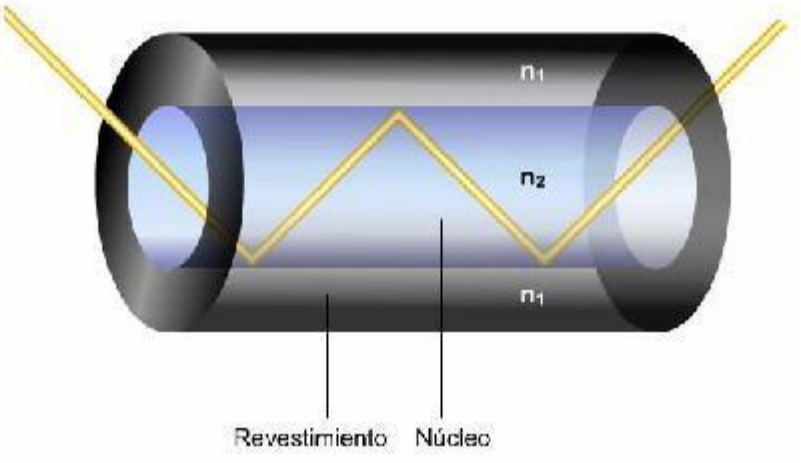


Fig. 1.e: Propagación de la luz en un cable de Fibra óptica

Las **ventajas** de los cables de fibra óptica respecto de los cables eléctricos son:

- Mayor velocidad de transmisión. similar a la velocidad de la luz (v = 3 X 10^8 m/s).
- Mayor capacidad de transmisión.
- Inmunidad total ante interferencias electromagnéticas.
- No existen problemas de retorno de tierra, o reflexiones.
- La atenuación aumenta con la distancia más lentamente que en el caso de los cables.
- Se consiguen cantidad de errores menores que los otros medios de transmisión vistos.
- No existe riesgo de cortocircuito o daños de origen eléctrico.
- Los cables de fibra óptica pesan la décima parte de los cables de corte apantallados.
- Los cables de fibra óptica son generalmente de menor diámetro.
- Los cables de fibra óptica son apropiados para utilizar en una amplia gama de temperaturas.
- Es más difícil escuchar sobre cables de fibra óptica que sobre cables eléctricos.
- Se puede incrementar la capacidad de transmisión de datos.
- La fibra óptica presenta una mayor resistencia a los ambientes y líquidos corrosivos
- Las materias primas para fabricar vidrio son abundantes.
- La vida media operacional y el tiempo medio entre fallos de la fibra óptica son superiores.Los costos de instalación y mantenimiento para grandes distancias son menores.

La mayor **desventaja** es que no se puede "pinchar" fácilmente este cable para conectar un nuevo nodo a la red.

Medios de Transmisión Aéreos

- ***Vía satélite***

Los datos entre computadoras también pueden transmitirse utilizando ondas electromagnéticas de radio a través del espacio libre por medio de satélites. Un haz de microondas se transmite al satélite desde la tierra. El haz lo recibe el satélite y lo retransmite empleando una antena direccional y un circuito interno llamado **transponder**. Ver Fig. 1.f.

Es posible lograr velocidades de transmisión de datos muy altas. Los satélites utilizados en comunicaciones son ***geoestacionarios***. Esto significa que el satélite realiza un giro a la órbita de la tierra en 24 horas de manera sincronizada con la rotación de la misma. Así aparece estático si se mira desde la superficie de la tierra. Las frecuencias para subir y bajar información del satélite son diferentes.

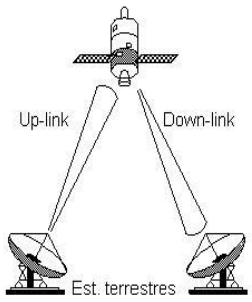


Fig. 1.f: comunicación vía satélite.

Algunas características de las comunicaciones vía satélite:

- Existe un retardo de 0,5 seg. en las comunicaciones.
- Los satélites tiene una vida de siete a diez años.
- Las estaciones terrenas suelen estar lejos de los usuarios y a menudo se necesitan caros enlaces de alta velocidad.
- Las comunicaciones con el satélite pueden ser interceptadas por cualquiera que disponga de un receptor en las proximidades de la estación.
- Los satélites geoestacionarios pasan por períodos en los que no pueden funcionar y además la órbita geoestacionaria está muy ocupada actualmente
- Cuando el satélite pasa directamente entre el Sol y la Tierra provocando un aumento de ruido térmico.

- ***Enlace de microondas***

Este sistema, similar en principio al del satélite, se utiliza en tierra para comunicar sitios separados por accidentes geográficos que hacen poco práctica y costosa la instalación de un medio físico como el cable. La condición principal para realizar un enlace de microondas, es la existencia de lo que se denomina **una línea de vista física** entre las antenas emisora y receptora. La máxima distancia de enlace que se logra sin problemas de atenuación es de aproximadamente **50 Km**. El haz de microondas sufre alteraciones cuando encuentra obstáculos similares a edificios, árboles, montañas y se afecta con las condiciones del clima como lluvia intensa, granizadas o neblina.

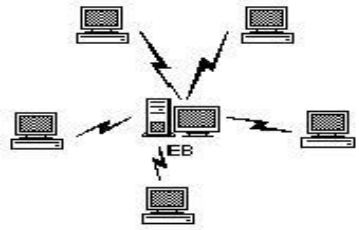
- ***Luz infrarroja***

Consiste en la emisión /recepción de un haz de luz, debido a esto, el emisor y receptor deben tener contacto visual (la luz viaja en línea recta). Debido a esta limitación pueden usarse espejos para modificar la dirección de la luz transmitida.

- ***Enlace de radio***

La transmisión de datos mediante ondas de radio a través de estaciones terrestres, también se utiliza para establecer comunicación entre computadoras localizadas en sitios relativamente cercanos. Por ejemplo, varios computadores ubicados en zonas rurales (vigilancia de la cuenca de un río, por ejemplo) estos pueden emitir sus datos, a través de radio, a un computador central.

Fig. 1.g: Enlace por radio.
La imagen muestra el proceso donde las siglas EB significan Estación Base



- ***Wireless***

Las tecnologías inalámbricas (*Wireless*) se están imponiendo sobre las tecnologías alámbricas convencionales por diversas razones:

- Más económicas, debito al alto costo de los cables y de la mano de obra.
- Permiten la conexión de gran cantidad de dispositivos móviles, aún en áreas complicadas.
- Brindan más libertad de movimiento para los dispositivos conectados.
- Posibilidad de conectar dispositivos a mayores distancias sin cableado.

Metodologías De Transmisión Aéreas

- ***Voice sobre IP***

VoIP es el transporte de voz digitalizada y encapsulada dentro de paquetes de datos, utilizando el Protocolo de Internet (IP), sobre redes públicas o privadas.

En redes **VoIP**, las señales analógicas deben ser convertidas en paquetes digitales antes de ser transportadas a través de las redes de datos **IP**. Una vez llegados a destino, estos paquetes deben ser nuevamente vueltos a su estado original de ondas de sonido analógicas para ser escuchados por el receptor.

- ***Telefonía IP***

Se refiere a la posibilidad de realizar llamadas telefónicas, cursando el tráfico sobre Internet en lugar de la red telefónica pública conmutada, **PSTN**. Es un sistema avanzado de comunicaciones que permite crear un sistema telefónico digital, agregando funcionalidades como integración de aplicaciones, movilidad, etc.

El software de comunicaciones se presenta en diversas formas. Para los usuarios que trabajan exclusivamente en una red local, pueden manejarse con un **sistema operativo de red**.

2- Redes Avanzadas de Alta Velocidad (RAAV)

Desde mediados de la década del 90 se están desarrollando en el mundo las **redes académicas avanzadas de alta velocidad**, las cuales tienen como principal objetivo desarrollar las tecnologías y aplicaciones avanzadas de Internet. En los Estados Unidos el proyecto que lidera este desarrollo es **Internet2**, en Canadá el proyecto CA*NET3, en Europa los proyectos TEN-155 y GEANT, y en Asia el proyecto APAN. Adicionalmente, todas estas redes están conectadas entre sí, formando una gran

red avanzada de alta velocidad de alcance mundial. En Latinoamérica, las redes académicas de México, Brasil y Chile ya se han integrado a **Internet2** entre los años 1999 y 2000; Argentina hizo lo propio en diciembre del 2001.

El *BACKBONE* de **Internet2** (la **Red ABILENE** y la red **VBNS**) tiene velocidades que superan los **10 Gbps**, y las conexiones de las universidades a este *BACKBONE* varían entre **622 Mbps** y **2 Gbps**.

El **objetivo básico** de los grupos que administran **RAAV** es desarrollar la próxima generación de aplicaciones *Telemáticas* (Telecomunicaciones - Informática) para facilitar las tareas académicas y educativas. Esto se debe a que las principales universidades consideran que los avances de las redes constituyen un aspecto fundamental para la labor en el campo de la enseñanza y de la investigación. Para llevar adelante estos proyectos, cada una de las universidades que participan cuentan con un equipo de desarrolladores e ingenieros que trabajan para hacer posible la creación de las aplicaciones necesarias para interactuar. Las universidades son instancias calificadas para desempeñar un papel principal en el desarrollo de los objetivos, ya que abarcan la demanda de tipos de aplicaciones que esta red de nueva generación desarrollará, junto con el aporte del talento necesario para llevar a cabo el proyecto.

Esquema general de las arquitecturas RAAV

La vedette en estas arquitecturas es sin duda el **GIGAPOP** termino acuñado a partir de **GIGA**byte capacity **P**oint **O**f **P**resence (*punto de presencia con capacidad de gigabits*).

El Gigapop es el punto de interconexión de tecnología avanzada y alta capacidad donde los participantes del proyecto RAAV intercambien tráfico de servicios avanzados entre si.

Las universidades de una determinada región se unen en un gigapop regional para conseguir una variedad de servicios de red. Los gigapops se unen para adquirir y gestionar la conectividad entre los mismos en una organización a la que denominamos **Collectivite Entity** (*entidad colectiva*). La Fig. 1 nos muestra a usuarios finales de las redes Baker, Charlie y Delta intercambiando servicios avanzados a través de los Gigapops y la entidad colectiva.